MASARYK UNIVERSITY JOURNAL OF LAW AND TECHNOLOGY

VOLUME 15 | NUMBER 2 | WINTER 2021 | ISSN 1802-5943

PEER REVIEWED

CONTENTS:

www.mujlt.law.muni.cz

Masaryk University Journal of Law and Technology
issued by Institute of Law and Technology
Faculty of Law, Masaryk University
www.mujlt.law.muni.cz

Official Partner (Czech Republic)
ROWAN LEGAL, advokátní kancelář s.r.o. (www.rowanlegal.com/cz/)
Na Pankráci 127, 14000 Praha 4

Subscriptions, Enquiries, Permissions
Institute of Law and Technology, Faculty of Law, MU (cyber.law.muni.cz)

listed in HeinOnline (www.heinonline.org)
listed in Scopus (www.scopus.com)
reg. no. MK ČR E 17653

MASARYK UNIVERSITY JOURNAL OF
LAW AND TECHNOLOGY

VOLUME **15** | NUMBER **2** | WINTER **2021**

LIST OF ARTICLES

DOI 10.5817/MUJLT2021-2-1

STANDARD SETTING ORGANISATIONS FOR THE IOT: HOW TO ENSURE A BETTER DEGREE OF LIABILITY?[1]

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

[1] 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)[2] 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[3] but also because it is bound to be one of the most widespread applications of IoT technology among consumers[4] and is sufficiently adaptable to possibly mix with more refined and pervasive technologies such as Edge Computing or AI[5]. 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

[2] We will use the terms SSOs and SDOs with the same meaning throughout the article.

[3] 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 [Accessed 10 May 2021] p. 46.

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

[5] 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 […]"* [6].

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[7]. There are several legal remedies to help create a level playing field for the different operators: Fair, Reasonable and Non-Discriminatory licenses (FRAND)[8], but also alternative dispute resolution systems[9] or traditional litigation under IP and competition law grounds.

[6] 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.

[7] 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[10] 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'"*[11].

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[12], 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 form other IoT objects is that these objects are directed mostly to consumers[13]. 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[14] (and eventually a fog layer before that) through a gateway within the same house. The variety of damages

---

[8] 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.

[9] 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.

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

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

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

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

[14] 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[15], 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[16]. 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[17]. In line with this approach, I will refer to the liability of classification societies[18] 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[19]. This coexistence of private and

[15] 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].

[16] 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*, 1st 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.

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

[18] 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.

[19] Ulfbeck, V. and Møllmann, 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[20]. 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[21]. 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[22]. 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"* [23].

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

[20] 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.

[21] Basedow J. and Wurmnest (2005) *op. cit*. p. 101.

[22] Basedow J. and Wurmnest (2005) *op. cit*. p. 102.

[23] 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.

[24] 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'*[25]. 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[26]. The case involved defective breasts implants made by P.I.P. company in the context of the Medical Devices Directive[27]. 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

[25] Wallerman, A. (2018) *op.cit.*, p. 273.

[26] 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.

[27] Council Directive 93/42/EEC of 14 June 1993 concerning medical devices *Official Journal of the European Union (O J L 169)* 12 Julv1993. 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[28]. 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[29]. 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[30]. Finally, there are Open Source SSOs which are characterised by more openness, due process and transparency in the decision-making process than private SDOs [31]. Some authors share the view that OSS and traditional SDOs are complementary, and therefore both necessary[32]. However, sometimes it takes just one company (single standard promoter), promoting its *de facto* standard, for the standard to become mainstream and

[28] 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.

[29] 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.

[30] Biddle, C. (2017) *ibid.*

[31] Biddle, C. (2017) *ibid*.

[32] 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[33]. 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[34]. 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[35]. 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[36].

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?

---

[33] 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.

[34] 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.

[35] 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.

[36] 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[37]. 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)[38] 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[39]. 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

[37] Bakhoum, M. et al. (2018) *Personal Data in Competition, Consumer Protection and Intellectual Property. Towards a Holistic Approach*. Berlin: Springer.

[38] 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].

[39] 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 [Accessed 10 Mayy 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[40]. 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[41].

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[42]. International standards of ISO and IEC accepted also OCF specifications[43]. Although its specifications are publicly available, OCFs members are private companies. By perusing the site, the organisational chart is clearly detailed[44]. Furthermore, there is one M2M which unites major ICT SSOs in the world included the European ETSI[45]. Its main effort is to create a '*common service layer*'[46] mostly for industrial IoT. Its site provides access to the identity of the members, its

[40] 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].

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

[42] 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 [Accessed 10 May 2021] p. 22.

[43] Nativi, S. et al. (2020), *ibid.*

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

[45] 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 [Accessed 10 May 2021], pp.22-23.

[46] Nativi S. et al. (2020) *ibid.*

organisational chart and its processes[47]. Finally, there is OMA Spec Works for a connected world[48] which comes from the fusion of IPSO, Open Mobile Alliance and Open Mobile SpecWorks[49]. 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[50]. 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[51], which will facilitate the object to object communication layer. Furthermore, there is the 'Project Connected Home over IP[52]' 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[53]. 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[54], 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

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

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

[49] 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 [Accessed 10 May 2021], p. 24.

[50] Nativi S. et al. (2020) *op.cit*. p. *23.*

[51] 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].

[52] Nativi, S. et al. (2020) *op.cit.,* pp. 22-24.

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

[54] 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 [Accessed 10 May 2021], pp. 22-23.

gaps in IoT standards[55]. It is divided in working groups and collaborates with other regional organisations and with international standardisations bodies[56].

The only private but open stand-alone promoter which will have an influence in Europe is Mozilla IoT and Web of things[57]. Mozilla can be considered a single promoter standard setting actor that is privacy driven[58]. 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 […]"*[59].

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 [60]. 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

---

55 Nativi, S. et al. (2020) *ibid.*

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

57 Nativi S. et al. (2020) *op.cit.* p. 24.

58 Nativi S. et al. (2020) *ibid.*

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

60 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[61].

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[62].

---

[61] 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.

[62] 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[63], 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[64]. As already pointed out by the Commission and restated by Commissioner Breton

[63] 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[65], a closer collaboration with patents offices in this respect is also desirable[66]. In conclusion, the actual system still works but the changes brought by the house 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

[64] 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].

[65] 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 potentialAn 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].

[66] 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] Bandhiopadyay, D. and Sen, J. (2011) Internet of Things: Applications and challenges in technology standardization. *Wireless Personal Communications*, 1.

[5] Bakhoum, 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*, 1st 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 potentialAn 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_iot_%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 Møllmann, 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.

DOI 10.5817/MUJLT2021-2-2

THE REFERENCE TO "A WORK OR SOFTWARE" AS THE FACTOR DETERMINING THE SCOPE OF THE EUROPEAN UNION PUBLIC LICENCE (EUPL) V. 1.2

by

KRZYSZTOF ŻOK*

Free and open source software (FOSS) has undoubtedly become an important element of intellectual property law. It is therefore not surprising that the European Commission developed its own non-proprietary licence, i.e. the European Union Public Licence (EUPL). The article examines the reference to 'a work of software' to determine the scope of the licence. For this purpose, the paper discusses the reasons for the creation of the EUPL, the relationship between a work and software as well as the structure of a computer program. The following considerations also include the compatible licences listed in the EUPL Appendix. The article concludes that the reference to a work or software is not accidental because it removes serious doubts arising from the concept of a computer program. Thus, this legal solution may facilitate the wider adoption of the licence.

KEY WORDS

Computer Program, Copyright Law, European Law, European Union Public Licence (EUPL), Non-proprietary Software Licences

* krzysztof.zok@amu.edu.pl, Assistant Professor (Adjunct), Adam Mickiewicz University in Poznań, Faculty of Law and Administration, Poland.

1. INTRODUCTION

1.1 THE SIGNIFICANCE OF THE EUROPEAN UNION PUBLIC LICENCE (EUPL)

On 20 October 2020, the European Commission adopted the new Open Source Software Strategy 2020-2034 'Think Open'.[1] According to one of the governing principles provided for in the document, the Commission will share the source code of its future IT project, wherever it is reasonable.[2] For this purpose, the European Union Public Licence (EUPL) v. 1.2 should be used as the preferred licence.[3] This makes the EUPL particularly interesting, although there are other reasons for investigating it as well.

Firstly, non-proprietary licences often reflect the point of view of the legal systems of common law countries, especially the point of view of American law.[4] This is the case, for example, with one of the most popular free and open source software (FOSS) licences, i.e. GNU General Public Licence (GPL), which has been identified as requiring internationalization.[5] The general focus on American law is understandable, given that the Free Software Movement and the Open Source Software Movement started in the United States.[6] Moreover, many IT companies are still located in the United States. The EUPL does not question the relevance or the usefulness of such non-proprietary licences. Indeed, its Appendix shows recognition, not negation, of some of the most popular FOSS licences developed in the United States. Instead, the EUPL offers the opportunity to take greater account of the European law perspective, which includes

---

1 Communication of 21 October 2020 'Open Source Software Strategy 2020-2023. Think Open'. COM(2020) 7149 final. Available from: https://ec.europa.eu/info/sites/info/files/en_ec_open_source_strategy_2020-2023.pdf [Accessed 22 July 2021].

2 Op. cit., p. 9.

3 Commission Implementing Decision (EU) 2017/863 of 18 May 2017 updating the open source software licence EUPL to further facilitate the sharing and reuse of software developed by public administrations. *Official Journal of the European Union* (2017/L-128/59) 19 May. Available from: https://eur-lex.europa.eu/eli/dec_impl/2017/863/oj [Accessed 22 July 2021].

4 Dusollier, S. (2007) Sharing Access to Intellectual Property Through Private Ordering. *Chicago-Kent Law Review*, 82(3), p. 1427-1428.

5 Gomulkiewicz, R.W. (2005) General Public License 3.0: Hacking the Free Software Movement's Constitution. *Houston Law Review*, 42(4), pp. 1034-1035.

6 See Dusollier, S. (2007) Sharing Access to Intellectual Property Through Private Ordering. *Chicago-Kent Law Review*, 82(3), p. 1398-1399; González de Alaiza Cardona, J.J. (2007) Open Source, Free Software, and Contractual Issues. *Texas Intellectual Property Law Review*, 15(2), pp. 165-169, 178-179; Unni, V.K. (2016) Fifty Years of Open Source Movement: an Analysis through the Prism of Copyright Law. *Southern Illinois University Law Journal*, 40(2), pp. 279-283.

solutions characteristic of the legal systems belonging to the civil law tradition.[7]

Secondly, non-proprietary licences are mostly written in English as the only official language of the agreement.[8] For instance, the Free Software Foundation, one of the major FOSS organizations, offers licences in English.[9] Other language versions are available as non-binding information. This creates a potential barrier for those who prefer to use their national language. It should be noted that licence intelligibility can be a decisive factor for a software developer or a company interested in FOSS. Besides, a clear wording of the licence is essential due to the potential gap between the formal language in which typical licences are drawn up and the informal language used in FOSS communities.[10] Moreover, Member States often oblige public organizations to use the local language.[11] As a result, there was a need for a licence which would be useful in all official languages of the European Union.[12] The EUPL uniquely addresses this issue, i.e. by offering multiple linguistic versions which have identical value.[13] This corresponds to the principle of linguistic diversity of the European Union, laid down in the Charter of Fundamental Rights of the European Union.[14]

---

[7] Dusollier, S. (2007) Sharing Access to Intellectual Property Through Private Ordering. *Chicago-Kent Law Review*, 82(3), p. 1430; Schmitz, P.-E. (2013) the European Union Public Licence (EUPL). *International Free and Open Source Software Law Review*, 5(2), p. 125; Schmitz, P.-E. (2014) *EUPL v.1.1. European Union Public Licence. Guides for Users and Developers*. Available from: https://joinup.ec.europa.eu/collection/eupl/guidelines-users-and-developers [Accessed 22 July 2021], p. 4. Similarly, Schmitz, P.-E. (2013) the European Union Public Licence (EUPL). *International Free and Open Source Software Law Review*, 5(2), p. 122.

[8] Dusollier, S. (2007) Sharing Access to Intellectual Property Through Private Ordering. *Chicago-Kent Law Review*, 82(3), p. 1428-1429.

[9] Free Software Foundation. (2021) *Licenses*. [online]. Available from: https://www.gnu.org/licenses/licenses.html.en [Accessed 22 July 2021].

[10] Villa, L. (2010) Lawyers in the Bazaar: Challenges and Opportunities for Open Source Legal Communities. *International Free and Open Source Software Law Review*, 2(1), p. 81-82.

[11] Schmitz, P.-E. (2013) the European Union Public Licence (EUPL). *International Free and Open Source Software Law Review*, 5(2), p. 122.

[12] Ibid.; Schmitz, P.-E. (2014) *EUPL v.1.1. European Union Public Licence. Guides for Users and Developers*. Available from: https://joinup.ec.europa.eu/collection/eupl/guidelines-users-and-developers [Accessed 22 July 2021], p. 4.

[13] EUPL, Article 13. Multilingualism of the EUPL is considered its distinctive feature, see Schmitz, P.-E. (2013) the European Union Public Licence (EUPL). *International Free and Open Source Software Law Review*, 5(2), pp. 121 and 125; Wiebe, A. and Heidinger, R. (2009) *European Union Public Licence – EUPL v. 1.1*. [online]. Available from: https://joinup.ec.europa.eu/collection/eupl/documentation-directory-articles-eupl [Accessed 22 July 2021], p. 3.

Thirdly, the multiplicity of non-proprietary licences is often considered a source of practical concerns about their compatibility.[15] In particular, the question may arise to what extent it is possible to distribute an original computer program under one licence and its modifications or components (e.g. libraries) under another licence. The EUPL aims to remove this doubt by providing the following list of compatible licences (hereinafter: 'the compatible licences'):

- CeCILL v. 2.0[16] and v. 2.1[17];
- Creative Commons Attribution-ShareAlike Unported v. 3.0 (CCPL)[18];
- Eclipse Public License (EPL) v. 1.0[19];
- European Union Public Licence (EUPL) v. 1.1[20] and 1.2;
- GNU Affero General Public License (AGPL) v. 3.0[21];
- GNU General Public License (GPL) v. 2.0[22] and v. 3.0[23];
- GNU Lesser General Public License (LGPL) v. 2.1[24] and v. 3.0[25];

---

[14] Charter of Fundamental Rights of the European Union. *Official Journal of the European Union* (2012/C-326/391) 26 October. Available from: http://data.europa.eu/eli/treaty/char_2012/oj [Accessed 22 July 2021], Article 22.

[15] Dusollier, S. (2007) Sharing Access to Intellectual Property Through Private Ordering. *Chicago-Kent Law Review*, 82(3), p. 1430; Schmitz, P.-E. (2013) the European Union Public Licence (EUPL). *International Free and Open Source Software Law Review*, 5(2), p. 123.

[16] Commissariat à l'Energie Atomique, Centre National de la Recherche Sceintifique, Institut National de la Recherche en Informatique et en Automatique. (2006) *CeCILL Free Software License Agreement*. [online]. Available from: https://cecill.info/licences/Licence_CeCILL_V2-en.html [Accessed 22 July 2021].

[17] Commissariat à l'Energies Alternatives, Centre National de la Recherche Sceintifique, Institut National de la Recherche en Informatique et en Automatique. (2013) *CeCILL Free Software License Agreement*. [online]. Available from: https://cecill.info/licences/Licence_CeCILL_V2.1-en.html [Accessed 22 July 2021].

[18] Creative Commons Corporation. *Creative Commons Attribution-ShareAlike v. 3.0 Unported*. [online]. Available from: https://creativecommons.org/licenses/by-sa/3.0/legalcode [Accessed 22 July 2021].

[19] Eclipse Foundation. *Eclipse Public License - v 1.0*. [online]. Available from: https://www.eclipse.org/legal/epl-v10.html [Accessed 22 July 2021].

[20] IDABC. (2009) *European Union Public Licence – EUPL v.1.1*. [online]. Available from https://wayback.archive-it.org/12090/20200212153832/https://ec.europa.eu/idabc/eupl.html [Accessed 22 July 2021].

[21] Free Software Foundation. (2007) *GNU Affero General Public License*. [online]. Available from: https://www.gnu.org/licenses/agpl-3.0.en.html [Accessed 22 July 2021].

[22] Free Software Foundation. (1991) *GNU General Public License, version 2*. [online]. Available from: https://www.gnu.org/licenses/old-licenses/gpl-2.0.html [Accessed 22 July 2021].

[23] Free Software Foundation. (2007) *GNU General Public Licence*. [online]. Available from: https://www.gnu.org/licenses/gpl-3.0.html [Accessed 22 July 2021].

[24] Free Software Foundation. (1999) *GNU Lesser General Public License, version 2.1*. [online]. Available from: https://www.gnu.org/licenses/old-licenses/lgpl-2.1.html [Accessed 22 July 2021].

[25] Free Software Foundation. (2007) *GNU Lesser General Public License*. [online]. Available from: https://www.gnu.org/licenses/lgpl-3.0.en.html [Accessed 22 July 2021].

- Mozilla Public Licence (MPL) v. 2.0[26];
- Open Source License (OSL) v. 2.1[27] and v. 3.0[28];
- Québec Free and Open-Source Licence Reciprocity (LiLiQ-R)[29];
- Québec Free and Open-Source Licence Strong Reciprocity (LiLiQ-R+)[30].

The EUPL lists several versions of the same compatible licence. This is understandable considering that newer versions do not automatically replace older versions. The licensor may thus still use a previous version of the licence. However, for the sake of brevity, the article indicates in the body text the version number of the licence where it is relevant to the argument. Otherwise, the version number is only displayed in the footnotes.

1.2 THE SCOPE OF THE ARTICLE

The analysis of FOSS licences often focuses on the rights and obligations of the parties. Such a perspective is justified and it certainly has practical significance. This article, however, aims to explore a different area, i.e. the subject matter covered by the licence. While the above issue has attracted less scholars' attention, it is not inconsequential. It should be noted that the EUPL is primarily directed to EU agencies. Nevertheless, it can also serve as a model licence for others interested in FOSS.[31] Indeed, according to the data on the Joinup, a platform established by the European Commission, by the end of 2015 about 15.000 projects were distributed under the EUPL.[32] From this point of view, the subject matter covered by the licence is essential since it determines the scope of application

[26] Mozilla Foundation. *Mozilla Public License Version 2.0*. [online]. Available from: https://www.mozilla.org/en-US/MPL/2.0/ [Accessed 22 July 2021].

[27] Open Source Initiative. (2004) the *Open Software License 2.1 (OSL-2.1)*. [online]. Available from: https://opensource.org/licenses/osl-2.1.php [Accessed 22 July 2021].

[28] Open Source Initiative. (2005) the *Open Software License 3.0 (OSL-3.0)*. [online]. Available from: https://opensource.org/licenses/OSL-3.0 [Accessed 22 July 2021].

[29] Québec – Forge gourvenementale. (2019) *Québec Free and Open-Source Licence version 1.0 – Reciprocity*. [online]. Available from: https://forge.gouv.qc.ca/licence/en/liliq-v1-0/ [Accessed 22 July 2021]; Québec – Forge gourvenementale. (2019) *Québec Free and Open-Source Licence version 1.1 – Reciprocity*. [online]. Available from: https://forge.gouv.qc.ca/licence/en/liliq-v1-1/ [Accessed 22 July 2021].

[30] Québec – Forge gourvenementale. (2019) *Québec Free and Open-Source Licence version 1.0 – Strong Reciprocity*. [online]. Available from: https://forge.gouv.qc.ca/licence/en/liliq-v1-0 [Accessed 22 July 2021]; Québec – Forge gourvenementale. (2019) *Québec Free and Open-Source Licence version 1.1 – Strong Reciprocity*. [online]. Available from: https://forge.gouv.qc.ca/licence/en/liliq-v1-1/ [Accessed 22 July 2021].

[31] Schmitz, P.-E. (2014) *EUPL v.1.1. European Union Public Licence. Guides for Users and Developers*. Available from: https://joinup.ec.europa.eu/collection/eupl/guidelines-users-and-developers [Accessed 22 July 2021], p. 4.

of the EUPL. This in turn potentially impacts the popularity of the licence. Furthermore, the rights and obligations of the parties relate to the subject matter. Its inadequate description may thus impede the use, modification or distribution of the licensed computer program.

According to the preamble, the EUPL v. 1.2 applies to 'the Work'.[33] This term is defined as 'the Original Work and its Derivative Works'.[34] The licence explains these expressions by indicating that they refer to 'a work or software'.[35] Interestingly, this description of the covered subject matter is sometimes regarded as an improvement over the EUPL v. 1.1. The latter licence applies to 'the Work or Software', which some scholars have found confusing.[36] In my opinion, however, the above comment requires a more detailed analysis. Despite the different wording of the preamble, the EUPL v. 1.2 still refers to 'a work or software'. Nevertheless, it should be noted that the previous version of the licence defines the terms 'the Original Work' and 'the Software' as software only. There is no reference to a work as the denotation. Hence, the EUPL v. 1.2 seems to adopt a broader scope of application, which is not necessarily clearer or more useful.

The article focuses on the examination of the concept of a 'work' or 'software' as the basis for determining the subject matter covered by the EUPL. Additionally, the paper considers the compatible licences to fill in the gaps which result from not clarifying what constitutes a work or software under the licence. This approach also makes it possible to reflect on the consistency of the EUPL as well as the advantages and disadvantages of the licence. Finally, it should be emphasized that the article does not analyse the question of the originality of a computer program as well as the question of derivative works. It would certainly be beyond the scope of this paper to consider these issues because of their complexity in the context of FOSS.

2. WORK AS THE COVERED SUBJECT MATTER

[32] Joinup. *Impact of the EUPL*. [online]. Available from: https://joinup.ec.europa.eu/collection/eupl/impact-eupl [Accessed 22 July 2021].

[33] EUPL v. 1.2, preamble.

[34] EUPL v. 1.2, Article 1.

[35] *Ibidem.*

[36] Schmitz, P.-E. (2013) the European Union Public Licence (EUPL). *International Free and Open Source Software Law Review*, 5(2), p. 126. See EUPL v. 1.1, preamble.

As in the previous version, the EUPL v. 1.2 does not define the term 'work'. However, it is worth noting that under the EUPL v. 1.1 some scholars treated this expression as a reference to the subject matter covered by copyright.[37] Others regarded the term 'work' as a synonym for 'software and/or documentation'.[38] In my opinion, the first position is correct and should also be adopted under the current version of the licence. The definition of 'the Original Work' in the EUPL v. 1.2 implies two different subject matters and thus precludes the term 'work' from being restricted to software only.[39] Otherwise, part of this provision would be redundant, which is difficult to accept. Instead, the discussed expression should be understood as the subject matter covered by copyright.[40] Besides, the other language versions of the EUPL v. 1.2 support this conclusion. For example, the French and German texts of the licence use in this context standard legal terminology for copyrighted material ('ouvre' and 'Werk' respectively).[41]

The above conclusion does not fully eliminate the uncertainty about the subject matter covered by the licence. Pursuant to Software Directive, computer programs are protected by copyright as literary works within the meaning of the Berne Convention.[42] Thereby, software also constitutes a work. More importantly, this classification is not only limited to European law. Rather, it can be seen as the international legal standard. For instance, the Treaty on Trade-Related Aspects of Intellectual Property (TRIPS) provides for that computer programs should be protected by copyright as literary works under the Berne Convention.[43] Consequently, the question

---

[37] Wiebe, A. and Heidinger, R. (2009) *European Union Public Licence – EUPL v. 1.1*. [online]. Available from: https://joinup.ec.europa.eu/collection/eupl/documentation-directory-articles-eupl [Accessed 22 July 2021], p. 6.

[38] Schmitz, P.-E. (2014) *EUPL v.1.1. European Union Public Licence. Guides for Users and Developers*. Available from: https://joinup.ec.europa.eu/collection/eupl/guidelines-users-and-developers [Accessed 22 July 2021], p. 7.

[39] EUPL v. 1.2, Article 1.

[40] Schmitz, P.-E. (2013) the European Union Public Licence (EUPL). *International Free and Open Source Software Law Review*, 5(2), p. 126.

[41] EUPL v. 1.2, preamble and Article 1 (the French and German texts).

[42] *Berne Convention for the Protection of Literary and Artistic Works*, 9 September 1886 (as amended on 28 September 1979). Available from: https://wipolex.wipo.int/en/treaties/textdetails/12214 [Accessed 22 July 2021] (hereinafter: 'Berne Convention'); Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version). *Official Journal of the European Union* (2009/L-111/16) 5 May. Available from: http://data.europa.eu/eli/dir/2009/24/oj [Accessed 22 July 2021] (hereinafter: 'Software Directive'), Article 1(1).

arises why the EUPL refers to the general concept of work when it also covers a specific type of work, i.e. software.

Moreover, the European Commission clearly stated that the main purpose of the EUPL is to 'further facilitate the sharing and reuse of software developed by public administrations'[44]. Therefore, the licence seems to be specifically intended for computer programs. The conclusion is in line with the fact that non-proprietary licences were initially developed for computer programs and are still often associated with them. Yet, the EUPL Appendix clarifies that the CCPL applies 'for works other than software'[45]. The EUPL thus appears to implicitly accept its broader scope. This makes the reference to a work as a way of describing the subject matter covered by the EUPL even more puzzling.

However, a similar solution can be found in some of the compatible licences.[46] Under the GPL v. 2.0, some scholars pointed out that the definition of a computer program goes beyond its literal meaning and includes other works such as a novel or a piece of music.[47] Yet, they also added that the licence mainly covers software. In my view, the acceptance of the broad scope of the GPL is correct and it corresponds with the position of the Free Software Foundation.[48] Nevertheless, the compatible licences are usually only analysed from the perspective of software. The term 'work' is then identified with a computer program (e.g. a software library).[49]

It should also be emphasized that referring to a work is not a uniform approach. Other compatible licences indicate that they apply to a computer

---

[43] *Marrakesh Agreement Establishing the World Trade Organization – Annex 1C. Agreement on Trade-Related Aspects of Intellectual Property Rights*, 15 April 1994. Available from: https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm [Accessed 22 July 2021], Article 10.

[44] Commission Implementing Decision (EU) 2017/863 of 18 May 2017 updating the open source software licence EUPL to further facilitate the sharing and reuse of software developed by public administrations. *Official Journal of the European Union* (2017/L-128/59) 19 May. Available from: https://eur-lex.europa.eu/eli/dec_impl/2017/863/oj [Accessed 22 July 2021], recital 4.

[45] EUPL v. 1.2, Appendix.

[46] AGPL, preamble; GPL v. 2.0, Article 0; GPL 3.0, preamble. Similarly, LiLiQ-R v. 1.0, Articles 1 and 2; LiLiQ-R+ v. 1.0, Articles 1 and 2; LiLiQ-R v. 1.1, Articles 1 and 2; LiLiQ-R+ v. 1.1, Articles 1 and 2. Moreover, according to the preamble of the LGPL v. 3.0, the licence incorporates the provisions of the GPL v. 3.0. As a result, both licences share the same scope.

[47] Schultz, C. (2005) Ziffer 0. In: *Die GPL kommenirt und erklärt.* Köln: O'Reilly, p. 37.

[48] Free Software Foundation. (2020) *Frequently Asked Questions about the GNU Licenses*. [online]. Available from: https://www.gnu.org/licenses/gpl-faq.html [Accessed 22 July 2021].

[49] See Bain, M. (2010) Software Interactions and the GNU General Public License. *International Free and Open Source Software Law Review*, 2(2), pp. 172-173.

program or software.[50] More importantly, they do not state that they cover broadly understood works. Only two compatible licences define their scope by using the general concept of 'any original work of authorship' or 'literary and/or artistic work', without mentioning a computer program or software.[51]

From this perspective, it appears that the reference to a work or software in the EUPL is not accidental. Otherwise, it could be expected that the revised version of the licence would remove the confusing reference to a work. This, in turn, raises the question of the reasons for adopting such a solution. In particular, it could be argued that extending the scope of the EUPL is necessary or else the purpose of the licence could not be achieved. The verification of this assumption, however, requires showing that the limitation of the covered subject matter to computer programs only is not satisfactory.

3. SOFTWARE AS THE COVERED SUBJECT MATTER

3.1 COMPUTER PROGRAM ACCORDING TO SOFTWARE DIRECTIVE

The EUPL does not explain what constitutes software. Some of the compatible licences follow the same approach.[52] However, most define the term 'computer program' or 'software', although it should be emphasized only a few of them provide a detailed explanation. They are discussed in the next subsection (see 3.2). The definitions in other compatible licences are based on a generalization (e.g. software is understood as a work)[53] or a tautology (e.g. software is understood as a computer program)[54]. As a result, they offer limited insight into the subject matter covered by the EUPL.

It is worth noting that proper understanding of software is not only a matter of theoretical dispute. The general purpose of the licence is to allow the licensee to undertake activities related to the work (e.g. a computer program) which would otherwise constitute an infringement of exclusive

[50] CeCILL v. 2.0, preamble; CeCILL v. 2.1, preamble; EPL v. 1.0, preamble; LGPL v. 2.1, Article 0; MPL v. 2.0, Articles 1.3, 1.4 and 2.1.

[51] CCPL v. 3.0, preamble, Article 1(h); OSL v. 2.1, preamble; OSL v. 3.0, preamble.

[52] OSL v. 2.1, preamble; OSL v. 3.0, preamble.

[53] AGPL v. 3.0, Article 0; GPL v. 2.0, Article 0; GPL v. 3.0, Article 0.

[54] CeCILL v. 2.0, Article 1; CeCILL v. 2.1, Article 1; EPL v. 1.0, Article 1; GPL v. 2.0, Article 0; LiLiQ-R v. 1.0, Article 2; LiLiQ-R+ v. 1.0, Article 2; LiLiQ-R v. 1.1, Article 2; LiLiQ-R+ v. 1.0, Article 2; MPL v. 2.0, Article 1.4.

rights (i.e. copyright). Consequently, if an element of the work is not protected, it can be used freely, without the need to obtain the rightholder's authorization. This, in turn, raises the question of parts of the software that are covered by a licence.

The answer is not always easy since the exact scope of protection may differ from one legal system to another.[55] Some of the compatible licences aim to solve this problem by choosing the applicable law[56] or stipulating that their terms should be interpreted in accordance with specific legal acts.[57] The EUPL adopts the first approach. In principle, the licence recognizes that parties are free to choose the applicable law.[58] In the absence of such a choice, the EUPL is governed by the law of the Member State where the licensor has its seat, resides or has its registered office. If the latter requirement is not met, the licence is subject to Belgian law. Therefore, the EUPL is always governed by the law of one or another Member State, unless the parties decide otherwise.

The EUPL also stipulates that the disputes arising from its provisions should be heard by the Court of Justice of the European Union.[59] Therefore, the Court can be expected to follow its own decisions based on Software Directive. This further strengthens the reference to European law, although express jurisdiction of the Court is limited to litigation between the European Union institutions, bodies, offices or agencies. Thus, the EUPL achieves one of its goals, effectively introducing the European perspective on software protection. Hence, in a typical situation other legal doctrines, e.g. Arbitration-Filtration-Comparison test which is often used in the United States, will probably have limited relevance.[60]

Moreover, the complex structure of computer programs can be another source of practical concerns. As provided for in Software Directive, the protection applies only to the expression of a computer program.[61] It does not extend to the ideas and principles underlying any element

---

[55] Bain, M. (2010) Software Interactions and the GNU General Public License. *International Free and Open Source Software Law Review*, 2(2), pp. 170-171.

[56] CeCILL v. 2.0, Article 13.1; CeCILL v. 2.1, Article 13.1; EPL v. 1.0, Article 7; LiLiQ-R v. 1.0, Article 11; LiLiQ-R v. 1.1, Article 11; LiLiQ-R+ v. 1.0, Article 11; LiLiQ-R+ v. 1.1, Article 11. OSL v. 2.1, Article 11; OSL v. 3.0, Article 11.

[57] CCPL v. 3.0, Article 8(f).

[58] EUPL, Article 15.

[59] EUPL, Article 14.

[60] Similarly, Bain, M. (2010) Software Interactions and the GNU General Public License. *International Free and Open Source Software Law Review*, 2(2), p. 169.

[61] Software Directive, Article 1(2) and Recital 11.

of the above type of work. This also refers to interfaces, i.e. parts of the computer program which enable the interconnection and interaction between elements of software and hardware.[62] Furthermore, Software Directive classifies logic, algorithms and programming languages as unprotected ideas and principles.[63] The Court of Justice of the European Union approved this conclusion in the *SAS Institute Inc.* case by stating that the functionality of a computer program as well as the programming language and the format of data files should not be treated as a form of expression of a computer program.[64] While this decision does not directly apply to FOSS, it may have an impact on the linking of computer programs (e.g. application programming interfaces (APIs)).[65]

More importantly, in the *Bezpečnostní softwarová asociace* case, the Court of Justice of the European Union held that interfaces, in particular graphic user interfaces (GUI), are not a form of expression of a computer program.[66] The Court put forward two arguments in support of its ruling. Firstly, the form of expression of a computer program should enable the reproduction of the software. This requirement is not met in the case of interfaces since they do not allow the user to copy the computer program. Secondly, interfaces are generally bound by their technical function. Therefore, a software developer who creates them often does not enjoy sufficient freedom of expression. As a result, interfaces do not meet the requirement of originality. However, an interface may be protected as a separate work under Directive 2011/29, if it constitutes its author's own intellectual creation.[67] Hence, the audio and visual components of the software in a general sense are not parts of the computer program in the legal sense.

While the above decision is correct, it may be counter-intuitive to a layperson. In particular, it can be expected that an average user will identify graphic user interfaces and other on-screen displays with

---

[62] Software Directive, Recital 10.

[63] Software Directive, Recital 11.

[64] Judgment of 2 May 2012, *SAS Institute Inc.*, C-406/10, EU:C:2012:259, paragraphs 39-46.

[65] Schmitz, P.-E. (2013) the European Union Public Licence (EUPL). *International Free and Open Source Software Law Review*, 5(2), pp. 127-128.

[66] Judgment of 5 October 2009, *Bezpečnostní softwarová asociace*, C-393/09, EU:C:2010:816, paragraphs 28-42 and 49-51.

[67] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. *Official Journal of the European Communities* (2001/L-167/10) 22 June. Available from: http://data.europa.eu/eli/dir/2001/29/oj [Accessed 22 July 2021].

the computer program itself. At the same time, these displays should not be considered irrelevant simply because they do not constitute a form of expression of software. On the contrary, they often impact the way the users experience the computer program. This, in turn, is a key factor which influences the popularity of the software. Limiting the scope of the EUPL to only computer programs could therefore be disadvantageous. This would introduce the uncertainty as to whether a specific part of the computer program can be treated as its form of expression. From this point of view, the reference to a work as a subject matter cover by the EUPL is justified. It removes these doubts and consequently allows the licensee to use the IT project as a whole, regardless of how its particular elements are classified.

The practical ramifications of the distinction between a work and software are evident in the case of a 'fork'. This term is used in FOSS communities to describe a situation in which an existing IT project is almost completely relaunched under a new leader.[68] Forking may be justified by philosophical reasons (i.e. the initial IT project is overtaken by a proprietary licensor) or technical reasons (i.e. the leader of the initial IT project refuses to merge new functions or modify software). From a legal point of view, however, forking often requires copying not only the computer program in the strict sense but also its name, logo and other intangible assets. The latter elements are usually outside the concept of software. Thus, a narrow definition of the covered subject matter could prevent the effective reuse of software, which is one of the main objectives of the EUPL.

From this point of view, it could be argued that the EUPL should simply refer to the work, without explicitly mentioning software in its scope of application. After all, the licence would then also cover computer programs with all their relevant components as copyrighted materials. However, the question arises whether this approach does not dilute the concept of a computer program. In my opinion, a negative answer should be given in this respect. It should be noted that the concept of a computer program and the concept of a work are determined by European and Member States legislation and case law. The parties cannot thus contractually extend the copyright protection because this

[68] Schmitz, P.-E. (2013) the European Union Public Licence (EUPL). *International Free and Open Source Software Law Review*, 5(2), p. 129.

would violate the closed catalogue of rights in *rem* (i.e. rights effective against anyone). Consequently, the concept of a computer program as such should be defined, in particular, on the basis of Software Directive, irrespective of the scope of the EUPL. If the licence referred only to a work, the court and the parties would still need to consider the type of work covered by the licence and the extent of its protection.

This is probably the weakest side of the above approach. A simple reference to the work does not solve the problem of making the scope of the EUPL clear and operational. The approach only reformulates the doubts from a different perspective. Therefore, it could be argued that the reference to 'a work or software' is helpful since it shows possible legal frameworks governing the licensed subject matter. Moreover, the parties cannot contractually extend the copyright protection. However, they can specify which protected elements of the computer program are covered by the licence. Hence, the reference to software could contribute to a more precise definition of the scope of the EUPL, if the licence clearly indicated these elements.

3.2 COMPUTER PROGRAM ACCORDING TO THE COMPATIBLE LICENCES

Unlike the EUPL, several compatible licences, including the most popular ones, define at least some software components, thus offering a more detailed description of a computer program. Therefore, it could be argued that the definitions contribute to the success of these compatible licences. On the other hand, the lack of a similar explanation seems unfavourable for the EUPL. Especially when one considers that the compatible licences indicate the parts of a computer program which have not been identified in the European case law.

A comprehensive set of definitions is found in the AGPL v. 3.0 and the GPL v. 3.0 which explain many key terms ('Standard Interface', 'System Libraries', 'Major Component' and 'The Corresponding Source'). The purpose of this clarification is to make sure that the recipient of the computer program in the form of object code has also access to the complete source code.[69] According to these licences, the conveying of non-source forms of software should be accompanied by the transfer

[69] AGPL v. 3.0, Article 1; GPL v. 3.0, Article 1.

of the Corresponding Source.[70] Similarly, the GPL v. 2.0 indicates that the complete source code covers 'all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable'[71]. Nevertheless, this does not refer to 'anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable'[72].

A similar provision can also be found in the LGPL v. 2.1.[73] More importantly, however, another set of definitions is provided for in the LGPL v. 2.1 ('library', 'Library' [sic], 'work that uses the Library' and 'work based on the Library')[74] and the LGPL v. 3.0 ('The Library', 'Application', 'Combined Work', 'Minimal Corresponding Source' and 'Corresponding Application Code')[75]. The latter licence also refers to 'Library Header Files' and 'Combined Libraries'.[76] The above definitions aim to address the uncertainty regarding the impact of using software libraries on the scope of these licences. It should be noted that linking a computer program to a library may create a derivative work.[77]

Moreover, it could be argued that distinguishing particular elements of a computer program is characteristic of free software licences which originated in the United States. This is, however, not correct. a similar solution can also be found in CeCILL which has been specially developed to meet the requirements of European (French) legislation. These licences introduce the concepts of 'Module', 'External Module' and 'Internal Module'.[78] The distinction is significant since CeCILL does not apply to External Modules which may be distributed under the license chosen

[70] AGPL v. 3.0, Article 6; GPL v. 3.0, Article 6.

[71] GPL v. 2.0, Article 3.

[72] GPL v. 2.0, Article 3.

[73] LGPL v. 2.1, Article 6.

[74] LGPL v. 2.1, Article 0.

[75] LGPL v. 3.0, Article 0.

[76] LGPL v. 3.0, Articles 3 and 5, respectively.

[77] See Bain, M. (2010) Software Interactions and the GNU General Public License. *International Free and Open Source Software Law Review*, 2(2), pp. 175-178; Dusollier, S. (2007) Sharing Access to Intellectual Property Through Private Ordering. *Chicago-Kent Law Review*, 82(3), pp. 1416-1418; Gue, Th. (2012) Triggering the Infection: Distribution and Derivative Works under the GNU General Public License. *University of Illinois Journal of Law, Technology & Policy*, 1, p. 129-139; Morgan, M.F. (2010) the Cathedral and the Bizarre: an Examination of the "Viral" Aspects of the GPL. *John Marshall Journal of Computer and Information Law*, 27(3), pp. 386-416 and 464-492.

[78] CeCILL v. 2.1, Article 1; CeCILL v. 2.0, Article 1.

by the licensee who created them.[79] In contrast, the EUPL does not specifically address any of the above issues.

From this point of view, the description of software as the subject matter covered by the EUPL is less precise than in some of the most popular compatible licences. As a result, the question of the completeness of source code, software libraries and supplementary functions and services is largely left with the parties and the courts. This may consequently hinder a wider adoption of the EUPL. However, it could also be argued that the lack of precision is a positive feature of the licence. The EUPL thus gains flexibility which is much needed in the rapidly changing area of IT law. Moreover, the use of general concepts may facilitate the adoption of the licence because it avoids the difficulties which could arise from the difference between the legal systems of the Member States. The increasing use of the EUPL suggests that the broad reference to the software may be satisfactory to the parties.

It is also worth noting that more wordy licences, particularly the GPL, has been criticized for lack of clarity.[80] For instance, despite the definitions, the completeness of the source code may still raise practical concerns. The GPL v. 3.0 illustrates this well:

> *"[f]or example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work."*[81]

As a result, it can be expected that an average user may find it difficult to understand these definitions since they raise doubts even among IT professionals. Therefore, the length of the licences does not translate into its intelligibility.

---

[79] CeCILL v. 2.1, Article 5.3.3 and 6.3; CeCILL v. 2.0, Article 5.3.3 and 6.3.

[80] Gomulkiewicz, R.W. (2005) General Public License 3.0: Hacking the Free Software Movement's Constitution. *Houston Law Review,* 42(4), p. 1035; Morgan, M.F. (2010) the Cathedral and the Bizarre: an Examination of the "Viral" Aspects of the GPL. *John Marshall Journal of Computer and Information Law*, 27(3), pp. 351-352.

[81] GPL v. 3.0, Article 1.

4. DOCUMENTATION

Some of the compatible licences also treat documentation as part of software.[82] The OSL even specifies that documentation should describe how to modify the computer program.[83] Yet, such a classification is considered rare among FOSS licences.[84] For example, the Free Software Foundation recommends a separate licence made specifically for manuals.[85] At first glance, the extension of the concept of software may seem irrelevant. However, a closer examination reveals serious legal doubts. In particular, the uncertainty arises whether documentation can be regarded as a protected element of a computer program within the meaning of Software Directive.

The importance of this question stems from the fact that documentation significantly facilitates understanding how a computer program works. This applies not only to FOSS but also to proprietary computer programs. As a result, the licensee is usually interested in obtaining the documentation. However, in the case of FOSS, documentation becomes almost essential. Such computer programs are often developed over an extended period by many people who do not directly interact with each other and who are not part of the same organization. As a result of this 'bazaar' method, it is crucial to get the most complete information about the software.[86] In contrast, proprietary computer programs are frequently developed according to the 'cathedral' method. This term refers to a situation in which one entity coordinates the process of creating a computer program and thus has all the necessary information.

Nevertheless, the answer to the above question seems negative due to the difference between software and its documentation. Indeed, in the *SAS Institute Inc.* case, the Court of Justice of the European Union held that user manuals can be protected under Directive 2001/29.[87] As a result, it can be

[82] CeCILL v. 2.0, Article 1; CeCILL v. 2.1, Article 1; EPL v. 1.0, Article 1(a); LiLiQ-R v. 1.0, Article 2; LiLiQ-R v. 1.1, Article 2; LiLiQ-R+ v. 1.0, Article 2; LiLiQ-R+ v. 1.1, Article 2.

[83] OSL v. 2.1, Article 3; OSL v. 3.0, Article 3.

[84] Osborne, K. (2015) License Profile: the Eclipse Public License. *International Free and Open Source Software Law Review*, 7(1), p. 4.

[85] Free Software Foundation. (2020) *Frequently Asked Questions about the GNU Licenses*. [online]. Available from: https://www.gnu.org/licenses/gpl-faq.html [Accessed 22 July 2021]. See Free Software Foundation. (2008) *GNU Free Documentation License*. Available from https://www.gnu.org/licenses/fdl-1.3.html [Accessed 22 July 2021].

[86] Raymond, E.S. (2000) the *Cathedral and the Bazaar*. [online]. Available from: http://www.catb.org/~esr/writings/cathedral-bazaar/cathedral-bazaar/ [Accessed 22 July 2021].

[87] Judgment of 2 May 2012, *SAS Institute Inc.*, C-406/10, EU:C:2012:259, paragraphs 63-70.

argued that books or files describing how a computer program works are excluded from the scope of Software Directive. Therefore, they do not fall within the concept of a computer program. This would once again point to the accuracy of the EUPL which refers not only to software but also to a work. Indeed, the conclusion is shared by some scholars.[88] At the same time, the broad description of the covered subject matter seems to be better suited for the needs of FOSS. Namely, it could be argued that software developers can distribute not only a computer program (with all its relevant components) but also related documentation under a single licence.

Without questioning this conclusion, it is worth noting that the status of documentation under Software Directive is more complex. According to the Directive, the term 'computer program' includes 'preparatory design work leading to the development of a computer program provided that the nature of the preparatory work is such that a computer program can result from it at a later stage'[89]. The Court of Justice of the European Union also approved this definition.[90] Moreover, it could be assumed that the significance of documentation in the context of FOSS may often translate into a precise description of the computer program. Hence, it cannot be ruled out that for this reason the documentation may be sufficiently complete for the reproduction of the software. The reference to a work in the EUPL could thus be seen as redundant since at least some of documentation would classify as a preparatory design work.

In my opinion, however, the above provision is not entirely without a doubt. The Swedish High Court requested a preliminary ruling which would determine how complete such materials should be to qualify as software.[91] Unfortunately, the question was withdrawn and the Court of Justice of the European Law could not answer it. Therefore, the reference to a work in the EUPL seems a better solution as it avoids the uncertainty related to the completeness of documentation.

---

[88] Schmitz, P.-E. (2013) the European Union Public Licence (EUPL). *International Free and Open Source Software Law Review*, 5(2), p. 126. Under the EUPL v. 1.1, see Wiebe, A. and Heidinger, R. (2009) *European Union Public Licence – EUPL v. 1.1*. [online]. Available from: https://joinup.ec.europa.eu/collection/eupl/documentation-directory-articles-eupl [Accessed 22 July 2021], p. 6.

[89] Software Directive, Recital 7 and Article 1(1).

[90] Judgment of 5 October 2009, *Bezpečnostní softwarová asociace*, C-393/09, EU:C:2010:816, paragraph 37; Judgment of 2 May 2012, *SAS Institute Inc.*, C-406/10, EU:C:2012:259, paragraph 37.

[91] Request of 9 May 2018, *Dacom Limited v IPM Informed Portfolio Management AB*, C-313/18, *Official Journal of European Union* (2018/C-268/31) 30 July. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CN0313 [Accessed 22 July 2021].

5. SUMMARY

The EUPL is an interesting legal solution aimed at creating a European non--proprietary licence. For this purpose, the licence is governed by the law of one of the Member States. As a result, the harmonized legal framework of Software Directive applies to the EUPL. Moreover, the licence is available in all the official languages of the European Union.

The article analyses the reference to 'a work or software' which defines the scope of the licence. The expression may seem puzzling since a computer program is a type of work. However, a closer examination shows that a reference only to the software would be unsatisfactory. The parties would then suffer the consequences of an incorrect assessment of what constitutes software. This could easily raise practical concerns due to the complex structure of computer programs. The reference to the broader concept of work reduces these doubts by including under the EUPL the components which are not protected as software. It also provides greater flexibility, much needed in the rapidly changing area of IT law. Besides, the generality of the EUPL facilitates seamless integration with the compatible licences.

The article also indicates that some of the compatible licences offer a more precise definition of software. The parties could probably benefit from the adoption of a similar solution in the EUPL. Nevertheless, the article shows that such definitions are not necessary for the proper functioning of the licence in question.

LIST OF REFERENCES

[1] Bain, M. (2010) Software Interactions and the GNU General Public License. *International Free and Open Source Software Law Review*, 2(2).

[2] *Berne Convention for the Protection of Literary and Artistic Works*, 9 September 1886 (as amended on 28 September 1979). Available from: https://wipolex.wipo.int/en/treaties/textdetails/12214 [Accessed 22 July 2021].

[3] Charter of Fundamental Rights of the European Union. *Official Journal of the European Union* (2012/C-326/391) 26 October. Available from: http://data.europa.eu/eli/treaty/char_2012/oj [Accessed 22 July 2021].

[4] Christensen, T.M. (2006) the GNU General Public License: Constitutional Subversion? *Hastings Constitutional Law Quarterly*, 33(4).

[5] Commissariat à l'Energie Atomique, Centre National de la Recherche Sceintifique,

Institut National de la Recherche en Informatique et en Automatique. (2006) *CeCILL Free Software License Agreement*. [online]. Available from: https://cecill.info/licences/Licence_CeCILL_V2-en.html [Accessed 22 July 2021].

[6] Commissariat à l'Energies Alternatives, Centre National de la Recherche Sceintifique, Institut National de la Recherche en Informatique et en Automatique. (2013) *CeCILL Free Software License Agreement*. [online]. Available from: https://cecill.info/licences/Licence_CeCILL_V2.1-en.html [Accessed 22 July 2021].

[7] Commission Implementing Decision (EU) 2017/863 of 18 May 2017 updating the open source software licence EUPL to further facilitate the sharing and reuse of software developed by public administrations. *Official Journal of the European Union* (2017/L-128/59) 19 May. Available from: https://eur-lex.europa.eu/eli/dec_impl/2017/863/oj [Accessed 22 July 2021].

[8] Communication of 21 October 2020 'Open Source Software Strategy 2020-2023. Think Open'. COM(2020) 7149 final. Available from: https://ec.europa.eu/info/sites/info/files/en_ec_open_source_strategy_2020-2023.pdf [Accessed 22 July 2021].

[9] Creative Commons Corporation. *Creative Commons Attribution-ShareAlike v. 3.0 Unported*. [online]. Available from: https://creativecommons.org/licenses/by-sa/3.0/legalcode [Accessed 22 July 2021].

[10] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. *Official Journal of the European Communities* (2001/L-167/10) 22 June. Available from: http://data.europa.eu/eli/dir/2001/29/oj [Accessed 22 July 2021].

[11] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version). *Official Journal of the European Union* (2009/L-111/16) 5 May. Available from: http://data.europa.eu/eli/dir/2009/24/oj [Accessed 22 July 2021].

[12] Dusollier, S. (2007) Sharing Access to Intellectual Property Through Private Ordering. *Chicago-Kent Law Review*, 82(3).

[13] Eclipse Foundation. *Eclipse Public License - v 1.0*. [online]. Available from: https://www.eclipse.org/legal/epl-v10.html [Accessed 22 July 2021].

[14] Free Software Foundation. (1991) *GNU General Public License, version 2*. [online]. Availabe from: https://www.gnu.org/licenses/old-licenses/gpl-2.0.html [Accessed 22 July 2021].

[15] Free Software Foundation. (1999) *GNU Lesser General Public License, version 2.1*. [online]. Available from: https://www.gnu.org/licenses/old-licenses/lgpl-2.1.html [Accessed 22

July 2021].

[16] Free Software Foundation. (2007) *GNU Affero General Public License*.

[17] Free Software Foundation. (2007) *GNU General Public Licence*. [online]..

[18] Free Software Foundation. (2007) *GNU Lesser General Public License*. [online]. Available from: https://www.gnu.org/licenses/lgpl-3.0.en.html [Accessed 22 July 2021].

[19] Free Software Foundation. (2008) *GNU Free Documentation License*. Available from https://www.gnu.org/licenses/fdl-1.3.html [Accessed 22 July 2021].

[20] Free Software Foundation. (2020) *Frequently Asked Questions about the GNU Licenses*. [online]. Available from: https://www.gnu.org/licenses/gpl-faq.html [Accessed 22 July 2021].

[21] Free Software Foundation. (2021) *Licenses*. [online]. Available from: https://www.gnu.org/licenses/licenses.html.en [Accessed 22 July 2021].

[22] Gomulkiewicz, R.W. (2005) General Public License 3.0: Hacking the Free Software Movement's Constitution. *Houston Law Review*, 42(4).

[23] González de Alaiza Cardona, J.J. (2007) Open Source, Free Software, and Contractual Issues. *Texas Intellectual Property Law Review*, 15(2).

[24] Gue, Th. (2012) Triggering the Infection: Distribution and Derivative Works under the GNU General Public License. *University of Illinois Journal of Law, Technology & Policy*, 1.

[25] IDABC. (2009) *European Union Public Licence – EUPL v.1.1*. [online]. Available from https://wayback.archive-it.org/12090/20200212153832/https://ec.europa.eu/idabc/eupl.html [Accessed 22 July 2021].

[26] Joinup. *Impact of the EUPL*. [online]. Available from: https://joinup.ec.europa.eu/collection/eupl/impact-eupl [Accessed 22 July 2021].

[27] Judgment of 5 October 2009, *Bezpečnostní softwarová asociace*, C-393/09, EU:C:2010:816.

[28] Judgment of 2 May 2012, *SAS Institute Inc.*, C-406/10, EU:C:2012:259.

[29] *Marrakesh Agreement Establishing the World Trade Organization – Annex 1C. Agreement on Trade-Related Aspects of Intellectual Property Rights*, 15 April 1994. Available from: https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm [Accessed 22 July 2021].

[30] Morgan, M.F. (2010) the Cathedral and the Bizarre: an Examination of the "Viral" Aspects of the GPL. *John Marshall Journal of Computer and Information Law*, 27(3).

[31] Mozilla Foundation. *Mozilla Public License Version 2.0*. [online]. Available from: https://www.mozilla.org/en-US/MPL/2.0/ [Accessed 22 July 2021].

[32] Open Source Initiative. (2004) the *Open Software License 2.1 (OSL-2.1)*. [online]. Available from: https://opensource.org/licenses/osl-2.1.php [Accessed 22 July 2021].

[33] Open Source Initiative. (2005) the *Open Software License 3.0 (OSL-3.0)*. [online]. Available from: https://opensource.org/licenses/OSL-3.0 [Accessed 22 July 2021].

[34] Osborne, K. (2015) License Profile: the Eclipse Public License. *International Free and Open Source Software Law Review*, 7(1).

[35] Québec – Forge gourvenementale. (2019) *Québec Free and Open-Source Licence version 1.0 – Reciprocity*. [online]. Available from: https://forge.gouv.qc.ca/licence/en/liliq-v1-0/ [Accessed 22 July 2021].

[36] Québec – Forge gourvenementale. (2019) *Québec Free and Open-Source Licence version 1.1 – Reciprocity*. [online]. Available from: https://forge.gouv.qc.ca/licence/en/liliq-v1-1/ [Accessed 22 July 2021].

[37] Québec – Forge gourvenementale. (2019) *Québec Free and Open-Source Licence version 1.0 – Strong Reciprocity*. [online]. Available from: https://forge.gouv.qc.ca/licence/en/liliq-v1-0 [Accessed 22 July 2021].

[38] Québec – Forge gourvenementale. (2019) *Québec Free and Open-Source Licence version 1.1 – Strong Reciprocity*. [online]. Available from: https://forge.gouv.qc.ca/licence/en/liliq-v1-1/ [Accessed 22 July 2021].

[39] Raymond, E.S. (2000) the *Cathedral and the Bazaar*. [online]. Available from: http://www.catb.org/~esr/writings/cathedral-bazaar/cathedral-bazaar/ [Accessed 22 July 2021].

[40] Request of 9 May 2018, Dacom Limited v IPM Informed Portfolio Management AB, C-313/18, *Official Journal of the European Union* (2018/C-268/31) 30 July. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CN0313 [Accessed 22 July 2021].

[41] Schmitz, P.-E. (2013) the European Union Public Licence (EUPL). *International Free and Open Source Software Law Review*, 5(2).

[42] Schmitz, P.-E. (2014) *EUPL v.1.1. European Union Public Licence. Guides for Users and Developers*. Available from: https://joinup.ec.europa.eu/collection/eupl/guidelines-users-and-developers [Accessed 22 July 2021].

[43] Schultz, C. (2005) Ziffer 0. In: *Die GPL kommenirt und erklärt*. Köln: O'Reilly.

[44] Unni, V.K. (2016) Fifty Years of Open Source Movement: an Analysis through the Prism of Copyright Law. *Southern Illinois University Law Journal*, 40(2).

[45] Villa, L. (2010) Lawyers in the Bazaar: Challenges and Opportunities for Open Source Legal Communities. *International Free and Open Source Software Law Review*, 2(1).

[46] Wiebe, A. and Heidinger, R. (2009) *European Union Public Licence – EUPL v. 1.1*.

DOI 10.5817/MUJLT2021-2-3

ONLINE PLATFORMS AND "DEPENDENT WORK" AFTER UBER[1]

by

SILVIA LATTOVÁ[*]

Digitalization is bringing new challenges, including changing the way how people work, which create uncertainty. Technology driven innovations are changing the way of work, while society react to such development by creating different types of jobs and workplaces. What is important today can be redundant tomorrow. Labour and civil laws will need to react to keep up with such changes. The main aim of this paper is to focus on the specific types of activities – such as virtual work or crowd work and the relationships between digital platforms, workers, employers, and clients while offering and providing services via online platforms. Further the paper will outline the responsibility of online platforms if considered to be in a position of an employer. Due to the lack of compliance with labour laws and related duties, online platforms can gain an unfair competition advantage compared to "traditional" employer. Virtual workers can potentially suffer from inadequate or limited access to the certain kind of protection (when compared to the "traditional" employees). Further the paper will consider the responsibility of online platforms if they are in fact to be considered an employer.

KEY WORDS

Virtual Work, Crowd Work, Online Platforms, Dependent Work, Uber

[1] The author would like to express her gratitude to doc. JUDr. Marianna Novotná, PhD. from Trnava University, Trnava, Slovakia for her valuable comments on the working version of this paper.

[*] E-mail: sisa.lattova@gmail.com, PhD candidate at Trnava University, Trnava, Slovakia.

1. INTRODUCTION

Online platforms are an important part of the digital economy. The growth of online platforms in the last decade is visible and well known. Platforms connect different subjects, providers/workers are offering services and customers are looking for such services via internet. Nowadays, it is easy to book an urban transport, find graphic designers, or people who will walk your dog. Some online platforms, such as Uber or Upwork, constantly promise freedom, flexibility and earning opportunity for those who choose to provide their "services" through such online platforms. Uber, for example, is offering a platform to connect the drivers and customers looking for transport, while promising flexibility for the drivers when earning money. These services can be described also as a "crowdsourcing", "virtual work" or "crowd working". The term "crowdsourcing", as defined by Howe, is "the act of taking a job traditionally performed by a designated agent (usually an employee) and outsourcing it to an undefined, generally large group of people in the form of an open call."[2] Taking such a definition into consideration and looking at the services provided by Uber, it is possible to see some similarities – as per the definition of crowd work, this is provided online, in cyberspace and so are the services offered by Uber. Felstiner[3] argued that crowd work is performed often anonymously and governed – to the extent that it is governed at all – by compulsory clickwrap participation agreements. Could this potentially be the condition applicable as per the definition of crowd work or virtual work? The term "virtual work" (as introduced by Cherry) could be understood as "an umbrella term to encompass work in virtual worlds, crowdsourcing, click working, and even sweeping in, to some degree, the commonplace telecommuting and "mobile executives" that have become ubiquitous over time".[4] Again, while looking at the Uber use case, we can most probably talk also about the virtual work as Ubers´ services are performed by an anonymous driver (anonymous to the customers) and are provided online.

---

[2] Howe,J. (2016) *Crowdsourcing: A Definition.* Available from: https://crowdsourcing.typepad.com/cs. [Accessed 14 December 2020].

[3] Felstiner, A. (2011) Working the Crowd: Employment and Labor Law in the Crowdsourcing Industry. *Berkeley Journal of Employment and Labor Law,* Vol. 32. No. 1. p. 145. Available from: https://ssrn.com/abstract=1593853 [Accessed 18 June 2021].

[4] Cherry, M. (2009) Working for (Virtually) Minimum Wage: Applying the Fair Labor Standards Act in Cyberspace. *Alabama Law Review*, Volume 60. N. 5. p. 1078. Available from: (PDF) Working for (Virtually) Minimum Wage: Applying the Fair Labor Standards Act in Cyberspace (researchgate.net). [Accessed 17 May 2021].

The rise of online platforms has not gone unnoticed by the regulatory bodies. The European Commission identified key areas of the online platforms on the market, interaction between the subjects, etc.[5] These online platforms share certain important characteristics:

- They can create and shape new markets, to challenge traditional ones, and to organise new form of participation or conducting business based on collecting, processing, and editing large amounts of data.
- They operate in multisided markets but with varying degrees of control over direct interactions between groups of users.
- They benefit from "network effect", where, broadly speaking, the value of the service increases with the number of users.
- *They play a key role in digital value creation, notably by capturing significant value (including through data accumulatio), facilitating new business ventures, and creating new strategic dependencies.*[6]

Online platforms are capable of bringing significant benefits to the whole of society; one can learn new skills, someone's business might reach larger audience, people can get real-time news from all over the world within a second. New job opportunities are another important benefit worth mentioning. However, the growing importance of the digital economy, linked with the diversity and fast-changing nature of platform ecosystems, also raises new policy and regulatory challenges. The platform economy presents major innovation opportunities for European start-ups, as well as for established market operators to develop new business models, products, and services.[7]

Platform capitalism is another term used when describing online platforms like Uber or Airbnb promoting their services to be able to provide competition to the "traditional" services offering transport services or accommodation services.

The idea of collaborative economy is not new. People are sharing goods, services, space and money with each other and the peer-to-peer commerce economy is enabling the crowd to become like a company, disrupting

---

[5] European Commission (2016) *Online Platforms and the Digital Single Market Opportunities and Challenges for Europe*. COM/2016/0288 final. p. 2. [online]. Available from: EUR-Lex - 52016DC0288 - EN - EUR-Lex (europa.eu). [Accessed 14 May 2021].

[6] *Ibid.*

[7] *Ibid.*

traditional business models.[8] But while in the past it was more related to the sharing of information and assets[9], these days it is more about saving time and money, which potentially is also having impact when it comes to the virtual workers.

The online platforms are also changing the view of the traditional labour law and employment relationship. People working for online platforms do not always have a clear position when it comes to the employment relationship. But such uncertainty results not only from the length of the working time as the "traditional" labour law is also offering the possibility to work part-time.

The main issue is related to the fact that online platforms usually argue that they are in the neutral position while offering the services, i.e., that they are only intermediaries.

If we take Uber as an example, drivers who work on the Uber platform do not pursue an independent activity that exists independently of the platform. On the contrary, the activity exists solely because of the platform, without which it would have no sense. Therefore, it is wrong to compare Uber to intermediation platforms such as those used to make hotel bookings or purchase flights. Similarities clearly exist (such as the mechanism for booking or purchasing directly on the platform, the payment facilities or even the ratings system). However, in a contrast to the situation of Uber´s drivers, both hotels and airlines are undertakings which operate completely independently of any intermediary platform and for which such platforms are simply one of a number of ways of marketing their services. Furthermore, it is the hotels and airlines – not the booking platforms – that determine the conditions under which their services are provided, starting with the prices.[10]

The following paper assesses the different types of relationship that could applied when talking about the work for the online platform. When

---

[8] "*Graphic: A Timeline of Corporations in the Collaborative Economy*". Catalyst Companies. Available from: http://www.catalystcompanies.co/graphic-a-timeline-of-corporations-in-the-collaborative-economy/. [Accessed 05 June 2021].

[9] For example, Kimpton Hotels launches a "Forgot it? We´ve got it!" list of travel essentials for travellers in 2004, Radiohead asks consumers to pay what they want for "In Rainbows" album in 2007 or Daimler launches car2to car-sharing service in 2009. See: *Graphic: A Timeline of Corporations in the Collaborative Economy*. Catalyst Companies. Available from: http://www.catalystcompanies.co/graphic-a-timeline-of-corporations-in-the-collaborative-economy/. [Accessed 05 June 2021].

[10] Opinion of Advocate General Szpunar delivered on 11 May 2017 in C-434/15, paragraphs 58-59.

looking at the specific set up of the online platforms, those who are providing services or are collaborating with the online platform (for the purpose of this paper they will be called "workers" or "virtual workers") could be in an unclear situation. The question is do we consider them to be in a proper employer/employee relationship, or are these self-employed, independent contractors? And in addition, what criteria will help to distinguish if we are talking about dependent worker or independent contractor? And what should such criteria look like? Would it be possible to set up a definition of "dependent work" applicable for online platforms and say that such a definition should serve as grounds for an employment relationship within the online platform? And do virtual workers deserve a legal protection, ranging from a minimum wage and working time regulation to collective rights?

2.CROWD (VIRTUAL) WORK: RISKS AND ADVANTAGES

Crowd employment is an employment form that uses an online platform to enable organisations or individuals to access an indefinite and unknown group of other organisations or individuals to solve specific problems or to provide specific services or products in exchange for payment.[11] Also known as crowd sourcing[12], crowd work or virtual work, it is a new form of organising the outsourcing of tasks, and what would normally be delegated to a single employee, is now delegated to a large pool of "virtual employees".[13] It is based on individual tasks or projects rather than on a continuous employment relationship. A larger task is usually divided up into smaller subtasks that are independent, homogenous and produce a specific output. Stable workforces are being replaced by networked "crowds". New platforms for online work allow firms to connect with

[11] Green, A., de Hoyos, M., Barnes, S. (2013) *Exploratory research on Internet-enabled work exchanges and employability: Analysis and synthesis of qualitative evidence on crowdsourcing for work, funding and volunteers*. JRC Scientific and Policy Report. European Commission. p. 5. Available from: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC85646/jrc85646.pdf. [Accessed 04 May 2021].

[12] Crowdsourcing is also sometimes understood to include volunteer-based, non-paid work such as editing material for Wikipedia or involvement in an open-source innovation movement developing community-based software such as Linux (Wexler, 2011).

[13] Saxton, G., Oh, O., Kishore, R. (2013) Rules of Crowdsourcing: Models, Issues, and System of Control, *Information System Management*, p. 3. Available from: file:///C:/Users/S7FX6B/OneDrive%20-%20Swiss%20Reinsurance%20Company%20Ltd/TU/DIZER%20MATERIAL/Saxton_Rules%20of%20crowdsourcing.pdf. [Accessed 03 June 2021]. See also: Eurofound (2015) *New forms of employment*. Publications Office of the European Union. Available from: https://www.eurofound.europa.eu/sites/default/files/ef_publication/field_ef_document/ef1461en.pdf. [Accessed 03 June 2021].

enormous numbers of prospective labourers and to distribute tasks to an amorphous collection of individuals, all sitting in front of computer screens or their mobile phones.[14]

Unlike traditional employment, which involves a one-to-many relationship between employer and employees, crowd work is characterized by many-to-many connections, with some connections lasting as little as a minute or two.[15]

There are several questions when it comes to the virtual or crowd work; what constitutes an employment relationship in such an environment? Can a worker genuinely operate as an independent contractor? What responsibilities, if any, are attach to the companies that develop, promote, and run crowdsourcing platforms?[16]

To the first question, companies and workers select each other in a global or local open space for sourcing contract work. The online platforms challenge traditional business models and undermine the common structure of the "employer-employee" scheme.[17]

For the second questions, i.e., if a worker can actually operate as an independent contractor, it could be argued that the level of flexibility, which is usually given to the virtual workers, is more significant for independent contractors than for traditional employees. But could this freedom of choice be the main condition? As described by Todolí-Signes a self-employed worker is a person who works directly for the market, i.e., someone who offers his/her services to one or more companies without becoming part of them. Self-employed people are owners of their own organisation and have the independence needed to choose whether to accept the risk.[18] In many cases (or maybe in most of the cases) the virtual

[14] Felstiner, A. (2011) Working the Crowd: Employment and Labor Law in the Crowdsourcing Industry. *Berkeley Journal of Employment and Labor Law*, Vol. 32, No. 1, p. 145. Available from: https://ssrn.com/abstract=1593853. [Accessed 06 May 2021].

[15] *Ibidem.*

[16] Cherry, M. (2009) Working for (Virtually) Minimum Wage: Applying the Fair Labor Standards Act in Cyberspace. *Alabama Law Review*, Volume 60, N. 5. Available from: https://www.researchgate.net/publication/228136183_Working_for_Virtually_Minimum_Wage_Applying_the_Fair_Labor_Standards_Act_in_Cyberspace., [Accessed 13 April 2021] and Cherry, M. (2010) A Taxonomy of Virtual Work. *Georgia Law Review, Forthcoming*. Available online: https://ssrn.com/abstract=1649055. [Accessed 13 April 2021].

[17] Aloisi, A. (2016) Commoditized Workers. Case Study Research on Labor Law Issues Arising from a Set of "On-Demand/Gig/ Economy" Platforms. In *Comparative Labor Law & Policy Journal,* Vol. 37, No. 3., p. 655. Available from: https://ssrn.com/abstract=2637485. [Accessed 13 April 2021].

[18] Todolí-Signes, A. (2017) The "gig economy": employee, self-employed or the need for a special employment regulation? *European Review of Labour and Research,* p. 5. Available from: https://ssrn.com/abstract=2900483. [Accessed 11 May 2021].

workers will not be in a position to own the online platform they are working for or in a position to decide whether some risk will be accepted or not. Todolí-Signes argues that the new types of workers – working through an online platform, owning the tools and materials needed for the work, choosing when (schedule freedom), for how long (freedom of working hours) and whether to perform the work – would therefore seem to fit more into the self-employed category and less into a traditional employment relationship.[19]

The last question is related to the responsibility of the online platforms if in the position of the employer. While offering different services, the platform will accumulating large number of virtual workers, usually without giving specific instruction related to the working hours, but still having control over the working conditions and over the services provided (as Uber does). It is crucial to determinate whether staff of the online platform somehow remain within the organisational field of a company and under its control. In the US and the UK, where the first conflicts have arisen, the literature and judicial rulings (Employment Tribunals case Mr. Y Aslam vs Uber case No. 22025502/2015) argue that these new companies are misclassifying their workers as self-employed.[20] Interestingly, in this case the court ruled that the drivers are classified as "workers" and not as "employees".[21]

When it comes to the structure of such relationship, we are talking about the tripartite structure consisting of vendors, firms (or companies) and workers. Vendors develop a platform upon which firms can broadcast their tasks, and workers can accept, perform and/or submit the work. As a condition of access to the platform and providing of the services, workers and firms usually must assent to an agreement, usually written and designed by the vendor. These agreements often bind participants to other terms of use separate from those governing the platform, including privacy policies and conduct requirements. The vendor generally serves as an intermediary, the worker hands over the work done and the firm pays the worker. [22] Although a huge number of workers are usually involved

[19] *Ibidem.*

[20] *Ibidem.*

[21] Davidov, G. (2005) Who is a worker? *Industrial Law Journal 34(1).* p. 8. Available from: https://ssrn.com/abstract=783465. [Accessed 13 April 2021].

[22] Felstiner, A. (2011) Working the Crowd: Employment and Labor Law in the Crowdsourcing Industry. *Berkeley Journal of Employment and Labor Law.* Vol. 32, No. 1., p. 148. Available from: https://ssrn.com/abstract=1593853. [Accessed 06 May 2021].

in the services provided through online platforms, most of the online platforms will introduce certain types of terms of use (or other types of the agreements) to specify, that such virtual workers are in the position of the independent contractors[23]. Under such conditions workers explicitly agree to perform tasks in their personal capacity as an independent contractor and not as an employee.[24] However, in most cases (Uber as an example) the reality might be different. The workers need to agree with the terms if they would like to provide services on the online platform. An independent contractor will usually have the power to decide over the work or services he/she is providing, will have direct contact with the market and will offer the services without being a part of a company. However, drivers working for Uber must meet and comply with various requirements set out in the terms, i.e., drivers are not allowed to share accounts (personal performance is requested), must provide services at a specific location, and must present various types of documents (e.g. driving license, insurance certificate, etc.). The ownership of the tools needed to provide the service is significant for the independent contractor. The drivers providing transportation services are owners of the cars used for the services offered through Uber, but Uber has the right to decide the makes and models of vehicles that are accepted based on a published list. Again, to follow such rule is not typical for the independent contractor. Therefore, in our view it will be not possible to agree with the argument that the terms and conditions of use of the online platform will be in a position to determine whether a worker is in the position of an employee or should be considered an independent worker.

The virtual work or crowdsourced work is dependent on the online environment and it seems to be particularly prevalent in industries or sectors related to cyberspace, such as web content, social media, software development or online advertising.[25] Anyway, this may not always be the case, as Uber, for example, provides transport services that are usually typical for the "offline" world.

---

[23] Amazon.com, Amazon Mechanical Turk Participation Agreement § 3a–e, Available from: https://www.mturk.com/mturk/conditionsofuse. [Accessed 06 May 2021].

[24] *Ibidem.*

[25] Felistiner, A. (2011) Working the Crowd: Employment and Labor Law in the Crowdsourcing Industry. *Berkeley Journal of Employment and Labor Law,* Vol. 32, No. 1. p. 150. Available from: https://ssrn.com/abstract=1593853. [Accessed 06 May 2021].

What are the benefits (for the employer and for the online platforms) when we talk about virtual work? One could potentially be the ability to pick and choose from the "crowd", meaning that there are number of potential workers ready to perform the task according to the customer´s (or potentially the online platform´s) requirements, rather than hiring an employee. While using a freelancer instead of an employee, an online platform can benefit from the additional costs of creating a permanent position or meeting all the conditions under the employment law – virtual working can bring significant flexibility and lower costs. Further, virtual workers will be not able to claim additional benefits, paid leave, or guaranteed pay. On the other hand, the virtual employer does not need to worry about safe and secure workspace, people´s management or procurement of working equipment.

Felstiner also highlights that employers can enter and exit crowdsourcing venues at their whim, without any significant transaction costs or logistical hurdles. They can also use the constant availability of global labour pool to avoid the delays commonly associated with identifying and vetting outside contractors.[26]

When we talk about employment and the relationship between employee and employer, one of the terms describing such a relationship is one of dependency. Dependent employment can be defined as superiority of the employer and subordination of the employee, in the employee´s personal capacity, whereby the employee follows employer´s instruction and at time and in the manner as determined by the employer.

Poor quality of work can be a problem due to the specifics of virtual work – for example, an anonymous pool, unexpected results, lack of control or insufficient qualification constraints in defining tasks.[27]

From the worker´s perspective, working as a crowd worker could bring different opportunities; a worker could easily decide to start (and in turn quit) different types of tasks for different online platforms. With this in mind, the freedom of choice will be one of the main advantages of working as a crowd worker; freedom to decide when, for how long and what kind of tasks one chooses to perform. In terms of equipment, usually not much is needed – a headset, computer or phone and internet connection

[26] Felstiner, A. (2011) Working the Crowd: Employment and Labor Law in the Crowdsourcing Industry. In *Berkeley Journal of Employment and Labor Law,* Vol. 32, No. 1. p. 152. Available from: https://ssrn.com/abstract=1593853. [Accessed 06 May 2021].

[27] *Ibidem.*

can be quite sufficient. Of course, if we are talking about Uber as an example, there will be other requirements in scope – e.g., driving license and own car will be a must in this case.

Interesting findings were noted by Felstiner and Howe, with one of these findings being the benefits of crowdsourcing on personal productivity. Crowdsourcing[28] promises to turn our "spare cycles[29]" (periods when the brain is working but not producing anything of value – into productive time, instead of wasting time on social media, playing online games, or surfing the internet, AMT engages you in work tagging photos. Without such platforms, how would a person be able to monetize the stray ten-minute intervals that pop up throughout the day? A single employer would not hire and hourly employee for these time periods. But thanks to crowdsourcing, every waiting room and bus stop becomes a temporary workspace.[30]

Zittrain argued, that because working assignments can change from minute to minute, the workers do not develop any particular sense of belonging to an employer, and do not gain a sense of the larger enterprise for which they have been asked to take just one small step.[31] We agree with these arguments as we conclude that there is a relationship between employer and employee built on tasks and goals that are established by employer and fulfilled by the employee. In many cases, employees are proud to work for particular employer or feel part of the company, being involved in major projects or strategic decisions. Sometimes, even when individuals within the same team are located in different geographic locations with a clear goal, there can be a strong team spirit and a satisfied sense of the employee being part of a team. It is important for the well-

[28] One of the definitions of the Crowdsourcing (as defined by Hargrave) is that "*Crowdsourcing involves obtaining work, information, or options from a large group of people who submit their data via the Internet, social media, and smartphone apps. People involved in crowdsourcing sometimes work as paid freelancers, while other perform small tasks on a voluntary basis. For example, traffic apps encourage drivers to report accidents and other roadway incidents to provide real-time updated information to app users"*. See also Hargrave, M. (2019) *Crowdsourcing*. Available from: https://www.investopedia.com/terms/c/crowdsourcing.asp. [Accessed 07 May 2021].

[29] "Spare cycles" means unused or unclaimed human capacity. Originally unused computer capacity made available for collaborative projects. Available from: http://onlineslangdictionary.com/meaning-definition-of/spare-cycles.

[30] Felstiner, A. (2011) Working the Crowd: Employment and Labor Law in the Crowdsourcing Industry. In *Berkeley Journal of Employment and Labor Law*, Vol. 32, No. 1. p. 155. Available from: https://ssrn.com/abstract=159385. [Accessed 06 May 2021].

[31] Zittrain, J. (2008) Ubiquitous Human Computing, In *Legal Research Paper Series No. 32/2008*, Oxford: University of Oxford, p. 5. Available from: http://ssrn.com/abstract=1140445. [Accessed 08 May 2021].

being of employees that they are motivated, engaged and rewarded. Lack of these factors leads to high turnover and negative feelings. When delivering services through online platforms, virtual workers might not feel engaged because they are working on a few and quite specific issues. Working with a mass of people, who don´t know each other and have no real colleagues could make you feel like you don´t belong somewhere as an employee.

3. CAN UBER BE AN EMPLOYER?

While trying to answer the question how dependent work should be defined in the online world, we´ve chosen Uber as an example to help with such a definition.

Uber is the name of an electronic platform developed by Uber Technologies, with its principal place of business in San Francisco. In the EU Uber is managed by Uber BV, company governed by Netherlands law.

Uber allows the users to order the transport within the city. The app recognises the user´s location and finds available drivers who are nearby. When a driver accepts a ride, the application notifies the user and displays the driver´s profile along with and estimated price for the trip to the destination specified by the user. Once the trip is completed, the fare is automatically withdrawn from the bank card that the user must enter when registering with the app. The app also includes a rating feature that allows drivers to rate passengers and passengers to rate drivers. The transportation services offered by the Uber platform are divided into different categories depending on the quality of the drivers and the type of vehicle.[32] Uber represent a specific offline crowd sourcing work where Uber owns a virtual platform on which the user can get urban transportation.

Uber´s activities bring new challenges and questions. On the one hand, it brings the new activities and opportunities to travel within the city, on the other hand, it brings concerns in terms of labour law and unfair competition.

Uber´s operation is simple. Users download the Uber app for free. When user wants to use the transport service, they can use the app to find the closest driver. Uber does not employ drivers or own any vehicles – Uber

[32] Opinion of Advace General Szpunar delivered on 11 May 2017, C-434/15 Asociación Profesional Elite Taxi vs. Uber System Spain SL.

expects its participating drivers to own the vehicles. Depending on the city, drivers may be tested on their geographic knowledge of the city and may be interviewed by an Uber employee. A driver´s vehicle must be no more than 10 years old. The price of the service is not negotiable but is set by Uber. Tipping is prohibited and Uber takes 10 to 20 % of the price. The driver must pay all costs – taxes, insurance, petrol, vignette, etc. Further, drivers can refuse rides, but Uber expect the driver to accept all assignment.[33] It follows that, although drivers are given a great deal of freedom, Uber has considerable control over the terms and conditions of the services provided through Uber platform. It tells drivers what to do and how to provide the service. Such behaviour (i.e., setting the rules and control) is more characteristic for the employee-employer relationship.

Uber can deactivate the drivers account[34], which shows that Uber has control over the services it provides, as it is not possible to offer and provide the driving activities without an account.

If we look at the online platforms, can we say that they actually offer additional job markets and easy entry for service providers (such as drivers "working" for Uber)? Or, on the contrary, are large online platforms reducing job stability and undermining worker´s rights?

As Pasquale argues[35] the "peer economy" of platform-ordered production will break down old hierarchies. Gig workers will be able to knit Etsy scarves in the morning, drive Uber cars in the afternoon, and write Facebook comments at nights, flexibly moving between work and leisure at will.

One digital job placement platform, Amazon´s Mechanical Turk (MTurk)[36], allowed buyers of "human intelligence tasks" to pay next to nothing for the work – resulting in effective remuneration well below the minimum wages.[37]

---

[33] Todolí-Signes, A. (2017) The "gig economy": employee, self-employed or the need for a special employment regulation? *European Review of Labour and Research*, p. 3. Available from: https://ssrn.com/abstract=2900483. [Accessed 06 May 2021].

[34] Huet, E. (2014) *Uber Deactivated A Driver For Tweeting A Negative Story About Uber*, Forbes, Available from: http://www.forbes.com/sites/ellenhuet/2014/10/16/uber-driver-deactivated-over-tweet/#545e7b8a36c8. [Accessed 06 May 2021]. See also Uber. (2020) *Uber Terms and Conditions.* Available from: www.uber.com/legal/usa/ terms. [Accessed 06 May 2021].

[35] Pasquale, F. (2016) Two Narratives of Platform Capitalism. *35 Yale Law & Policy Review 309*. University of Maryland, Francis King Carey School of Law, p. 313. Available from: Two Narratives of Platform Capitalism by Frank A. Pasquale :: SSRN. [Accessed 08 May 2021].

[36] Amazon Mechanical Turk. Available from: https://perma.cc/FFU8-7VAR. [Accessed 08 May 2021].

Crawford[36] places similar emphasis on new digital platforms as it does on large telecommunication firms failing to meet their social obligations as utilities. Crawford fears that Uber will quickly monopolize urban transport services while avoiding regulation and taxes. While it may offer a good term to many drivers and passengers now, there is no guarantee that it will continue to do so in the future. Crawford goes on to argue that when it comes to the urban transport and communication networks, it is more important to serve everyone fairly at a high level – including drivers – than to allow one company to make huge profits from a substitute basic private service.[38]

4. COURT DECISIONS

Recently, the Swiss court upheld Uber´s status as employer when the court in the canton Vaud upheld a previous ruling that a former Uber driver was an employee of the ridesharing company, not an independent contractor, and that the man had lost his job unfairly. In a verdict published in October 2020, the judges of the cantonal Court of Appeal said the man had been dismissed "unjustly" and that he should have the same right as a taxi driver who has a contract with a cab company. The driver worked for a subsidiary of Uber, and his account was deactivated in late 2016 due to complaints against him as a driver, prompting him to take legal action.[39]

According to the driver´s lawyer, this is the first time in Switzerland that a cantonal court, ruling as an appellate authority, has ruled that the Uber Group must behave like an employer.[40]

This decision follows a June court ruling in neighbouring canton Geneva, when judges ruled that the food delivery service Uber Eats is an employer and has a duty to employ its drivers, classifying Uber Eats as a staffing agency. Like Uber offering transportation services, Uber Eats employees can choose when to work and are paid a delivery wage.[41] Uber

---

[37] Pasquale, F. (2016) Two Narratives of Platform Capitalism. In *35 Yale Law & Policy Review 309*. University of Maryland, Francis King Carey School of Law, p. 313. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3002529. [Accessed 06 May 2021].

[38] Crawford, S. (2015) *Getting over Uber*, Backchannel. Available online: https://perma.cc/VV7A-KZYA. [Accessed 22 December 2020].

[39] *SWI Workplace Switzerland*. (2020) Swiss court confirms Uber status as "employer". 16 September 2020. Available from: https://www.swissinfo.ch/eng/business/swiss-court-confirms-uber-status-as--employer-/46036976. [Accessed 13 May 2021].

[40] *Ibidem.*

[41] *SWI Workplace Switzerland*. (2020) Uber Eats suffers setback in Geneva court ruling. 11 June 2020, Available online: https://www.swissinfo.ch/eng/business/legal-responsibilities_uber-eats-suffers-setback-in-geneva-court-ruling/45828814. [Accessed 13 May 2021].

Eats, on the other hand, claims that it does not consider itself an employer, as couriers are completely free to decide when, how often and for how long to use Uber Eats app, and whether they want to perform other activities.[42]

Similar cases have been referred the European Court of Justice. In one of them (Uber Spain C-434/15) the question was raised whether Uber´s activities violated the law and could be considered as "unfair practice". As regards the regulatory acts (following questions referred to the ECJ concerning the qualification of the services provided by Uber) that could potentially apply to Uber´s services, the court was considering if the Directive 2000/31/ES and Directive 2006/123/ES could apply in this case.[43]

However, as far as the status of the drivers is concerned, in Uber´s view, they are seen more as independent contractors who own their own car to provide the transport services, as Uber likes to claim. Or is it Uber´s employees who are entitled to benefits, overtime pay and collective bargaining?[44]

In its contract, Uber defines drivers as "partners", not employees. Uber claims to provide "business opportunities" to drivers and refers to itself as a "technology company" or a "platform", not a transportation company.[45] Uber views its business as a "service" (referring to the Directive 2015/1535) i.e., any Information Society service, provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of service.

In Uber Spain C-434/15 the Court address the question whether Uber should be considered as an intermediary or rather a provider of transport services. Although Uber is an online platform, the actual service it offers to customers is a transport service. The main conclusion is that Uber is a transport service (like a taxi service) and not just an online platform that offers the possibility to find, book and pay for the transport service. Uber controls the essential parts of the transport service; it connects non-

[42] *SWI Workplace Switzerland*. (2020) Uber Eats suffers setback in Geneva court ruling. 11 June 2020, Available online: https://www.swissinfo.ch/eng/business/legal-responsibilities_uber-eats-suffers-setback-in-geneva-court-ruling/45828814. [Accessed 13 May 2021].

[43] Križan, V. (2017) Uber v rozhodovacej činnosti orgánov aplikácie práva. *Pracovné právo v digitálnej dobe*. Praha: Leges, p. 114.

[44] *Forbes*. (2017) Are Uber Drivers Employees? The Answer Will Shape The Sharing Economy. 15 November 2017. Available from: https://www.forbes.com/sites/omribenshahar/2017/11/15/are-uber-drivers-employees-the-answer-will-shape-the-sharing-economy/#39cedc815e55. [13 May 2021].

[45] *Ibidem.*

-professional drivers with passengers, sets the rules applicable to drivers and passengers, limits on the types of vehicles used for the transport service etc. [46]

To provide transportation services through the Uber app, the driver must have a vehicle suitable for the services and meet the conditions required by Uber (vehicle age or recommended colour).

Uber does not set fixed working hours. On the other hand, Uber provides financial rewards to those who have a high number of city trips and informs drivers of times and locations where drivers can count on a higher number of city trips and/or preferential fares.[47]

As mentioned earlier, the Uber app includes a rating feature, that allows drivers to rate passengers and vice versa. Uber thus exercises control, albeit indirect, over the quality of the services provided by drivers. In addition, Uber sets the price of the service provided. Although Uber´s representatives have argued that drivers are in principle free to ask for a lower price than that quoted by the app, such an option does not appear to be feasible.[48]

Uber thus exercises control over all relevant aspects of an urban transport service: over the price, but also over the minimum safety conditions through up-front requirements for drivers and vehicles, over the availability of transport, over the offer to encourage drivers to work when and where demand is high, over the behaviour of drivers through a ratings system and, finaly, over possible exclusion from the platform.[49]

Indirect management such as that practiced by Uber, based on financial incentives, and decentralised evaluation by drivers with economic scale, allows for management that is as effective, if not more effective, than management based on formal orders issued by the employer to its employees and on direct control of compliance with those order.[50]

Uber´s core business involves the single provision of transport in a vehicle that is located and booked through smartphone app and that this service is provided (the classification of the relationship between Uber and its drivers being a matter of national law), by Uber or on its behalf.

---

[46] Barancová, H. (2017). *Nové technológie v pracovnoprávnych vzťahoch.* Praha: Leges, p. 29.

[47] Barancová, H. (2017). *Nové technológie v pracovnoprávnych vzťahoch*. Praha: Leges, p. 30.

[48] Opinion of Advocate General Szpunar delivered on 11 May 2017 in C-434/15. paragraphs 49-50.

[49] Opinion of Advocate General Szpunar delivered on 11 May 2017 in C-434/15. paragraph 51.

[50] Opinion of Advocate General Szpunar delivered on 11 May 2017 in C-434/15. Paragraphs 53-54.

The quality of the transport shall be ensured by Uber. However, such a finding does not necessarily mean that Uber´s drivers are to be regarded as Uber´s employees, as the company may provide its services through independent traders acting on its behalf as subcontractors.[51]

Taking all the already mentioned points into account, Uber is not just an intermediary between drivers and passengers. On the contrary, Uber is a true organiser and operator of urban transport services. Within this service, Uber drivers can only find passengers through the Uber app, and the app only allows you to find drivers working on the platform. One service is therefore inseparable from the other and together they form one service.[52]

Based on the abovementioned ruling of the Case C-434/15 we believe that Uber should be considered an employer as it has overall control over the transportation services offered through Uber app.

As regards the status quo of drivers, these issues have been raised in United States of America, in Great Britain and Northern Ireland.

The London Employment Tribunal ruling in relation to Uber concerns drivers working for the Uber taxi platform. The Employment Tribunal ruled that the drivers are entitled to the most basic worker´s rights, including the right to the national minimum wage and paid holiday, which were previously denied to them.[53] This ground-breaking decision will affect not only thousands of Uber drivers working in this country, but also all workers in the so-called gig economy who are misclassified by their employers as self-employed and denied the rights to which they are entitled.[54]

In another legal case, in June 2015, the Labour Inspectorate of Catalonia ruled that Uber´s drivers were employees. The Inspectorate gave several reasons for this, including:

The company provided drivers with smartphones so that they could carry out their professional activity.

An "incentives system" offered by Uber was based on drivers´ productivity.

---

[51] OOpinion of Advocate General Szpunar delivered on 11 May 2017 in C-434/15. paragraph 52.

[52] Opinion of Advocate General Szpunar delivered on 11 May 2017 in C-434/15. paragraph 63.

[53] This decision of the Employment Tribunal was later affirmed by the Court of Appeal, as we will show later.

[54] Labour Market Notes. (2017) *Irish Congress of Trade Unions*. Issue 7, Spring 2017. Available from: https://www.ictu.ie/download/pdf/lmn_issue_7.pdf. [Accessed 13 May 2021].

It gave assurances to drivers that it would intervene if they experience any issues with courts or police.[55]

Returning to the UK legal case[56] – *Employment Tribunals case Mr. Y. Aslam vs Uber, No. 2202550/2015*, the tribunal argued that there is no prohibition on "inactive" drivers, i.e., the drivers are under no obligation to turn on the Uber app. However, if the app is turned on, the court concluded that any driver who (a) has the application turned on, (b) is in the territory in which he or she is authorised to work, and (c) is able and willing to accept assignments, so long as those conditions are met, is working for Uber under a "worker" contract. As the decision further notes, in promotional materials and correspondence, individuals speaking on behalf of Uber frequently used language that included terms like "Uber drivers" or "our drivers".[57]

The UK Supreme Court recently dismissed an appeal by Uber BV following an earlier Employment Tribunal decision. The Court again addressed an issue relating to the legal status of the drivers, i.e. whether they should be considered as workers (entitled to the special rights) or rather as self-employed.

As stated in the UK Supreme Court decision, there are three employment categories under UK law: employees who are guaranteed employment rights and benefits, workers, who enjoy some of these rights, and the self-employed workers who have very little protection. The Supreme Court has moved the Uber´s drivers from self-employed to the second category.[58]

In comparison with the Slovak legal acts[59], we can only speak of two categories: employees with the guaranteed rights and self-employed persons.

The "transfer" of drivers into the category of workers (in UK), or the introduction such a category in other countries (e.g. Slovakia) will

[55] Labour Market Notes. (2017) *Irish Congress of Trade Unions*. Issue 7, Spring 2017. Available online: https://www.ictu.ie/download/pdf/lmn_issue_7.pdf. [Accessed 13 May 2021].

[56] Mr. Y. Aslam vs Uber (2015) No. 2202550/2015, Available from: https://www.judiciary.uk/wp-content/uploads/2016/10/aslam-and-farrar-v-uber-reasons-20161028.pdf. [Accessed 13 May 2021].

[57] *Ibidem.*

[58] Naughton, J. (2021) Uber´s UK supreme court defeat should mean big changes to the gig economy. *The Guardian.* 27 February 2021. Available from: https://www.theguardian.com/commentisfree/2021/feb/27/ubers-uk-supreme-court-defeat-should-mean-big-changes-to-the-gig-economy. [Accessed 13 May 2021].

[59] Act No. 311/2001 Slovak Labour Law Coll. (Zákonník práce) Articles 11 – 14, and Act No. 455/1991 Coll. On small business activity (Trade Licensing Act) (Živnostenský zákon).

certainly have an impact on Uber´s future business; possibly Uber will try to compensate for higher cost with the higher prices.

In the meantime, Uber has decided to introduce "Proposition 22" in California; Uber paid $200 million to successfully support Proposition 22[60], a measure that allows it to continue classify its drivers as "independent contractor" rather than "employees" with mandatory benefits.

As Uber has stated, it is difficult to both offer flexible work opportunities and provide benefits as "regular" employer. Based on a recent UK Supreme Court decision, it appears that, in the UK at least, this question has been answered[61].

The principal issue on appeal to the UK Supreme Court is whether an Employment Tribunal was entitled to find that drivers whose work is brokered through Uber smartphone app are working for Uber under worker´s contract and are therefore entitled to the national minimum wage, paid annual leave and other employee rights or whether, as Uber contends, the drivers do not have those rights because they work for themselves as independent contractors who perform services under the contracts with passengers through Uber as their booking agent.[62]

Where drivers work for Uber under an employment contract, a further question arises as to whether the Employment Tribunal was entitled to find that the drivers who brought these claims were working under such contracts whenever they were logged into the Uber app in the territory in which they were licensed to operate and were prepared to accept journeys, or whether, as Uber contends, they were only working when they were taking passengers to their destinations.[63] The UK Supreme Court upheld the conclusion of the Employment Appeal Tribunal and the majority of the Court of Appeal that the Employment Tribunal was entitled to decide both issues in favour of the claimants.

As described earlier in this article, Uber´s service delivery model is simple; potential customers download the Uber app, create an account, and

---

[60] Wikipedia. (2020) *California Proposition 22.* 3 November 2020. Available online: https://en.wikipedia.org/wiki/2020_California_Proposition_22. [Accessed 13 May 2021].

[61] Naughton, J. (2021) Uber´s UK supreme court defeat should mean big changes to the gig economy. *The Guardian.* 27 February 2021. p. 4. Available from: https://www.theguardian.com/commentisfree/2021/feb/27/ubers-uk-supreme-court-defeat-should-mean-big-changes-to-the-gig-economy. [Accessed 13 May 2021].

[62] Uber BV and others v. Aslam and others (2018). No. EWCA Civ 2748, paragraph 1. Available from: https://www.supremecourt.uk/cases/uksc-2019-0029.html. [Accessed 13 May 2021].

[63] *Ibidem.*

add their credit card payment details. When they request a ride, the Uber app identifies the passenger´s location and pair them with the nearest driver.

At this stage, the driver learns the passenger´s name and Uber´s rating and has to decide whether to accept the request. When the driver accepts the request, the ride is assigned and the booking is confirmed to the passenger.[64]

It is important to note (and it was also highlighted in the European Court of Justice decision C-434/15), that the Uber app is the only communication channel used by the driver and the passenger to arrange the journey. We consider that Uber (and Uber app) plays an essential role in the transport services provided by the drivers through such application.

The payment is made by withdrawing funds from passenger´s credit or debit card registered in the Uber app. Drivers can accept payment in a lower but not a higher amount calculated by the app. Further, drivers may accept tips, but Uber does not recommend asking them.[65]

Such a condition for the provision of transport services demonstrates Uber´s control over the transport provided, as well as the power to decide on the price of the services.

Uber pays the driver on a weekly basis the amounts paid by passengers for rides taken by the driver, less a "service fee" retained by Uber.[66]

To become an Uber driver, you need to follow certain procedure; you need to provide documents such as a driver´s license, insurance certificate, logbook etc. In addition, the applicant must attend an interview, which the Employment Tribunal described as "an interview, albeit not a search interview" and watch a video presentation about the Uber app and a procedure.[67] Such a procedure could easily remind us of a job interview when an applicant is applying for a job.

In terms of working conditions, drivers who choose to provide transport services sign up the Uber app; needless to say, signing up to the app is

---

[64] Uber BV and others v. Aslam and others (2018). No. EWCA Civ 2748, paragraph 6 Available from: https://www.supremecourt.uk/cases/uksc-2019-0029.html. [Accessed 13 May 2021].

[65] Uber BV and others v. Aslam and others (2018). No. EWCA Civ 2748, paragraph 9. Available from: https://www.supremecourt.uk/cases/uksc-2019-0029.html. [Accessed 13 May 2021].

[66] *Ibidem.*

[67] Uber BV and others v. Aslam and others (2018). No. EWCA Civ 2748, paragraph 14. Available from: https://www.supremecourt.uk/cases/uksc-2019-0029.html. [Accessed 13 May 2021].

essential to provide the service. Access to the app is free for the drivers, but they must have a smartphone or rent one from Uber for a small fee. Drivers pay for their own vehicles (including fuel, insurance, and road tax), while such vehicles must be no older than a certain age and preferably silver or black.[68]

Although such an arrangement is not typical for the employee-employer relationship (where the employer is usually obliged to provide all the equipment necessary for the employee´s work), it does not prove that the ride should be considered as an independent service provided; we believe that an independent service provider will have much more discretion as to the selection of the vehicle, including the type and colour.

As mentioned by the Employment Tribunal[69], there are many given standards of performance which drivers are expected to fulfil. Uber´s "Welcome Packet" contains a numerous of guidelines for new drivers, such as courteous conversation, professional behaviour, etc.[70]

In addition, drivers whose acceptance rate for ride requests falls below a certain level – 80% according to evidence before tribunal – receive warning messages reminding them that signing up to the Uber app is an indication that the driver is willing and able to accept ride requests. If the number of requests accepted does not improve, the warnings escalate, culminating in the driver being automatically logged out of the Uber app for ten minutes if the driver refuses three trips in a row. Further, the driver ratings from passengers are also monitored, and the employment tribunal found that drivers who have made 200 or more trips and whose average rating is below 4.4 are subject to a graduated series of "quality interventions" designated to help them improve. If their rating does not improve to an average of 4.4 or better, they are "removed from the platform" and their accounts are "deactivated".[71]

---

[68] Uber BV and others v. Aslam and others (2018). No. EWCA Civ 2748, paragraph 15. Available from: https://www.supremecourt.uk/cases/uksc-2019-0029.html. [Accessed 13 May 2021].

[69] Mr. Y. Aslam vs Uber (2015). No. 2202550/2015, Available from: https://www.judiciary.uk/wp-content/uploads/2016/10/aslam-and-farrar-v-uber-reasons-20161028.pdf. [Accessed 13 May 2021].

[70] For example, the "Welcome Packet" under heading "What Uber looks for" stated: High Acceptance Rate: *"Going on duty means you are willing and able to accept trip requests. Rejecting too many requests leads to rider confusion about availability. You should be off duty if no table to take requests."*

[71] Uber BV and others v. Aslam and others (2018). No. EWCA Civ 2748, paragraph 18. Available from: https://www.supremecourt.uk/cases/uksc-2019-0029.html. [Accessed 13 May 2021].

Such activities do not demonstrate Uber´s position as an "independent platform acting as an intermediary"; we believe it demonstrates Uber´s control and the power to make decisions about the activities of drivers in urban transport.

In addition, we need to consider the contractual relationships between Uber, drivers, and customers. Before drivers begin providing transportation services, they must sign a "partner registration form" stating that they agree to be bound by and abide by the terms and conditions described as "Partner Terms" (date 1 July 2013). Later (in October 2015), a new "Service Agreement" was introduced to which drivers had to electronically agree before they could again log into the Uber app and accept trip requests.[72]

This Service Agreement is formulated as a legal agreement between Uber and "an independent company in the business of providing transportation services", referred to as "Customer". Later on, it is expected, that "Customer" will enter into a contract with each driver in the form of an accompanying "Driver Addendum". Such a condition will be inappropriate for most drivers operating as private individuals.[73]

There is an additional relationship between Uber and passengers (the "Rider Terms") that passengers must accept in order to use the Uber app. Under the Rider Terms, Uber claims to act only as an intermediary between passengers and drivers (it calls them "Transportation Provider").[74]

Depending on the jurisdiction, employees´ rights are regulated in different laws; for example, in Slovakia, the Labour Law Act includes basic rights relating to payment of the basic wages, health and safety at work, the right to rest as well as the right to fair working conditions.

In Uber, the claimants sought the following rights: rights under the National Minimum Wage Act 1998 and related regulations to be paid at least the minimum wage for work performed; right under the Working Time Regulation 1998, which include the right to paid annual leave; and in the case of two claimants, one of whom is Mr Aslam, the right under

---

[72] *Ibidem.*

[73] Uber BV and others v. Aslam and others (2018). No. EWCA Civ 2748, paragraph 23. Available from: https://www.supremecourt.uk/cases/uksc-2019-0029.html. [Accessed 13 May 2021].

[74] Uber BV and others v. Aslam and others (2018). No. EWCA Civ 2748, paragraph 27. Available from: https://www.supremecourt.uk/cases/uksc-2019-0029.html. [Accessed 13 May 2021].

the Employment Rights Act 1996 not to be treated unfavourably on the basis that they had made a protected disclosure ("whistleblowing").[75]

When considering the rights of the Ubers drivers (or any other virtual workers providing their work through an online platform), one of the questions was about the status of "worker", i.e., who should be considered a worker.

The term "worker" is defined in section 230(3) of the Employment Rights Act 1996.[76] In a previous case (decided by the Employment Tribunal), it was held that the claimants (Uber drivers) were workers, although not employed under a contract of employment, but working for Uber London under a "workers´ contract" within the meaning of paragraph (b) of the statutory definition[77]. The Tribunal further decided that for the purposes of the relevant legislation, the claimants were working for Uber London during any period when a claimant (a) had the Uber app switched on, (b) was in the territory in which he was authorised to work, and (c) was able and willing to accept assignments.

Subparagraph (b)[78] of the statutory definition of a "worker´s contract" has three elements: (1) a contract by which an individual agrees to perform work or render services for the other party; (2) a commitment to perform or render the services personally; and (3) a requirement that the other party to the contract not be a client or customer of any occupation or business enterprise carried on by the individual.[79]

The crucial question is whether the drivers are to be regarded as working under contracts with Uber London under which they undertook

---

[75] Uber BV and others v. Aslam and others (2018). No. EWCA Civ 2748, paragraph 71. Available from: https://www.supremecourt.uk/cases/uksc-2019-0029.html. [Accessed 13 May 2021].

[76] Worker under Employment Rights Act 1996 is defined as: "*an individual who has entered into or works under (or, where the employment has ceased, worked under); a) a contract of employment, or b) any other contract, whether express or implied and (if it is express) whether oral or in writing, whereby the individual undertakes to do or perform personally any work or services for another party to the contract whose status is not by virtue of the contract that of a client or customer of any profession or business undertaking carried on by the individual; and any reference to a worker´s contract shall be construed accordingly.*"

[77] Uber BV and others v. Aslam and others (2018). No. EWCA Civ 2748, paragraph 112. Available from: https://www.supremecourt.uk/cases/uksc-2019-0029.html. [Accessed 13 May 2021].

[78] Uber BV and others v. Aslam and others (2018). No. EWCA Civ 2748, paragraph 41. Available from: https://www.supremecourt.uk/cases/uksc-2019-0029.html. [Accessed 13 May 2021].

[79] Uber BV and others v. Aslam and others (2018). No. EWCA Civ 2748, paragraph 41. Available from: https://www.supremecourt.uk/cases/uksc-2019-0029.html. [Accessed 13 May 2021].

to perform services for Uber London; or whether, as Uber submits, they are to be regarded as providing services solely for and on the basis of contracts entered into with passengers through Uber London.[80]

Following the decision of Employment Tribunal and UK Supreme Court, this question seems to have been answered, at least as far as the UK is concerned. Although the UK Supreme Court did not "classify" the Uber drivers as employees, it did move them into the category of workers with certain guaranteed rights. The UK Supreme Court also nicely described the subordination and dependency of drivers on Uber (particularly in relation to pricing, non-negotiable contracts, penalties for cancelled ride requests, control over how drivers provide their services, limited communication between passenger and driver etc.). On these facts, UK Supreme Court seen that the transport services performed by drivers and offered to passengers through the Uber app is very narrowly defined and controlled by Uber.[81]

Uber provides its activities in many jurisdictions. It will be interesting to see whether (and how) the UK Supreme Court decision will change Uber ´s business in UK and potentially in EU (it is worth mentioning that Uber is already attempting a Proposition 22 approach in Brussels[82] where it has published a white paper[83] explaining the importance of flexible working opportunities for 600 000 European workers).

5. CONCLUSION

Based on the recent legal actions and rulings of various courts (European Court of Justice and UK Supreme Court) we have concluded that there is a discrepancy between the legal terms as presented by Uber and the reality of the provision of its services. Uber claims that it is the free will of drivers to accept or refuse a customer´s request for a ride. Uber therefore consider itself to be only an intermediary in this process. On the other hand, Uber

[80] Uber BV and others v. Aslam and others (2018). No. EWCA Civ 2748, paragraph 71. Available from: https://www.supremecourt.uk/cases/uksc-2019-0029.html. [Accessed 13 May 2021].

[81] Uber BV and others v. Aslam and others (2018). No. EWCA Civ 2748, paragraph 75. Available from: https://www.supremecourt.uk/cases/uksc-2019-0029.html. [Accessed 13 May 2021].

[82] Lomas, N. (2021) Uber lobbies for "Prop 22" – style gig work standards in the EU. Available from: Uber lobbies for 'Prop 22'-style gig work standards in the EU | TechCrunch. [Accessed 13 May 2021] .

[83] Uber: "A better deal: partnering to improve platform work for all", Available from: https://www.uber.com/global/en/about/reports/a-better-deal/.

punishes drivers who refuse a request for a ride and, moreover, the driver is not really free to decide the route he/she would like to take, while Uber has control over it (including the knowledge of the customer´s identification data without sharing it with the driver). Following this argument (and the decisions of various courts) we do not see Uber as a neutral provider of the underlying platform, but rather as someone who has influence when it comes to the transport services.

As stated above, dependent work can be defined as employer´s superiority over and the employee´s subordination to the employee, in the employee´s personal capacity, while following the employer´s instruction, on behalf of the employer and at times and in manner determined by the employer. If Uber drivers rely on the ratings in the platform, their relationship will be closer to employer-employee than to independent contractor relationship.

In addition, Uber also acts as an employer in deciding who (as a driver) can provide services to customers. Applicants are interviewed, drivers have to comply with various rules (e.g. only drive certain types of vehicles "approved" by Uber), meet and comply with Uber´s requirements regarding the transport service itself, etc. Again, such activities are more reminiscent of an employer-employee relationship than of a neutral information society service provider offering an online platform for the transport services. Taking into account the (possible) employer-employee relationship, this is also reflected in the fact that Uber assumes the liability for damage in the event of fraud or vehicle pollution, which (assuming the drivers act as independent service providers) will be borne by the drivers.[84]

Uber also has the upper hand in negotiating the price of a ride; the driver does not have the right to negotiate potentially higher price based on the agreement with the customer. Furthermore, as far as discounts are concerned, these are also fully within Uber´s control.[85] Such activities, or rather, such a relationship is quite similar to dependent work, which is one of the main principles applicable in the employment law and in the relationship between employee and employer. Uber assesses drivers in deciding their remuneration in similar way to an employer (based on the assessment, the driver may be penalised to a certain extent). Our

[84] Križan, V. (2017) Uber v rozhodovacej činnosti orgánov aplikácie práva. In *Pracovné právo v digitálnej dobe*. Praha: Leges, p. 125.

[85] *Ibidem.*

view of the relationship between Uber and the drivers is that such relationship can be described as *sham contract* rather than the way Uber describes it (i.e., that drivers are independent contractors).

Based on all of these arguments, we conclude that there is a room for consideration regarding Uber´s status as an employer and that the drivers have a sham contract with Uber. Another topic for discussion is whether a similar conclusion may apply to different online platforms offering a different type of service. We can try to list some of the conditions applicable for online platforms to be considered an employer: control, financial incentive, and time management. On the other hand, it is clear that even if these conditions will be considered as prerequisite for defining the dependent work, there is still room for further specification of the individual condition.

LIST OF REFERENCES

[1] Aloisi, A. (2016) Commoditized Workers. Case Study Research on Labor Law Issues Arising from a Set of "On-Demand/Gig/ Economy" Platforms. In *Comparative Labor Law & Policy Journal,* Vol. 37, No. 3. Available from: https://ssrn.com/abstract=2637485. [Accessed 13 April 2021].

[2] Barancová, H. (2017). *Nové technológie v pracovnoprávnych vzťahoch.* Praha: Leges.

[3] Crawford, S. (2015) *Getting over Uber*, Backchannel. Available online: https://perma.cc/VV7A-KZYA. [Accessed 22 December 2020].

[4] Davidov, G.: Who is a worker? *Industrial Law Journal 34(1).* 2005. Available from: https://ssrn.com/abstract=783465. [Accessed 13 April 2021].

[5] European Commission (2016) *Online Platforms and the Digital Single Market Opportunities and Challenges for Europe*. COM/2016/0288 final, [online]. Available from: EUR-Lex - 52016DC0288 - EN - EUR-Lex (europa.eu). [Accessed 14 May 2021].

[6] Felstiner, A. (2011) Working the Crowd: Employment and Labor Law in the Crowdsourcing Industry. *Berkeley Journal of Employment and Labor Law,* Vol. 32, No. 1. Available from: https://ssrn.com/abstract=1593853 [Access on 18 June 2021].

[7] Green, A., de Hoyos, M., Barnes, S. (2013) *Exploratory research on Internet-enabled work exchanges and employability: Analysis and synthesis of qualitative evidence on crowdsourcing for work, funding and volunteers*, Luxembourg: Publications Office of the European Union. Available from: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC85646/jrc85646.pdf. [Accessed 04 May 2021].

[8] Howe, J. (2016) *Crowdsourcing: A Definition, CROWDSOURCING.* [online]. Available from: http://www.crowdsourcing.com/cs/2006/06/crowdsourcing_a.html [Access on 16 June 2021].

[9] Huet, E. (2014) *Uber Deactivated A Driver For Tweeting A Negative Story About Uber*, Forbes, Available from: http://www.forbes.com/sites/ellenhuet/2014/10/16/uber-driver-deactivated-over-tweet/#545e7b8a36c8. [Accessed 06 May 2021].

[10] Cherry, M. (2009) Working for (Virtually) Minimum Wage: Applying the Fair Labor Standards Act in Cyberspace. *Alabama Law Review*, Volume 60, N. 5. Available from: (PDF) Working for (Virtually) Minimum Wage: Applying the Fair Labor Standards Act in Cyberspace (researchgate.net) [Access 17 May 2021].

[11] Križan, V. (2017) Uber v rozhodovacej činnosti orgánov aplikácie práva. *Pracovné právo v digitálnej dobe*. Praha: Leges.

[12] Lomas, N. (2021) *Uber lobbies for "Prop 22" – style gig work standards in the EU*. Available from: Uber lobbies for 'Prop 22'-style gig work standards in the EU | TechCrunch. [Accessed 13 May 2021].

[13] Naughton, J. (2021) Uber´s UK supreme court defeat should mean big changes to the gig economy. *The Guardian.* 27 February 2021. Available from: https://www.theguardian.com/commentisfree/2021/feb/27/ubers-uk-supreme-court-defeat-should-mean-big-changes-to-the-gig-economy. [Accessed 13 May 2021].

[14] Pasquale, F. (2016) Two Narratives of Platform Capitalism. *35 Yale Law & Policy Review 309.* University of Maryland, Francis King Carey School of Law. Available from: Two Narratives of Platform Capitalism by Frank A. Pasquale :: SSRN. [Accessed 08 May 2021].

[15] Saxton, G., Oh, O., Kishore, R. (2013) Rules of Crowdsourcing: Models, Issues, and System of Control, In *Information System Management.* Available from: file:///C:/Users/S7FX6B/OneDrive%20-%20Swiss%20Reinsurance%20Company%20Ltd/TU/DIZER%20MATERIAL/Saxton_Rules%20of%20crowdsourcing.pdf. See also: New forms of employment. *Eurofound*. Available from: https://www.eurofound.europa.eu/sites/default/files/ef_publication/field_ef_document/ef1461en.pdf. [Accessed 03 June 2021].

[16] Todolí-Signes, A. (2017) The "gig economy": employee, self-employed or the need for a special employment regulation? *European Review of Labour and Research.* Available from: https://ssrn.com/abstract=2900483. [Accessed 11 May 2021].

[17] Zittrain, J. (2008) Ubiquitous Human Computing, In *Legal Research Paper Series No. 32/2008*, Oxford: University of Oxford. Available from: http://ssrn.com/abstract=1140445. [Accessed 08 May 2021].

DOI 10.5817/MUJLT2021-2-4

EXPLORING THE RELATION BETWEEN THE INDEGREE CENTRALITY AND AUTHORITY SCORE OF A DECISION AND THE REASON FOR WHICH IT WAS CITED: A CASE STUDY[1]

by

TEREZIE SMEJKALOVÁ[*], TEREZA NOVOTNÁ[**]

Some of the recent network citation analyses conducted in continental legal settings have suggested that the most cited decisions tend to be related to procedural issues, or issues of a more general nature. Such decisions are by nature capable of being referred to in a more varied situations, therefore scoring high in indegree centrality or authority score.

While it may seem intuitive that decisions with the highest indegree centrality or authority score would settle issues of a more general nature, hence making them more widely applicable to various kinds of subsequent cases, we were wondering, whether this trend would be noticeable in less exposed decisions. To this end, we have conducted a case study within the boundaries of the Czech legal system. We have chosen five decisions containing a chosen keyword based on their indegree centrality in a corpus of Czech apex courts' decisions. Subsequently, we have constructed eleven chains of decisions (connected to one another by a citation) leading to these five decisions, again paying attention to their indegree. We theorize that the decisions with higher indegree centrality as well as decisions with higher authority score will be cited in situations seeking a case-law argument for either procedural issue, or an issue of a more general nature, or an issue of principle, while the decisions with low indegree centrality or low authority score will be cited

[1] This paper is a part of a project titled "Judikatura, nebo precedens: Podobnost citovaných rozhodnutí při citacích judikatury" (Project No. MUNI/A/0952/2019).

[*] terezie.smejkalova@law.muni.cz, Department of Legal Theory, Faculy of Law, Masaryk University, Brno, Czech Republic.

[**] tereza.novotna@law.muni.cz, Institute of Law and Technology, Faculty of Law, Masaryk University, Brno, Czech Republic.

for their substantive law merit. This paper seeks to demonstrate how the network analysis in combination with a qualitative approach may serve as a useful method in further exploring this hypothesis.

We show that the actual citation environment in Czech legal setting might be more complex than this hypothesis suggests and that this methodological approach may be further useful in exploring the normative nature of judicial decisions in non-precedential legal settings.

KEY WORDS

Judicial Decision, Centrality Network Analysis, Citation Analysis, Normative Nature of Case Law

1. INTRODUCTION

The question of whether or not do continental courts' decisions have any normative, or precedential, value has long been a part of legal discussions, attracting attention from numerous legal scholars.[2] Recently, this question has been given a more quantitative attention, employing network analysis to use citations to past decisions as a tool to determine the courts' actual practice in this matter.[3] Empirical data-driven research on theoretical legal concepts as well as various legal practices is one of the directions legal informatics follows recently. Despite that legal information retrieval is still more common direction in this field, with the development of advanced natural language processing techniques, legal scholars are capable of tackling some purely theoretical fundamental legal questions as well. Citation network analysis is a great example of a method used for both purposes. On the one hand, it serves well in, for example, providing data

[2] Let us, for one noteable example, mention a comparative study of precedent across various jurisdictions edited by MacCormick, N., Summers, R. S. (eds.) (1997) *Interpreting Precedents. A Comparative Study*. Dartmouth: Aldershot.

[3] See for example Fowler, J.H., Johnson, T.R., Spriggs, J.F., Jeon, S., Wahlbeck, P.J. (2007) Network Analysis and the Law: Measuring the Legal Importance of Precedents at the U.S. Supreme Court. *Political Analysis*, 15(3), pp. 324–346; Hitt, M. (2016) Measuring Precedent in Judicial Hierarchy. *Law and Society Review*, 50(1): pp. 57-81; Derlén, M. and Lindholm, J. (2017) Peek-a-Boo, It's a Case Law System! Comparing the European Court of Justice and the United States Supreme Court from a Network Perspective. *German Law Journal*, 18(3), pp. 647–686; Derlén, M. and Lindholm, J. (2014) Goodbye van Gend en Loos, Hello Bosman? Using Network Analysis to Measure the Importance of Individual CJEU. *Judgments. European Law Journal*, 20(5), pp. 667-687; or Derlén, M. and Lindholm, J. (2015) Characteristics of Precedent: The Case Law of the European Court of Justice in Three Dimensions. *German Law Journal*, 16(5), pp. 1073–1098.

Fowler et al. (2007) op. cit., pp. 324–346.

suitable for court decisions retrieval and recommendation systems.[4] On the other hand, it is commonly used for finding out how the judicial systems work in general. Specifically, citation analysis can help understand abstract legal concepts such as relevance or importance of court decisions as well as citation practice of different courts and judges.

Until very recently, the Czech citation practices have remained empirically unexplored.[5] The classical doctrinal approach yielded no fixed agreement on the normative nature of past judicial decisions for subsequent decision-making, often settling on conclusions that while the decisions are not precedents in the common law sense, they have some sort of fluid normative value.[6] However, the analyses of judicial decisions often use concepts borrowed from the doctrine of binding precedent (such as ratio decidendi and obiter dictum), with one notable exception: the requirement of similarity of the facts of the cases.

Ignoring questions of fact may lead to decontextualized use of case law, where a case is cited not because its facts are similar and it has a recognizable precedential value, but just because it contains something loosely legally related to the decision in which it is cited. There have been voices criticising this decontextualized approach in the use of case law in judicial decision-making, usually citing the (risk of) infringement of the separation of powers thesis, and – in consequence – diluting the legitimacy of such judicial decision making.[7] Should we put together this practice together with the prevalent opinion that citing past case law is somewhat bordering on good manners[8] an environment is created that encourages citing any past judicial decision relevant to any legal issue

---

[4] For example, legal information systems employ features recommending decisions cited in certain decision, or a citation index of a decision is used as a measure determining its importance and its position in list of results when searching for relevant court decisions.

[5] This has been changed by research published in Harašta, J., Smejkalová, T., Novotná, T. et al. (2021) *Citační analýza judikatury*. Praha: Wolters Kluwer. This publication brings the overview of the Czech apex courts' citation practice, concluding that while it is very far from precedent, the research suggests development to some sort of weak principle of stare decisis. See Harašta, Smejkalová, Novotná et al. (2021) op. cit., pp. 225-233.

[6] See Bobek, M., Kühn, Z. et al. *Judikatura a právní argumentace*. 2nd edition. Praha: Auditorium, 2013.

[7] See e.g. Smejkalova, T. (2019) Judikatura, nebo precedens? *Právník*, 158(9), pp. 852-864; Polčák, R. (2012) *Internet a proměny práva*. Praha: Auditorium, p. 228-232; or David, L. (2008) Co je precedent v rozhodnutích českých civilních soudů? In: *Dny práva – 2008 – Days of Law*. Brno: Tribun EU [online]. 2008 [accesseed 1.2.2013]. Available from http://www.law.muni.cz/sborniky/dp08/files/pdf/prteorie/david.pdf.

[8] Currently, around 70% of decisions by Czech apex courts contain at least one reference to past judicial decision. See Harašta, J., Smejkalová, T., Novotná, T. et al. (2021) op. cit., pp. 165-178.

the decision tackles, including the ones related to general issues of principle, or procedure. Moreover, a suggestion was made by a study within the Dutch legal environment[9] that the judicial decisions more frequently cited by other decisions are cited because of an issue of a procedural or a more general nature.

We have designed a study to explore this suggestion further. We have used network analysis to construct a number of chains of decisions that were further analysed in terms of their content. These chains were chosen based on the indegree centrality of the decisions which allowed us to explore the claim above, that the judicial decisions more frequently cited by other decisions are cited because of an issue of a procedural or a more general nature. It also allows us to explore, whether it does, in turn, suggest that decisions with low indegree centrality would be cited rather for substantive law reasons.

To explore these hypotheses, we have analysed the chains of citations, categorized the citation occurrences and compared them not only to the indegree centrality but also to the authority score of cited decision. We show that while in our sample the decisions with high indegree centrality and high authority scores do, indeed, tend to be cited for procedural, or unquestionably general, reasons, the opposite side of this hypothesis points towards a more complicated reality. While this article must be seen as a proof of concept case study and while its limited scope does not allow us to generalize on our findings, it suggests that the actual citation environment in Czech legal setting (and likely in other continental legal settings sharing basic systemic similarities[10]) might be more complex than the hypotheses suggest.

2. THEORY OVERVIEW

Recent studies employing network analysis[11] of citations of judicial decisions usually rely on simple operationalizations of citations of judicial decisions as an indicator of some sort of relevance,[12] importance,[13] noteworthiness[14] etc. of such a decision in the legal system, usually connecting it with

[9] Winkels, R. and Ruyter, J. (2012) Survival of the Fittest: Network Analysis of Dutch Supreme Court Cases. In: Palmirani, M. et al. (eds.) *AICOL Workshops 2011*. Heidleberg: Springer Verlag, pp. 106-115.

[10] The Czech legal system is said to belong to the "Germanic" family within the continental law tradition. Our discussion and conclusions might not be transferrable to differing continental jurisdictions, notably to the French one, that does not allow judges to rely on previous case law at all. See Art. 5 of Code Civil.

network of measures of degree centrality,[15] eigenvector centrality or more complex measures based on iterative algorithms (authority and hub score).[16] These methods – developed in the context of precedential legal systems – have been used in continental legal systems with varied results.[17]

The number of times a decision is cited (which in network analysis terms corresponds to its indegree centrality) may be intuitively seen as an indicator of a decision's prominence in the network and, consequently, the legal system as a whole. Fowler et al.,[18] Fowler and Jeon[19] and Whalen[20] have shown that it is oversimplified and cannot by itself grasp the complexities of the judicial decision-making. For this reason, Fowler et al., Fowler and Jeon, and in continental legal settings for example Derlén and Lindholm[21] make use of authority and hub scores.[22]

It may seem tempting to use these metrics to determine relevance of a judicial decision and explore employing them in legal information retrieval systems. Citation analysis is commonly used to retrieve legally

[11] Network analysis is a set of techniques based on network and graph theories. It is based on an assumption that various social phenomena (such as judicial decisions in our case) are linked together by various relationships (in our case citations). Analysis of these relationships and their structures is capable of bringing new information about the network as a whole. For detailed explanation see Brandes, U. and Erlebach, T. (eds.) (2005) *Network Analysis. Methodological Foundations*, Heidelberg: Springer.

[12] Black, R.C. and Spriggs, J.F. II. (2013) The Citation and Depreciation of U.S. Supreme Court Precedent. *Journal of Empirical Legal Studies.* 10(2), pp. 325–358.

[13] Fowler, J.H., Johnson, T.R., Spriggs, J.F., Jeon, S., Wahlbeck, P.J. (2007) Network Analysis and the Law: Measuring the Legal Importance of Precedents at the U.S. Supreme Court. *Political Analysis*, 15(3), pp. 324–346.

[14] Hitt, M. (2016) Measuring Precedent in Judicial Hierarchy. *Law and Society Review*, 50(1): pp. 57-81.

[15] See Fowler et al. (2007) op. cit., pp. 324–346, or Fowler, J. and Jeon, S. (2008) The Authority of Supreme Court precedent. *Social Networks*, 30, pp.16–30.

[16] See Fowler et al. (2007) op. cit., pp. 324–346 or Fowler and Jeon (2008) op. cit., pp. 16–30.

[17] Derlén, M. and Lindholm, J. (2017) Peek-a-Boo, It's a Case Law System! Comparing the European Court of Justice and the United States Supreme Court from a Network Perspective. *German Law Journal,* 18(3), pp. 647–686; Derlén, M. and Lindholm, J. (2014) Goodbye van Gend en Loos, Hello Bosman? Using Network Analysis to Measure the Importance of Individual CJEU. *Judgments. European Law Journal*, 20(5), pp. 667-687; or Derlén, M. and Lindholm, J. (2015) Characteristics of Precedent: The Case Law of the European Court of Justice in Three Dimensions. *German Law Journal*, 16(5), pp. 1073–1098.

[18] Fowler et al. (2007) op. cit., pp. 324–346.

[19] Fowler and Jeon (2008) op. cit., pp. 16–30.

[20] Whalen, R. (2013) Modelling Annual Supreme Court Influence: The Role of Citation Practices and Judicial Tenure in Determining Precedent Network Growth. In: Menzes, R., Evsukoff, A., Gonzales, M.C. (eds.) *Complex Networks*. *Studies in Computational Intelligence*. Berlin, Heidelberg: Springer, pp. 169–176, p. 269.

[21] Derlén and Lindholm (2017) op. cit., pp. 647–686.

[22] Authority and hub scores are based on Kleinberg's iterative algorithms – HITS. See Kleinberg, J. M. (1998) Authoritative sources in a hyperlinked environment. In: *Proceedings of ACM-SIAM Symposium on Discrete Algorithms 1998*, pp. 668-677.

relevant court decisions in recommendation systems. Wagh and Anand showed that decisions connected by citations are more similar than decisions similar according to the cosine similarity.[23]

However, there have been voices who disputed the automatic borrowing of these operationalizations from studies in precedential legal systems and using them in continental legal setting.[24] While the results of Derlén and Lindholm's research suggest similarity in network patterns between the decision-making practice of the Supreme Court of the United States,[25] the underlying processes leading to overt similarities in network patterns are not the same.

Before building any concepts of relevance or importance of a decision in a system in continental legal settings on indegree centrality or authority score, more research needs to be undertaken.

Winkels and de Ruyter, who explored the citation environment of the Dutch Supreme Court found out that most of the most cited cases are – unsurprisingly – of a procedural nature.[26] While they do not elaborate on this point further, a recent research related to the citation environment of apex courts in the Czech Republic[27] agrees that in continental legal settings, this is, indeed, unsurprising as most apex courts, such as Supreme Courts or Constitutional Courts often do not resolve questions of fact, they focus on questions of law, usually those having wider impact on the legal system, not only to the individual claimants. The questions of law often tend to be related to issues of procedure, court competence, or more general

---

[23] Wagh, R., Anand, D. (2017). Application of citation network analysis for improved similarity index estimation of legal case documents: A study. *2017 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC),* 1–5. https://doi.org/10.1109/ICCTAC.2017.8249996.

[24] Frankenreiter, J. (2017) Network Analysis and the Use of Precedent in the Case Law of the CJEU – A Reply to Derlén and Lindholm. *German Law Journal,* 18(3), p. 687- 693 and Petersen, N. and Towfigh, E. V. (2017) Network Analysis and Legal Scholarship. 18 *German Law Journal*, 18(3), p. 695-700 critically discussed Derlén and Lindholm's conclusions about a "precedential" nature of the decision-making practice of Court of Justice of the European Union. See Derlén, M. and Lindholm, J. (2017) Peek-a-Boo, It's a Case Law System! Comparing the European Court of Justice and the United States Supreme Court from a Network Perspective. *German Law Journal,* 18(3), pp. 647–686. Recently, this critique has also been voiced in Harašta, J., Smejkalová, T., Novotná, T. et al. (2021) *Citační analýza judikatury*. Praha: Wolters Kluwer. In addition, for a recent analysis of an alternative framework to approach both precedential as well non-precedential legal systems see Smejkalová (2020) op. cit.

[25] See Derlén and Lindholm (2017) op. cit.

[26] Winkels and de Ruyter (2012) op. cit., pp. 106-115.

[27] Harašta, J., Smejkalová, T., Novotná, T. et al. (2021) *Citační analýza judikatury*. Praha: Wolters Kluwer.

questions of principle (such as in the case of a court deciding upon constitutionality of individual legal rules).

However, we should note that since we are dealing with law and individual legal systems more elements of a given legal system may be at play, especially the role of their supreme courts. For example, research within the Italian legal system has shown that the above link between the number of times a decision was cited and the substantive/procedural nature of the cited case might not necessarily be generally applicable as the most cited cases are rather of substantive, not procedural nature.[28]

Moreover, the details on how to use past case-law in judicial decision-making in continental legal settings differ from system to system, ranging from a prohibition[29] to overt resemblance of a precedential system.[30] In systems, where the role of case law seems to be rather fluid, such as the Czech legal system, the textbooks usually try to paint a picture of a continental type of case-law – 'judikatura' – as something different from precedent.[31] Nevertheless, the theory borrows doctrine-of-precedent terms such as ratio decidendi or obiter dictum, making 'judikatura' seem conceptually closely related to precedent. However, the most notable difference between the way continental legal systems – and the Czech system, within which we have conducted present research – handle the case-law is the (possibly seeming?) omission of the similarity of facts as a condition for a precedent's applicability.[32]

Therefore, a part of the goal of this paper is to shed more light onto the question as to what extent we can or cannot utilise the same operationalisations in citation analysis in continental legal system as in presidential systems, given the specifics and possible differences between individual legal systems.

In a system where judges are not compelled to consider the factual similarity between cases, they tend to use past case law as something between a legal rule and doctrine (or jurisprudence), subjecting it

[28] See e.g. Agnoloni, T., Pagallo, U. (2015) The case law of the Italian constitutional court, its power laws, and the web of scholarly opinions. In: *ICAIL'15: 15th International Conference on Artificial Intelligence and Law*, pp. 151–155, or Agnoloni, T. Pagallo, U. (2015) The Power Laws of the Italian Constitutional Court, and Their Relevance for Legal Scholars. In: *Legal Knowledge and Information Systems*. pp. 1-10.

[29] Such as in the context of Article 5 of Code Civil in case of French legal system.

[30] Such as the practice of the Court of Justice of the European Union.

[31] Harvánek, J. et al. (2008) *Teorie práva*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, p. 250.

[32] Smejkalová, T. (2019) Judikatura, nebo precedens? *Právník*. 158(9), pp. 852-864.

to interpretation, and focusing on general coherence of the legal system.[33] Therefore, it is not surprising that within such a legal setting, the more general or procedural issue the decision solves or the more important legal principle it helps to paint, the more appealing it might be for other judges to call upon those decisions in their own decision-making. Simply said, the more general the decision, the more likely it is to be prominent in the legal system.[34] Or, in network analysis terms, the higher indegree centrality – or authority score (measures based on the inward citations of the decision) – the decision might have. Consequently, this might mean that in continental legal settings courts may refer to such a general decision even in situations that are not factually similar with the case decided by the general decision and could not strictly be called 'precedents'. It is not clear, however, whether the opposite would be the case, i.e. tendency to choose less-cited decisions for substantive law reasons and in factually similar situations.

3. METHODOLOGY AND DATA

We have designed a proof-of-concept case study that allows us to test this assumption and to determine whether the lower indegree centrality (and authority score) decisions tend to be cited for substantive law reasons in factually similar situations.

We closely build upon a previous study that constructed and analysed a network of judicial decisions of Czech apex courts. Technical details of the network analysis and its parameters are, therefore, reported

[33] See e.g. Araszkiewicz, M., Šavelka, J. (eds.) *Coherence: Insights from Philosophy, Jurisprudence and Artificial Intelligence*. Heidleberg: Springer; or in the Czech legal context Smejkalová, T. A Matter of Coherence. In: Araszkiewicz, M., Myška, M., Smejkalová, T., Šavelka, J., Škop, M. (eds.) *Law and Literature. Argumentation 2012 Workshop Proceedings*. Brno: Masarykova univerzita, pp. 31-44.

[34] It must be noted that this is by no means the only factor determining the decision's prominence in the system, nor its normative value of any kind, see MacCormick, N., Summers, R. S. (eds.) (1997) *Interpreting Precedents. A Comparative Study*. Dartmouth: Aldershot; in Czech legal context see Kühn, Z. (2001) Nová koncepce normativity judikatury obecného soudnictví na pozadí rozhodnutí Ustavního soudu. *Právní rozhledy*, (6), pp. 265 - 269, nor the reason and circumstances why it was chosen to be cited in another judicial decision. This question has been discussed in more detail by Smejkalová, T. (2020) Importance of judicial decisions as a perceived level of relevance. *Utrecht Law Review,* 16 (1): pp. 39-56. doi:10.36633/ulr.504.

elsewhere.[35] For the purpose of this study, we used two outputs of this previous analysis: indegree centrality[36] and authority score.[37]

The indegree centrality was the criterion used to construct 11 chains of decisions leading to 5 different decisions containing the keyword ('azyl', eng. 'asylum') within the network of decisions within the corpus of Czech apex courts decisions.[38]

The first three decisions have the highest indegree centrality of all the decisions in the corpus containing the chosen keyword, the fourth one's indegree corresponds to the mean value, the fifth's indegree to the median value of indegree of all the decisions in the corpus containing the chosen keyword.

To construct the chains of decisions, these decisions formed Level 1 in our chain construction. To each of these decisions we have determined the set of all the decisions within the corpus that contained a citation to Level 1 decision. These decisions formed Level 2 in our chain. Consequently, we have determined the set of all the decisions within the corpus that contained a citation to at least one Level 2 decisions. We have repeated this process until we had five such levels. The construction scheme for our chains is illustrated in Figure 1.

As mentioned above, the decisions for each of the chains were chosen from individual levels based on their own indegree centrality: one of the chains led through decisions with maximum indegree decisions on each level, one led through median indegree decisions on each level, one led through minimum indegree decisions on each level.[39] Therefore, there are three chains leading to each one of the first three Level 1 decisions. Given the diminishing number of decisions at each level, there is only one

[35] Harašta, Smejkalová, Novotná et al. (2021) op. cit.

[36] The indegree centrality of a decision refers to the number of inward citations, i.e. the number of links leading to this decision.

[37] Authority score is based on connecting the meaning of both inward and outward citations in a more complex manner by means of an iterative algorithm. In Kleinberg's words, "[hubs] and authorities exhibit what could be called a mutually reinforcing relationship: a good hub is a [node] that points to many good authorities; a good authority is a [node] that is pointed to by many good hubs." See Kleinberg (1998) op. cit.

[38] Harašta, J., Novotná, T., Šavelka, J. (2020) Citation Data of Czech Apex Courts : *arXiv:2002.02224*, ISSN 2331-8422, available from: https://github.com/czech-case-law-relevance/czech-court-citations-dataset.

[39] Where there were more than one decision with the same median or minimum indegree value, we have chosen a decision at random.

chain to each of the fourth and fifth Level 1 decisions, both leading through median indegree centrality value decisions on each level.[40]

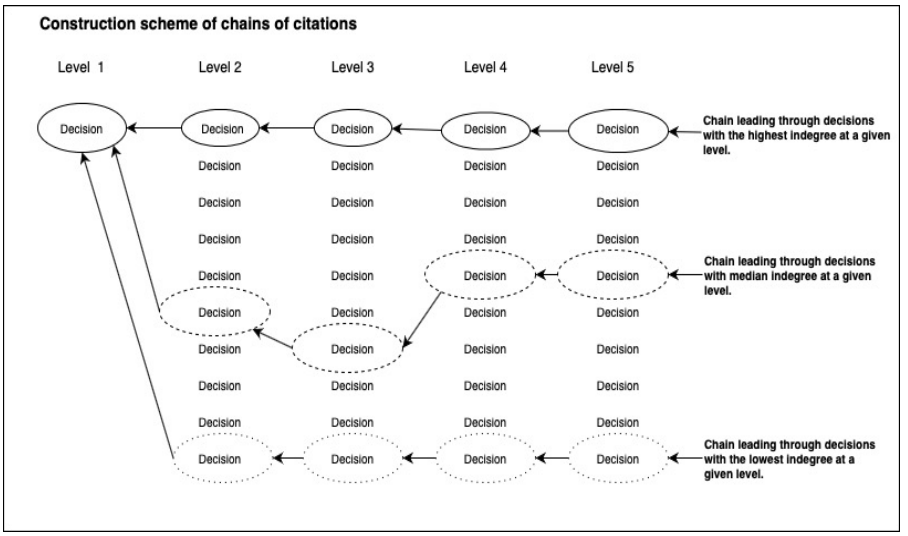

Figure 1. Construction scheme of citation chains

In short, in each chain of decisions, the one on lower level cites the one on the upper level, leading all the way to a given Level 1 decision. Within these chains, there are forty-four edges (links) – citations leading from lower level decision to upper level decision – which are relevant to our analysis.

The following Table 1 provides an overview of the chains and individual decisions for reference.[41]

[40] Sometimes a decision in these chains was cited by only one or two other decisions, which mean that a chain based on maximum indegree centrality decisions would look practically the same as a chain based on median value. We have chosen median to capture at least an attempt at a middle route.

[41] The decisions are listed under their file designations. Given our choice of keyword, most of the decisions were made by the Supreme Administrative Court of the Czech Republic, 6 decisions were made by the Constitutional Court of the Czech Republic and 3 decisions were made by the Supreme Court of the Czech Republic. For the purpose of the tables, "Route" means the indegree centrality value for which each of the decisions were chosen from their individual levels. When there were more decisions with the same indegree centrality on a given level, a random decision was chosen.

Chain designation	Level 1	Route	Level 2	Level 3	Level 4	Level 5
Asylum 1	1 Azs 13/2006 - 39	Max Med Min	3 Azs 89/2007 3 Azs 35/2006 1 Azs 43/2009	8 Azs 23/2008 7 Ans 15/2012 3 Azs 29/2010	5 Azs 74/2008 29 Cdo 5069/2015 3 Azs 6/2011	5 Azs 66/2008 33 Cdo 4050/2016 4 Azs 3/2012
Asylum 2	3 Azs 33/2004 – 98	Max	1 As 9/2009	Pl. ÚS 17/10-2	I. ÚS 4019/13	I. ÚS 1565/14
		Med	8 Aps 8/2007	6 Afs 46/2014	2 Ads 126/2014	2 As 107/2017
		Min	6 Ads 113/2009	7 Afs 1/2007	5 Azs 248/2017	10 Azs16/2017
Asylum 3	2 Azs 92/2005 - 58	Max	2 As 69/2008	IV. ÚS 2170/08	III. ÚS 1976/09	Pl. ÚS 29/11
		Med	4 As 3/2008	1 Ans 7/2012	1 Afs 362/2016	7 Afs 68/2017
		Min	4 As 3/2008	2 As 97/2016	1 As 343/2017	28Cdo729/2018
Asylum Mean	3 Azs 77/2004	Med	5 Azs 6/2010	7 Azs 79/2009	3 Azs 56/2012	2 Azs 220/2014
Asylum Median	3 As 84/2013	Med	5 Azs 209/2016	2 Azs 273/2016	2 Azs 331/2017	2 Azs 365/2017

Table 1: Overview of case file designations of decisions in each chain of decisions.

Table 2 shows the indegree centrality and Table 3 the authority scores of each of the decisions in the chains. For clarity, in the following text we will use special designations when talking about individual decisions. The five original decisions are referred to as Asylum 1, 2, 3, Mean and Median, depending on their indegree centrality. The chains are leading either through the decisions with the highest (max), median (med) or lowest (min) indegree centrality on a given level. Individual decisions will always be referred to by their level and chain designation. For example, decision 3 Azs 89/2007 will be referred to as Asylum 1 max Level 2 decision.

Chain designation	Level 1	Route	Level 2	Level 3	Level 4	Level 5
Asylum 1	1991	Max	30	33	5	186
		Med	42	5	12	0
		Min	15	4	63	0
Asylum 2	589	Max	5	44	20	79
		Med	10	12	3	0
		Min	11	130	2	0
Asylum 3	492	Max	23	52	18	1362
		Med	332	1	4	0
		Min	332	3	1	0
Asylum Mean	9	Med	60	131	3	0
Asylum Median	2	Med	2	3	4	1

Table 2: Indegree centrality of individual decisions[42]

[42] Indegree centrality refers to the decision's indegree centrality in the whole corpus referred to above.

High authority score			Low authority score		
Place in chain	Decision designation	Authority score	Place in chain	Decision designation	Authority score
Asylum 1 Level 1	1 Azs 13/2006 - 39	1,9 · 10−5	Asylum mean Level 1	3 Azs 77/2004 – 86	8,2 · 10−9
Asylum 3 min Level 2	4 As 3/2008 - 78	1,5 · 10−5	Asylum 3 min Level 3	2 As 97/2016	3,1 · 10−9
Asylum 3 med Level 2	4 As 3/2008 - 78	1,5 · 10−5	Asylum 1 med Level 4	29 Cdo 5069/2015	3, 0 · 10−9
Asylum 3 Level 1	2 Azs 92/2005 - 58	1,3 ·10−5	Asylum 2 min Level 2	6 Ads 113/2009 - 43	2,6·10−9
Asylum mean Level 3	7 Azs 79/2009 - 84	5,2·10−6	Asylum 1 med Level 3	7 Ans 15/2012 - 15	2,0·10−9
Asylum 3 max Level 3	IV. ÚS 2170/08-1	4,6 ·10−6	Asylum 1 min Level 3	3 Azs 29/2010 - 63	1,7·10−10
Asylum 3 max Level 4	III. ÚS 1976/09-1	4,0·10−6	Asylum median Level 1	3 As 84/2013	1,6·10−10
Asylum 2 Level 1	3 Azs 33/2004 – 98	1,9·10−6	Asylum 1 max Level 4	5 Azs 74/2008 - 88	9,6·10−10
Asylum 1 med Level 2	3 Azs 35/2006 - 104	1,4·10−6	Asylum 3 med Level 4	1 Afs 362/2016 - 36	9,2·10−10
Asylum 2 med Level 2	8 Aps 8/2007-90	1,3·10−6	Asylum 3 med Level 3	1 Ans 7/2012 - 43	3,5·10−10
			Asylum 2 min Level 4	5 Azs 248/2017 - 35	7,0·10−11
			Asylum 3 min Level 4	1 As 343/2017	4,0·10−11

Table 3: Authority score of individual decisions in order from the highest to the lowest[43]

All the texts of all the decisions in these chains were subsequently analyzed with special attention to the facts of the case of each decision and the individual context – procedural/general or substantive – for which it was cited by a decision on a lower level. Based on what has been explained above, we have sought to explore the following hypothetic tendencies within our 11 citation chains:

Hypothesis 1a: Decisions with higher indegree centrality are cited for their procedural/more general issues with which they deal.

Hypothesis 1b: Decisions with higher authority score are cited for their procedural/more general issues with which they deal.

Hypothesis 2a: Decisions with low indegree centrality are cited for their substantive issues with which they deal.

Hypothesis 2b: Decisions with low authority score are cited for their substantive issues they with which they deal.

4. ANALYSIS AND DISCUSSION

While being aware of the thin divide between what may be categorized as substantive and procedural law-related reason for which a decision was

[43] Authority scores of individual decisions are related to the whole network of decisions in the corpus referred to above.

cited, for the purpose of this paper, we understand the procedural/substantive divide as follows.

Since the substantive law is a label related to rights and obligations of individuals (subjects of law), substantive law usually refers to actual claims of individuals. In our corpus of asylum-related decisions, these would comprise of interpretation of rights or reasons to grant asylum). Procedural law, on the other hand, comprises of rules governing the given procedure to test and protect these claims. In our asylum-related corpus, the procedural elements manifested in admissibility issues, burden of proof or competence of a body). In addition, some of the reasons for which the decisions were cited were somewhere between procedural and some sort of general nature, such as asking about the purpose of a discussed concept. Since these issues could not be classified as being of substantive law nature, and because of their conceptual closeness to the procedural baselines, we have included these borderline issues into the procedural category, which we label as "procedural/general".

Therefore, we have classified the reasons for which a decision was cited in another decision of the chain as either

- Procedural/general (comprising situations as admissibility of claims, burden of proof, obligations of a state body when making a decision, competence of a body or purpose of a concept);
- Substantive (interpretation of basic rights, interpretation of specific positive law concepts, application of specific requirements on a practically identical situation);
- Inconclusive (comprising situations where the court cited a decision for more than one reason).[44]

To differentiate between high and low indegree and high and low authority score, we have set up the lines as outlined in Table 4, taking into consideration the variation across these indicators.

[44] It must be noted that in law, it is not always easy to clearly categorize the reason for which a decision was cited as either of procedural or substantive nature. Even in cases where the decision itself was rather procedural (because it was not per se a decision on the merit of the case, just a decision on inadmissibility of the claim), the reason for which it was cited might not be related to the 'ratio decidendi' of the case, because it could have been some marginal issue the court opened when justifying the decision.

Categorization	Indegree	Authority score
High	> 50	$> 1{,}3 \cdot 10^{-6}$
Mid-range	11 to 49	$1{,}0 \cdot 10^{-8}$ to $3{,}8 \cdot 10^{-7}$
Low	< 10	$< 8{,}2 \cdot 10^{-9}$

Table 4: Distribution of high/mid-range/low indegrees and authority scores

After leaving out decisions of Level 5 (our citation chains did not go beyond Level 5), thirteen decisions were categorized as having high indegree centrality, twenty-five decisions were categorized as having low indegree centrality, while ten decisions were categorized as having high authority score and twelve as having low authority score.

Indegree centrality vs. Context of citation

Although the lines between these categories are rather blurred and debatable and although it is to be expected that the decision-making of apex courts in the analyzed situations would be predominantly of procedural/general nature,[45] we have identified nine situations where a judicial decision was cited predominantly as an argumentative support for a substantive law related claim.

Only six of the decisions cited in substantive circumstances were categorized as having low indegree and no decision with high indegree centrality was cited for substantive law reasons.

Unsurprisingly, out of forty-four situations in which a decision could be cited in our chains thirty-one citations were used to support procedural/general arguments the court makes in the rationale of its decision. Out of the thirty-one, sixteen citations led to decisions with high indegree centrality, seven to mid-range and eight to low indegree centrality decisions.

Authority score vs. Context of citation

We have found out that in 16 cases the reason a high authority score decision is cited is of procedural/general nature; this means that all the decisions whose authority score we have categorized as high are cited only for procedural/general reasons. In seven cases, a decision categorized as having low authority score was cited for procedural/general reasons. Only two decisions categorized as having low authority score were cited for

[45] As further discussed below, most of the decisions of Czech apex courts are those deciding the case is inadmissible. The reasons for these decisions are grounded in procedural reasons. Hence the abundance of procedural/general decisions available.

their substantive law considerations. In all the other instances (5) where a decision was cited for a substantive law reason the decision was categorized as having mid-range authority score.

Abundance of procedural/general reasons for citation

It is clear that in a significant number of cases (31) the reason for which a decision was cited was a procedural/general one. When it comes to apex court decision-making in the Czech legal system, this is not surprising: overviews of decision-making of the apex courts in the Czech Republic show that a significant amount of the decisions of these courts are in fact decisions on inadmissibility of the claim,[46] therefore being decisions falling into our procedural/general category. Even in situations where the courts would consider the similarity of the cases' facts, the facts of decisions containing considerations of procedural/general nature would be assessed on a higher level of abstraction. It cannot be ruled out, that in these situations – and in accordance with basic legal principles (such as that of due process) – the relevant facts even should be judged on a higher level of abstraction, disregarding more detailed factual differences. Some of these cases may in fact not really be judged as omitting to consider the similarity of facts, but simply working with the facts on a more abstract and general level.

We can observe this situation in particular in the *Asylum 1, 2* and *3* chains: *Asylum 1 Level 1* decision is always cited because it is specifying the meaning of a phrase/concept closely related to admissibility of a claim; *Asylum 2 Level 1* decision is always cited for one particular feature related to procedural matters – identification of the right provision of the procedural code that applies to a particular case of admissibility of a claim; *Asylum 3 Level 1* decision is always cited as an example of settled case-law of the way the points of a court claim should be formulated. On a very abstract level, all the Level 2 decisions' facts are comparable to the respective Level 1 decisions (e.g. in *Asylum 2* chain, all the Level 2 decisions dealt – apart from other issues – with an incorrect designation

[46] In 2019, Supreme Administrative Court decided 1381 out of 3880 claims were inadmissible, while Constitutional Court decided 409 out of 430 claims were inadmissible. See Statistical Overviews available at <http://nssoud.cz/Main2col.aspx?cls=StatistikaNewAlldata=1statoid=4year=2019menu=190> and <https://www.usoud.cz/fileadmin/userupload/ustavnisoudwww/Statistika/VSA2019.pdf.> Even though the decisions on inadmissibility are of procedural nature, they may still be picked up in later decision-making where a court's opinion on individual reasons of inadmissibility is found useful.

of points of claim). On a more detailed level, however, the facts of the Level 2 decisions would have to be judged as dissimilar. In *Asylum 2* and *Asylum 3* chains, Level 2 decisions were not even made in asylum matters. *Asylum 1* chains (especially the *Asylum 1 max* chain), however, seem to be a slight exception to this rule.

Asylum 1 max chain is one of the most thematically coherent citation chains in our sample: Level 5 to Level 2 decisions were made in factually very similar situations: asylum cases of nationals of Kazakhstan, who claim to be persecuted in their country of origin for their practice of so-called Pure Islam. Similar level of factual cohesion may only be partially seen in the *Asylum Mean* chain (where all the decisions are related to situations of legal expulsion of a person, but the reasons for it differed) and *Asylum Median* chain (all the decisions are related to situations of legal expulsion of a person as well as one particular circumstance – interpretation of the concept of "a relationship analogical to family relationship").

The *Asylum Median* chain is notable for one additional feature: all the decisions have very low indegree centrality (ranging between 1 and 4) and as in the only chain in out sample, all the decisions were cited for substantive law reasons.

While it seems that decisions with higher indegree centrality are cited for their procedural/general reasons (hypothesis 1a) and that decisions with higher authority score are cited for their procedural/more general reasons (hypothesis 1b), our experiment's data seem inconclusive when it comes to hypotheses 2a and 2b. Although in no situation was a high indegree/high authority score decision cited for substantive law reasons, the indegree centrality as well as the authority score of the decisions cited for substantive law reasons varied greatly: 1 to 44 in case of indegree centrality of cited decision; between $1{,}10^{-11}$ and $1{,}10^{-7}$ in case of authority scores of cited decisions.[47]

Nevertheless, the only case where a whole chain of decisions was cited for substantive law reasons AND had low indegree centrality was the *Asylum Median* chain, consisting of decisions that were cited truly scarcely. However, their authority scores were predominantly in the mid--range we specified above.

[47] To compare, authority score of the most cited decision in our corpus – decision of Czech Constitutional Court no. IV. ÚS 73/03 has authority score 0,13 and indegree centrality 6112.

We believe that our results may be interpreted in light of what the theory suggests about the continental use of case-law: while the whole system may at surface exhibit similar tendencies as a precedential system,[48] the similarities may very well be based on very different reasons[49] which may further dispute the automatic borrowing of operationalization of "importance" of a decision by means of their citation in another decision.[50]

Furthermore, when analyzing the decisions themselves, the guiding motivation to use past case-law in judicial argumentation may be described more as a call to coherence rather than a call to a precedent, even in situations where the court itself uses the word 'precedent' when citing another decision.[51] These 'precedential' situations are not always the core (to borrow a term from the doctrine of precedent – the ratio decidendi) of what the court dealt with. Especially in situations where the cited decision is of high indegree centrality or high authority score, the reason for which it is cited is often a marginal one in the whole of the rationale. However, it must be noted that within the Czech legal system what is 'marginal' in an apex court decision's rationale is rather relative. The court pieces its argument from different points of view, identifies various legal and argumentative points that add up to the justification of the final decision, drawing upon previously published legal opinion of itself or another apex court in each of these points. Consequently, this leads to situations where a single decision refers to many other past decisions, sometimes to support the ratio decidendi, but also to support general claims related to the competence of the court itself.[52] In a setting where each piece of argumentation starting with competence and procedure tends to be supported by past decisions, it is inevitable that these decisions will score higher in various network metrics.

Moreover, we believe that the main reason why past decisions are cited for procedural/general reasons even in situations where the particular

[48] See Derlén and Lindholm (2017) op. cit., pp. 647–686 or Harašta, Smejkalová, Novotná et al. (2020) op. cit.

[49] Loughlin. M. (2010) *Foundations of Public Law*. Oxford: OUP, p. 313.

[50] As already mentioned above, the automatic borrowing of this operationalization used originally in research in legal systems following the doctrine of binding precedent has been critically discussed by Smejkalová (2020) op. cit., pp. 39-56.

[51] See decision *Asylum 1 max Level 2* (Supreme Administrative Court decision no. 3 Azs 89/2007 – 68).

[52] The decision with the highest indegree as well as a decision with the highest authority score in the corpus of decisions we work with is being cited for a simple claim about the competence of Constitutional Court of the Czech Republic. See Constitutional Court's decision No. IV. ÚS 73/03 referred to above.

reason is not anywhere near the ratio decidendi of a case may be to simply provide a symbolical proof of coherence with the rest of the decision-making practice, most often based on similarity of legal claims,[53] or, occasionally, to reason by analogy. The individual choice to cite a judicial decision would then be guided by the principle of optimal relevance: 'the greater the cognitive effect achieved, and the smaller the mental effort required, the more relevant this input will be (…) at the time'[54] and in the particular context, therefore influenced by numerous external and internal factors.[55] This human tendency, thoroughly explained by pragmatic theories of relevance,[56] when assessed in the context of judicial decision making, results in using a reference to a past decision in support of the court's decision only if the result is better than what it would have been without it, and using the decision (including finding it, analysing it etc.) is worth the effort.

Therefore, we believe that the more interesting results of our study are actually those that seem inconclusive in relation to the tendencies listed as hypotheses 2a and 2b. It was rather clear in the texts of this very limited sample of decisions we worked with that while the court seemed to care about citing a decision to support its claim, it was not always necessarily one with the most prominence in the legal system. We have observed situations where the cited decision in our chains was one made by the same panel of judges a couple of months earlier (such as when *Asylum Mean Level 3* cites *Asylum Mean Level 2*) as well as distinguishing a truly 'precedential' decision in a very similar situation (such as when *Asylum 1 max Level 5* decision cites *Asylum 1 max Level 4* decision).

We believe that these findings are telling with respect to the fluid and inconsistent way the normative nature of case law in the Czech legal system is treated. When there is no clear rule to guide the court when and how should it cite past judicial decisions, the guiding mechanism will be that of optimal relevance: as long as citing past decisions is not reprimanded and

---

[53] Feldman, M. S., March, J. G. (1981) Information in Organizations as Signal and Symbol. *ADMIN. Scl. Q*, 26(2), p. 171-186, or in Czech context Smejkalová, T. (2013) Odkazy na soudní rozhodnutí a symbolická hodnota informace. *Jurisprudence*, 8: pp. 3-9.

[54] Wilson, D. (2016) Relevance Theory. In: Huang, Y. (ed.) *Oxford Handbook of Pragmatics*. Oxford: OUP, p. 87.

[55] For more details on how to understand an optimally relevant choice in citing past case law, regardless of legal system in question see Smejkalová (2020) op. cit.

[56] Sperber, D. and Wilson, D. (1995) *Relevance: communication and cognition*. 2nd Edition. Oxford: Blackwell.

as long as it brings the sought for results (i.e. a well-reasoned decision coherent with the rest of the legal system) and as long as the decision is accessible the court will continue to do so. To what extent does this practice constitute a normative practice with normative expectations is yet another question.

5. CONCLUSION

In our research, network analysis and network metrics of indegree centrality and authority score were used as a part of a mixed method approach, complemented by analysis of the texts of thus chosen decisions. We have used network analysis to construct the chains to further analyze the decisions by traditional means – textual analysis – mainly to avoid bias in choosing decisions to which – or from which to construct chains of citations. In this regard, we follow a similar line of research as Olsen and Kücküksu[57] did when analyzing a set of European Court of Human Rights' decisions.

Our limited study's results seem to suggest that the expectation of decisions with high indegree centrality and/or high authority score would be cited for their procedural or other general reasons might be the correct one. They are, however, not conclusive as to the opposite of this claim as decisions with lower indegree centrality and low authority score in our sample were not necessarily cited for the substantive law reason, since only two out of nine decisions categorized as having low authority score were actually cited for these reasons.

While our results must be treated as limited proof-of-concept case study, we believe that its results are conducive with the fact that the normative role of case law in the Czech legal system is not a settled matter, which makes the actual citation environment in continental legal setting more complex than our hypotheses suggest. However, present methodological approach seems capable to be highly useful in further exploring the normative nature of judicial decisions in non-precedential legal settings.

Additionally, our research approach may contribute to practical use of this type of citation analysis as well, since citation analysis is commonly used in legal recommendation systems. Wagh and Anand provided a study

[57] Olsen, H.P., Kücküksu, A. (2017) Finding hidden patterns in ECtHR's case law: On how citation network analysis can improve our knowledge of ECtHR's Article 14 practice. *International Journal of Discrimination and the Law*. 17(1): pp. 4-22.

proving higher similarity of the decisions connected with citations than the decisions similar according to the cosine similarity.[58]

On the other hand, our conclusions suggest that not all the cited decisions are relevant when it comes to considering the legal issue. Therefore, a recommendation system based only on the citations might retrieve a set of decisions only with low precision. Thus, it requires additional post-processing which makes the precise judicial decisions retrieval time consuming. To achieve higher precision of retrieved decisions, we suggest including a subsequent semantic processing to distinguish between different court decisions cited for different legal reasons. We believe that a combination of a citation analysis and semantic similarity may lead to a more efficient and more precise judicial decisions retrieval.

LIST OF REFERENCES

[1] Agnoloni, T., Pagallo, U. (2015) The case law of the Italian constitutional court, its power laws, and the web of scholarly opinions. In: *ICAIL'15: 15th International Conference on Artificial Intelligence and Law*, pp. 151–155.

[2] Agnoloni, T. Pagallo, U. (2015) The Power Laws of the Italian Constitutional Court, and Their Relevance for Legal Scholars. In: *Legal Knowledge and Information Systems*. pp. 1-10.

[3] Araszkiewicz, M., Šavelka, J. (eds.) *Coherence: Insights from Philosophy, Jurisprudence and Artificial Intelligence*. Heidleberg: Springer.

[4] Black, R.C. and Spriggs, J.F. II. (2013) The Citation and Depreciation of U.S. Supreme Court Precedent. *Journal of Empirical Legal Studies*, 10(2), pp. 325–358.

[5] Bobek, M., Kühn, Z. et al. *Judikatura a právní argumentace*. 2nd edition. Praha: Auditorium, 2013.

[6] Brandes, U. and Erlebach, T. (eds.) (2005) *Network Analysis. Methodological Foundations*, Heidelberg: Springer.

[7] David, L. (2008) Co je precedent v rozhodnutích českých civilních soudů? In: *Dny práva – 2008 – Days of Law*. Brno: Tribun EU [online]. 2008 [accesseed 1.2.2013]. Available from http://www.law.muni.cz/sborniky/dp08/files/pdf/prteorie/david.pdf.

[58] Wagh, R., & Anand, D. (2017). Application of citation network analysis for improved similarity index estimation of legal case documents: A study. *2017 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC)*, 1–5. https://doi.org/10.1109/ICCTAC.2017.8249996.

[8] Derlén, M. and Lindholm, J. (2017) Peek-a-Boo, It's a Case Law System! Comparing the European Court of Justice and the United States Supreme Court from a Network Perspective. *German Law Journal*, 18(3), pp. 647–686.

[9] Derlén, M. and Lindholm, J. (2014) Goodbye van Gend en Loos, Hello Bosman? Using Network Analysis to Measure the Importance of Individual CJEU. *Judgments. European Law Journal*, 20(5), pp. 667-687.

[10] Derlén, M. and Lindholm, J. (2015) Characteristics of Precedent: The Case Law of the European Court of Justice in Three Dimensions. *German Law Journal*, 16(5), pp. 1073–1098.

[11] Feldman, M. S., March, J. G. (1981) Information in Organizations as Signal and Symbol. *ADMIN. Scl. Q*, 26(2), p. 171-186.

[12] Fowler, J.H., Johnson, T.R., Spriggs, J.F., Jeon, S., Wahlbeck, P.J. (2007) Network Analysis and the Law: Measuring the Legal Importance of Precedents at the U.S. Supreme Court. *Political Analysis*, 15(3), pp. 324–346.

[13] Fowler, J. and Jeon, S. (2008) The Authority of Supreme Court precedent. *Social Networks*, 30, pp. 16–30.

[14] Frankenreiter, J. (2017) Network Analysis and the Use of Precedent in the Case Law of the CJEU – A Reply to Derlén and Lindholm. *German Law Journal*, 18(3), p. 687- 693.

[15] Harašta, J., Novotná, T., Šavelka, J. (2020) Citation Data of Czech Apex Courts. : arXiv:2002.02224, ISSN 2331-8422, available from: https://github.com/czech-case-law-relevance/czech-court-citations-dataset.

[16] Harašta, J., Smejkalová, T., Novotná, T. et al. (2020) *Citační analýza judikatury*. Praha: Wolters Kluwer (in print).

[17] Harvánek, J. et al. (2008) *Teorie práva*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk.

[18] Hitt, M. (2016) Measuring Precedent in Judicial Hierarchy. *Law and Society Review*, 50(1): pp. 57-81.

[19] Kleinberg J.M. (1998) Authoritative sources in a hyperlinked environment. In *Proceedings of ACM-SIAM Symposium on Discrete Algorithms*, p. 668-677.

[20] Kühn, Z. (2001) Nová koncepce normativity judikatury obecného soudnictví na pozadí rozhodnutí Ustavního soudu. *Právní rozhledy*, (6), pp. 265 – 269.

[21] Loughlin. M. (2010) *Foundations of Public Law*. Oxford: OUP.

[22] MacCormick, N., Summers, R. S. (eds.) (1997) *Interpreting Precedents. A Comparative Study*. Dartmouth: Aldershot.

[23] Olsen, H.P., Kücküksu, A. (2017) Finding hidden patterns in ECtHR's case law: On how citation network analysis can improve our knowledge of ECtHR's Article 14 practice. *International Journal of Discrimination and the Law*. 17(1): pp. 4-22.

[24] Petersen, N. and Towfigh, E. V. (2017) Network Analysis and Legal Scholarship. 18 *German Law Journal*, 18(3), p. 695-700

[25] Polčák, R. (2012) *Internet a proměny práva*. Praha: Auditorium, p. 228-232.

[26] Smejkalova, T. (2019) Judikatura, nebo precedens? *Právník*, 158(9), pp. 852-864.

[27] Smejkalová, T. (2013) Odkazy na soudní rozhodnutí a symbolická hodnota informace. *Jurisprudence*, 8: pp. 3-9.

[28] Smejkalová, T. A Matter of Coherence. In: Araszkiewicz, M., Myška, M., Smejkalová, T., Šavelka, J., Škop, M. (eds.) *Law and Literature. Argumentation 2012 Workshop Proceedings*. Brno: Masarykova univerzita, pp. 31-44.

[29] Smejkalová, T. (2020) Importance of judicial decisions as a perceived level of relevance. *Utrecht Law Review,* 16 (1): pp. 39-56. doi:10.36633/ulr.504

[30] Wagh, R., & Anand, D. (2017). Application of citation network analysis for improved similarity index estimation of legal case documents: A study. *2017 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC),* 1–5. https://doi.org/10.1109/ICCTAC.2017.8249996.

[31] Whalen, R. (2013) Modelling Annual Supreme Court Influence: The Role of Citation Practices and Judicial Tenure in Determining Precedent Network Growth. In: Menzes, R., Evsukoff, A., Gonzales, M.C. (eds.) *Complex Networks. Studies in Computational Intelligence*. Berlin, Heidelberg: Springer, pp. 169–176.

[32] Wilson, D. (2016) Relevance Theory. In: Huang, Y. (ed.) *Oxford Handbook of Pragmatics*. Oxford: OUP, p. 79-100.

[33] Winkels, R. and Ruyter, J. (2012) Survival of the Fittest: Network Analysis of Dutch Supreme Court Cases. In: Palmirani, M. et al. (eds.) *AICOL Workshops 2011*. Heidleberg: Springer Verlag, pp. 106-115.

DOI 10.5817/MUJLT2021-2-5

"A ROBOT IS WATCHING YOU": HUMANOID ROBOTS AND THE DIFFERENT IMPACTS ON HUMAN PRIVACY

by

LUCAS CARDIELL*

Robots, particularly the ones that are designed and deployed for communicating and interacting with people, slip into more and more domains of human life - from the research laboratories and operating rooms to our kitchens, bedrooms, and offices. They can interact with humans with facial expressions, gaze directions and voices, mimicking the affective dynamics of human relationships. They consequently present opportunities and risks to peoples' privacy, among other human rights and values. Such rights and values include the right to the integrity of a person, social and private life, the best interests of individuals, personal autonomy, and human dignity. They all are essential to the exercise of the right to privacy.

The literature on privacy issues in the context of humanoid has a strong focus on information privacy and data protection. It has given, however, less attention to other dimensions of privacy, e.g. physical, emotional, or social privacy. This article argues for an "evolving" or "transformable" notion of privacy, as opposed to the "elusive" concept of privacy elaborated by leading privacy theorists such as Daniel J. Solove (2008) and Judith J. Thomson (1975). In other words, rather than assuming that privacy has a single core or definition (as defined, e.g., in Warren and Brandeis' 1890 paper), it maintains that it is important to conceptualize privacy as distinguishable into various aspects, including, but not limited to, informational privacy, the privacy of thoughts and actions, and social privacy. This inductive approach makes it possible to identify new dimensions of privacy and

* E-mail: Lucas.Cardiell@eui.eu, Ph.D. researcher at the European University Institute, Florence, Italy.

therefore effectively respond to the challenges raised by humanoid robots that constantly introduce new spheres of privacy intrusions.

KEY WORDS

Artificial Intelligence; Robotics; Human Rights; Technology; Privacy; Humanoid Robots

1. ARTIFICIAL INTELLIGENCE, HUMANOID ROBOTS, AND HUMAN RIGHTS AND VALUES – SETTING THE SCENE

In search of the meaning and the value of the appearance of humanoid robots (hereinafter HR), I came across an interview with Emmanuel Lévinas – On the Face and Responsibility for the Other – which gave me a way of thinking. Here is a part of it:

> *"Thou shall not kill" is the first word of the face. The look is always awareness, perception. In the face, there's something quite exposed, threatened as if inviting us to an act of violence. At the same time, the face is what forbids us to kill. When we see a nose, eyes, forehead, and chin, and are able to describe them, we turn towards the Other as an object. The best way to look at the Other isn't even to notice their eyes' color. The other person is, at first glance, a part of the ensemble, which is given to me like other objects, like the whole world, like the "spectacle" of the world. And the other person breaks through this ensemble in some way precisely by their appearance as a face which isn't simply a form of plastic, but is immediately a commitment for me, an appeal to me, and order, an order for me to be at the service of this face. And that's what I call the commanding manner of the face: "the expression of God in the face".*[1]

I shall discuss the issue of HRs' appearance in-depth in the next section (2). For the moment, my intention is to explain the core and the purpose of this Article.

Artificial intelligence, or AI, with its various systems, virtual or embodied, creates great impacts on various domains of social life. It also reveals and brings forth serious challenges not only to social domains, e.g., unemployment, transparency, human rights. This is true particularly

[1] Emmanuel Lévinas, 2020. Lucas Cardiell, a doctoral researcher and host of the fresh YouTube channel "Conversation with Nobel Minds" (https://www.youtube.com/c/ConversationwithNobelMinds).

concerning the speculations of possible dangers around the emergence of "artificial general intelligence (also called Singularity)".[2] Moreover, AI challenges our fundamental human-centric understanding of the universe where we see ourselves in *general as* unique social-political- or rational animals who are, to put it in Aristotelian words, caught in a natural web of necessity. Such an idea makes us also rethink our relationships with others, with, for example, non-living things such as human- or animal-like robots, on a far grander scale.

AI is interesting because of the moral, ethical, and legal puzzles it reveals and the debates it provokes in academia and the world of practice.[3] It points at traditional issues that have been unthinkable, e.g., attributing rights to non-human entities. New entities now are holders of rights and legal protection, for example, animals[4] and rivers[5]. A related discussion about the attribution of rights to non-humans extends to intelligent machines, with, e.g., deep learning neural networks have come to the surface with challenges concerns foundations key concepts or questions. These include "what is a human", "who is responsible for harms caused by robots?" (also, good, for example, when a machine creates art, music and literary works), human biases (think of discriminatory decisions made by algorithms), "how and why do we draw lines between things and persons and what consequences if we do not?", "are robot rights and human rights the same?", and, following Kant's observation on avoiding cruelty to non--humans entities, "do or should robots deserve rights protections?".

To have an understanding of AI and privacy and their dynamic relations, I decided to investigate HRs as a representative case of AI systems. However, so far there has not been any case-law or judgments related to this

---

[2] There have been systematic and serious studies about of the possible dangers issuing from the advancements of intelligent machines that surpass human intelligence. See, Bostrom, N (2014). *Superintelligence: paths, dangers, strategies*. Oxford University Press, Kurzweil, R. (2005) *The Singularity Is Near: When Humans Transcend Biology.* VIKING Published by the Penguin Group. Equally important, there have also been scholars refuting the singularity and called it a fallacy. For critiques of singularity, see Dreyfus, H. (1972). *What Computers Can't Do*. MIT Press.

[3] For further discussions on the ethical and moral issues raised by AI and robotics see, e.g., Collin, A.; Wallach, W. and I. Smit (2006). "Why Machine Ethics?," in *IEEE Intelligent Systems*, vol. 21, no. 4, pp. 12-17, Wallach, W. & Allen C. (2009). *Moral machines: Teaching robots right from wrong.* Oxford: Oxford University Press, Gunkel, D. J. (2018). *Robot Rights*. Cambridge, MA: The MIT Press.

[4] See, for example: Regan, T (1987). The Case for Animal Rights. In M. W. Fox & L. D. Mickley (Eds.), *Advances in Animal Welfare Science 1986/87*. Martinus Nijhoff Publishers.

[5] See, for example: The Supreme Court of Columbia granting rights to the Atrato River, its basin and tributaries (*Center for Social Justice Studies et al. v. Presidency of the Republic et al.*, Constitutional Court of Colombia, Judgment T-622/16. (2016).

specific type of technology and its implications for human rights, perhaps because it is not yet highly advanced and used, and its autonomy is very limited at its current stage. Thus, I decided to use and benefit from an exciting technology-related case-law to discuss these rather complicated topics. This Article takes and extrapolates a landmark case-law, *Kyllo v. the United States* ,[6] which deals with the use of technology that violates the legally protected right to privacy under the 4th Amendment (that protects individuals from unreasonable searches and seizures by the government).

The US Supreme Court addressed questions relating to the legality of the use of a thermal-imaging technology (an imager known as Forward--looking infrared (FLIR)) by the Department of the Interior for determining the amount of heat emitted from a private home. Danny Kyllo was under suspicion of growing marijuana (which requires typically high-intensity lamps) as, based on information obtained, his garage roof and a side wall were relatively hotter than the other parts of his home. Agents of the Department, using thermal imaging technology that is typically used by the military and is not generally available in public, scanned and detected heat radiating from Kyllo's home in order to gather evidence towards issuing a search warrant. This use of heat-sensing technology without having first obtained a warrant was deemed unconstitutional by the Supreme Court, as the home is preserved as private, where Kyllo had an expectation of privacy, and thus constitutionally protected. The agents scanned the residence from their car from outside without physical intrusion. As a result, with the collected information the Department was able to obtain a search warrant. The Court held that the Department (thus the government) was in violation of the Fourth Amendment of the US Constitution that deals, *inter alia*, with the protection of people's right to privacy and freedom from unreasonable searches and seizures by the government.[7] The Court concluded that the use of thermal imaging technology constitutes a "search" within the meaning of the Fourth Amendment and that because of the thermal technology as it is not available for public use, the use of such technology was illegal.[8]

---

[6] The judgement was one of the landmark United States Supreme Court cases which dealt with a type of technology that constitutes a search under the Fourth Amendment. *Kyllo v. United States*, 533 U.S. 27 (2001).

[7] *Id. at* 40.

[8] *Id. at* 27.

Now let us examine a continuation of the aforementioned case and develop it fictional scenarios in which Kyllo purchases a HR hereinafter Pandora[9], which becomes later on a robotic partner) Kyllo and Pandora have interesting and dynamic relationships which produce several legal complexities. And the idea is to find answers or at least identify these complexities. It is true that these robots are futuristic, and their current market has not led to commercial success, it is unclear yet how much social acceptance or successful marketing they will gain. Admittedly, the legal precedent case, *Kyllo v. the United States*, might not totally involve the same facts as of the fictional Pandora platform. What the aim from making use for the case is to "learn lessons", no more, no less.

Kyllo is a single man who lives alone in his home. He decided to grow his own cannabis indoors. To accomplish his goal, he decides to seek help from Pandora. This is because he does not have the technical expertise for growing cannabis. With the advancement of AI techniques, Pandora can accomplish several tasks, from moving around independently, cooking and cleaning, to socializing with Kyllo. After a period of time, the relationship between Kyllo and Pandora becomes strong and Kyllo finds himself in an unexpected inclination to share his everyday stories and even deepest secrets and innermost thoughts with Pandora. The information Pandora can collect, store and perhaps share is sensitive personal information as Pandora is able to observe even the intimate relationships which Kyllo has. As a result, Pandora, with its smiley face and pleasant manner, has now social meaning for Kyllo, as if social bond has formed between them. The way Pandora behaves makes her "social". By social, I refer to the dynamic relationships between Kyllo and Pandora as social agents. With the advancement of AI techniques, Pandora is able to offer Kyllo with two-way interaction: it expresses and understands his thoughts and feelings and it detects his emotions. Consequently, it seems to be socially aware, interacts, and provides a feeling of Humanoidship and care to Kyllo. Pandora, empowered with affective computing, is capable of influencing not only Kyllo's external/physical activities but also his thoughts, feelings, and emotions.

[9] The name Pandora is an inspiration by the first human android created by Hephaestus, god of invention, on the instructions of Zeus, according to Greek Mythology. The term Pandora, I think, evokes a powerful image of the story of today's humanoid social robots as it reflects on imagination, power, good and evil. Pandora was not born; it was made for specific purposes, revealing evils of humanity.

In the US, owing or handling cannabis is illegal. Furthermore, Rule 1 of the Constitution of the US, states that: "A robot may not injure a human being or, through inaction, *allow a human being to come to harm*." (First Law of Asimov's Three Laws of Robots, emphasis added).

The local police obtained new information about Kyllo's indoors cultivation of cannabis and decided to initiate a secret investigation to find out whether the information they obtained is valid. Nevertheless, the police do not have a warrant to enter Kyllo's home, but they do have detailed information that an advanced robot operates inside the house.

Does Rule 1 establish Pandora's duty to cooperate with the police, in compliance with Rule 1, in order to limit owing or handling of drugs? On which account of accountability, responsibility, or liability should a robot cooperate autonomously with the police, without the consent of Kyllo? Could the police hack the robot in an effort to gather more information about Kyllo's activities?

This case envisages a useful starting point for the focus of this Article. The hypothetical case works towards illustrating the debates about potential privacy intrusions and the use of data, given the deeper relationship that has developed between Kyllo and Pandora.

Consequently, this Article promises to rekindle and provoke several points. The main argument is that humanizing, anthropomorphizing (ascribing human features) or zoomorphizing (ascribing animal features) HRs creates fundamental moral, societal, and legal implications. The distinctive treatment of HRs, in comparison to other technologies, by people, puts the latter in a particularly vulnerable situation vis-à-vis these robots. Such outcomes have been proven by several studies,[10] according to which people often react differently to technology that is humanistic/anthropomorphic in appearance and actions. However, the core of the problem is elsewhere: what are the legal dynamics of the relationship between HRs and individuals? Does the intervention of giant tech companies,[11] small tech companies, or States into this relationship, by whatever means, transform them (the HRs) into Trojan horses, placed at the very heart of people's private lives.

[10] See e.g., Shamsuddina, Yussof, H., Ismail, L. I., Salina, Hanapiah, F. A., and Zahari, N. I (2012) Initial Response in HRI- a Case Study on Evaluation of Child with Autism Spectrum Disorders Interacting with a HR NAO. *Procedia Engineering (IRIS)* 41:1448-55.

[11] Also called "information fiduciaries", in Balkin, J. M. (2016) Information Fiduciaries and the First Amendment. *UC Davis Law Review*. Vol. 49, No. 4.

To return to Kyllo's case, does Pandora present only challenges to Kyllo's informational privacy? Or does the presence of Pandora and her activities at Kyllo's home bring about other issues, beyond collecting, storing and sharing information about Kyllo and his home, for example issues relating to his social, psychological, or physical privacy? The following sections attempt to shed light on these issues.

In the following part, in order to prepare for an analysis of privacy benefits and harms with a wide variety of forms of HRs, I shall begin with an exploration of what a "robot" is. Furthermore, to answer the question "what can robots do and what can be done with them?" the part introduces a classification of the uses of robots, within which it then distinguishes HRs.

2. VOCABULARIES AND IDEAS

Before discussing what constitutes robotics as a field of research or robots as programmable machines by computers, it must be kept in mind, that AI and robotics are *often* used exchangeable in academic literature and in the work of practice. As an umbrella term, AI covers robotics, but robotics does not necessarily cover AI. The scope of this article is interested in the intersection between the two fields.

2.1 ROBOTICS AND ROBOTS

Robotics, the scientific field of studying robots, originates from fiends such as mechanics, computer science, cybernetics, and AI. To make the integration of robots into societies more manageable, it draws from several other disciplines including, but not limited to, physics, linguistics, neuroscience, psychology, biology, physiology, and anthropology and other sciences. Moreover, robotics as a generic term refers to automated labor-intensive processes and the replacement in an action of the human element by a robot.[12] A robot might be purely mechanic, fully autonomous or semi-autonomous, or fully controlled by humans through the so-called teleoperation.

[12] For further readings on the history and development of robots and robotics, see Calo, R (2015) Robotics and The Lessons of Cyberlaw, *103 Calif. L. Rev.* 1.

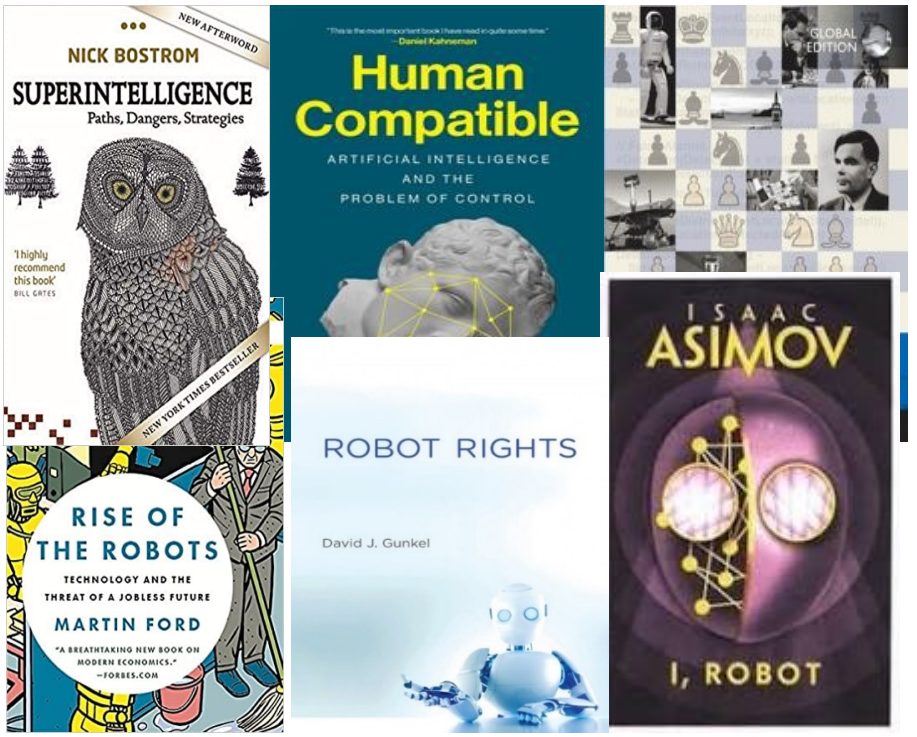

Figure 1. A sample of some popular books that have shaped the way we think about AI and robots

So, what is a robot?

Initially, the term 'robot' appeared in a play by Czech writer Karel Čapek, titled RUR, or Rossum's Universal Robots. This play also introduced the word into the English language. It comes from a Slavonic word 'robota' for 'slavery,' 'forced labour' or 'monotonous work.'[13] The term "roboticist", describing one investigating or creating robots, with their different shapes, was coined by Isaac Asimov in 1941.[14] However, reflecting the diverse literature which engages with robots, conceptualizations and definitions vary. There is not a single concise, uncontested definition of what a 'robot' is. Even professional roboticists, AI experts, authoritative scholars of science and technology do not refer to any settled, clear definition, let alone philosophers or legal theorists. Following are just a few approaches to defining a robot:

1. A robot is, according to The International Organization for Standardization, an "actuated mechanism programmable in two or

[13] Szabolcsi, R (2014) The Birth of the Term Robot. *AiMT Advances in Military Technology* Vol. 9, No. 1.

[14] Asimov, I. (1950) Liar. In *Astounding Science Fiction*, Reprinted in "I, Robot".

more axes with a degree of autonomy, moving within its environment, to perform intended tasks."[15]

2. A robot is a constructed system that displays both physical and mental agency but is not alive in the biological sense.[16]
3. A robot is a machine that senses, thinks and acts.[17]

Beyond these definitions, several scholars have attempted to define robots more comprehensively. One of the most cited accounts is that by Russell and Norvig (1995), who provide a concise categorization of robots. For them, most of today's robots are considered to be one of the following categories:

1. **Manipulator robots**. This type of robot is physically anchored to its workplace, for example, robots in a factory assembly line or on the International Space Station.
2. **Mobile robots**. These are robots that move around their environment using wheels, legs, or similar mechanisms. They have been put to use delivering food in hospitals, moving containers at loading docks, and performing other similar tasks. Examples are Unmanned Ground Vehicles (UGVs), or any robots that drive autonomously on streets, highways and off-road.
3. Robots that combine mobility with manipulation, often called **mobile manipulators**. This type of robots includes HRs that mimic the human torso.[18]

A robot is open to different definitions and interpretations. To complicate matters further, Gunkel believes, correctly, that words and their definitions related to robots are not stable; they evolve, often in ways that cannot be anticipated or controlled.[19]

Additionally, the earlier first references to robots were mainly given to the anthropomorphic appearance of the human-like robot. Usually, a robot is instructed by human programmers and performs many tasks often carried out by an individual. However, robotics is not necessarily restricted

---

[15] International Organization for Standarization, 2012. ISO 8373. Robots and robotic devices – Vocabulary. TC 184/SC 2.

[16] Richards, N. M. and Smart, W. D. (2013). How Should the Law Think About Robots? Available at *SSRN*: https://ssrn.com/abstract=2263363 or http://dx.doi.org/10.2139/ssrn.2263363 [Accessed June 6, 2020].

[17] Bekey, G. (2017) Autonomous Robots: From Biological Inspiration to Implementation and Control. *MIT Press.* p. 2

[18] Russell, S. and Norvig, P. (1995) *Artificial Intelligence: A Modern Approach.* Third ed. Alan Apt. pp. 970-973

[19] Gunkel, D. J (2018) *Robot Rights.* Massachusetts Institute of Technology. pp. 20-21

to mechatronic devices. Robotics expands further and might also comprise remotely or human controlled devices, such as drones.

Moreover, to sum up the various views of what robots are, and what can they do or what can be done with them, I define two short but concise categories:

1. Hard-task robots: This category includes robots that explore the surface of Mars, dismantle bombs in the battlefields, perform manufacturing tasks in factories.
2. This category includes robots that are deployed in private spaces such as homes. These robots can carry our various tasks including, but not limited to, cleaning and cooking.

Finally, what is a "robot" for the purposes of this Article? It should be clear that such a definition excludes certain types of software-based AI systems that exerts no ability to manipulate the physical environments. In this Paper, I make use of the view of Ryan Calo, who emphasizes the "essential qualities" – embodiment, emergence, and social valence—that characterize robots as unique technologies.[20]

2.2 SPECIFICITY OF HUMANOID ROBOTS

Humanoid robots are the most sophisticated thinking machines among the robotic applications, not only in terms of the level of intelligence but also in aesthetics. They are becoming more integrated in our society. A large community of roboticists and AI researchers believe that human-like, also called anthropomorphic, humanoid, or android, machines are to become dominant and representative of AI. What they try to do is to develop human body-like organs, faces, noses, arms, legs, and speech capabilities that could move around in a human world and serve people in their homes. Examples of these machines are sex robots, tutor robots, or elderly carer robots. Those roboticist and AI researchers see an auspicious future for these robots and believe these robots will have important role to either complement humans or to help humans fulfill their desires and needs and amplify human capabilities. This point was noted by Ishiguro in an interview. He stated that "in Japan, we are moving from industrial

[20] Calo, C (2012) Robots and Privacy. In Patrick Lin, Bekey G., Abney, K. (Eds.), *Robot Ethics: The Ethical and Social Implications of Robotics* (1st ed.) Cambridge, MA: MIT Press.

Figure 2. Photograph of Erica, Ishiguro's latest and most intelligent android.

robots – manufacturing robotics to HRics because for robots to be active in social contexts they should have a human-like appearance. When a robot has a human-like appearance, it can be easily recognized by humans because our brains recognize humans more naturally compared to other objects."[21]

Along similar lines, in another interview, Gunkel, agreeing with Ishiguro, stated that "things happening in Japan seem to be at the leading edge of social robotics because of various cultural factors that have to do with the Japanese and the pressure of their social system with regard to declining birth rate and the need for caregivers in the home. Looking at Japan, we see that things might evolve elsewhere in the world because Japan is ahead of us here in Northern America and Europe."[22] With their artificial body, they resemble the human one.[23] The unique tasks HRs can get accomplished are manifold. They can be adaptable to new environments. With their shape and appearance, sophisticated human-robot interaction, they are believed, that they are humans.

[21] *Author's interview with Ishiguro* (April 2021). The interview is available online at: Conversation with Nobel Minds https://www.youtube.com/channel/UChOFP5qUDU9Y6Y_u_bDZt4A.

[22] *Author's interview with Gunkel* (May 2021). The interview is available online at: Conversation with Nobel Minds https://www.youtube.com/channel/UChOFP5qUDU9Y6Y_u_bDZt4A

[23] Veruggio, O. G. (2008) Roboethics: Social and Ethical Implications of Robotics, in *Springer Handbook of Robotics*.

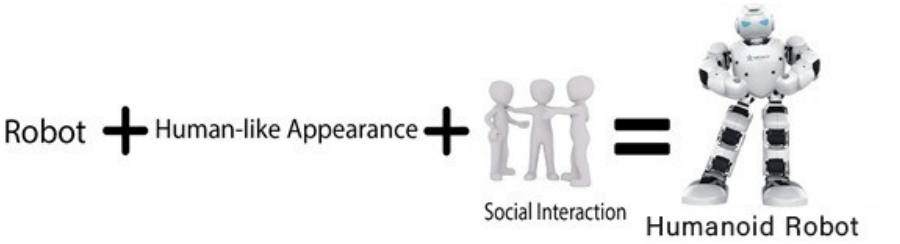

Figure 3. A humanoid robot

I make use of arguments and agree with scholars, such as Ryan Calo and Duffy, Fong et al., Breazeal, and Bartneck et al.,, who emphasizes the important of social interactivity, embodiment, emergence, and social valence—that characterize robots as unique technologies.[24]

Building on previous definitions, a HR, for the purpose of this Article, is:

> *"A virtual and physical entity supported with sensors, actuators, and mobility, human-like in appearance, and people might communicate with it in a natural social manner."*

Considering this, a HR is a combination of three main components (*see Figure 3*). The three components make it get close to humaneness.

2.3. ROBOT AND HUMANOID ROBOTS IN SOCIETY – NOW AND IN THE FUTURE

Yet, before exploring futuristic views and scenarios, it is important and helpful to review some of today's statistics about robots and their use. In other words, answering the question: "Where are the robots in today's world?". As it became evident, robots, humanoid, industrial etc., are being used and deployed in a vast array of settings and for various purposes. The International Federation of Robotics (IFR) and The International Organization for Standardization (ISO), among other, provide useful updates about topical issues regarding robots and automation and their role in society. They annually report about the average robot density in both industrial and non-industrial environments. According to IFR's latest report about the density of robots in manufacturing industry, robots "hit a new global record of 113 units per 10,000 employees. By regions, Western Europe (225 units) and the Nordic European countries (204 units) have the most

[24] Calo, (2012) Robots and Privacy. In Patrick Lin, George Bekey, Keith Abney (Eds.), *Robot Ethics: The Ethical and Social Implications of Robotics* (1st ed.) Cambridge, MA: MIT Press.

automated production, followed by North America (153 units) and South East Asia (119 units)".[25] In another IFR's report of 2020 shows "a record of 2.7 million industrial robots operating in factories around the world – an increase of 12%. Sales of new robots remain on a high level with 373,000 units shipped globally in 2019. This is 12% less compared to 2018, but still the 3rd highest sales volume ever recorded."[26] Such figures might be interesting from the perspective of social robotics as industrial robotics is important, not only, for the progress of social robotics. Kanda and Ishiguro, notable roboticists, note that Japanese companies such as Sony and Honda developed key components of socially interactive robotics.[27]

As it is not possible to list all types of humanoid social robots, because they operate, or in the process of being developed to be deployed, in so many settings including, but not limited to, healthcare, education, entertainment, assistive living, domestic or household chores. These robots continue to experience a tremendous growth in the market and are deployed in to execute various tasks. Care robots and sex robots will be discussed briefly to give an overall imagine about the use of these HRs.

Care robots, as part one type of HRs that are deployed in nursing homes and hospitals or home healthcare robots, are currently at high level in health care sector and they are increasingly being integrated for different tasks. They can support human care, e.g., in cooking and cleaning for the elderly and the younger generation.

Sex robots are used for various purposes, but they are primarily socially interactive robots and created and used for sexual and intimate purposes, such as sexual stimulation. The provide two-ways of interaction, they are

[25] The International Federation of Robotics. Available at: https://ifr.org/ifr-press-releases/news/robot-race-the-worlds-top-10-automated-countries [Accessed Feb. 28, 2021].

[26] The International Federation of Robotics. Available at: https://ifr.org/ifr-press-releases/news/record-2.7-million-robots-work-in-factories-around-the-globe [Accessed Feb. 28, 2021].

[27] Kanda, T., Ishiguro, H (2013) *Human-Robot Interaction in Social Robotics.* (1st ed.). CRC Press. Available at: https://doi.org/10.1201/b13004 [Accessed Oct. 10, 2020].

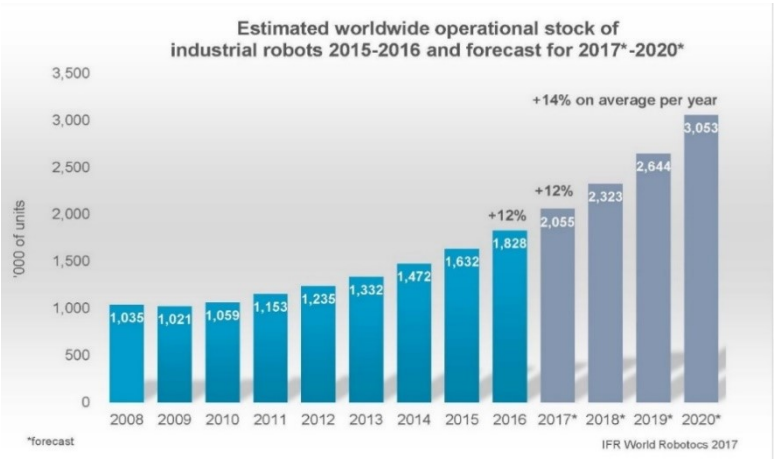

Figure 4.

equipped with cameras, speakers and microphones. For example, in addition to reasons related to lack of ability of some people (with physical disabilities, for example) to build intimate relationships with other humans, human-like features and development of AI techniques, presumably, sex HRs, as David Levy, one of the leading experts in AI argues, can be functionally autonomous, capable of learning, have physical support, and adapt to their environment.[28]

The market is not well established yet and so far, the history of social robotics indicates failures in promoting their products. One could claim that these robots suggest human-like capabilities, but this is more entertainment than practical utility beyond publicity. There have been several examples about this fact. Manufacturer Honda's iconic and most advanced HR of its time Asimo is one of them. The production of Asimo was halted in 2018.[29] One the other side, we see some promising projects such as David Hanson's most celebrated HR Sophia. Sophia is an even more extreme case of publicity seeking with little commercial possibility. Sophia, according to the website wants to "connect with humans".[30] Marketing this robot has been flourishing recently, particularly during the Pandemic.[31] Sophia was

[28] Levy, D. (2007). *Love and Sex with Robots: The Evolution of Human-Robot Relationships.* New York: Harper & Co.

[29] Honda (2019). Asimo: *The world's most advanced humanoid robot.* Available at: https://asimo.honda.com/ [Accessed April 2, 2020].

[30] Hanson Dynamics. Sophia, Hanson *Robotics' most advanced human-like robot*. Available at: https://www.hansonrobotics.com/sophia/ [Accessed April 20, 2020]

[31] Reuters (2020). *Makers of Sophia the robot plan mass rollout amid pandemic. robot.* Available at: https://www.reuters.com/article/us-hongkong-robot-idUSKBN29U03X [Accessed April 2, 2020].

granted honorary citizenship by the Kingdom of Saudi Arabia in 2017 marking a historical move. It was only in a Sci-Fi movie "Short Circuit (1986 film)", in which a non-human became a US citizen.

There are few other institutions are currently working on creating HRs such as Ishiguro's Laboratories and they generated a lot of attention. Genimoids, Erica, Telenoid, Elfoid, Hugvie, Android I are few examples.[32] In an interview, Ishiguro claimed that "I want to bring robots to life". Their marketing seems to be very successful so far. Erica for example will be the first robot lead actress in a Hollywood movie.[33] The Japanese information technology and investor giant, Softbank, has also a promising project, e.g., HRs Pepper. It's website states that Pepper is "the world's first social HR able to recognize faces and basic human emotions […] Pepper is available today for businesses and schools. Over 2,000 companies around the world have adopted Pepper as an assistant to welcome, inform and guide visitors in an innovative way."[34] Softbank robotics has also another ongoing and promising project. Its robot NAO which "is also used as an assistant by companies and healthcare centers to welcome, inform and entertain visitors." NAO (and also Pepper) are used in various fields ranging from retail to tourism, health and education and there have been 5, 000 pieces sold around the world.[35]

All in all, we should, of course, exercise caution when studying how and in what speed technological developments are headed to. At this moment we can only say these developments are unpredictable and might likely fail not only in Japan but in other countries as well. This has been noticed by so many leading scholars. Among them, Melanie Mitchell who stated in her book Artificial Intelligence: A Guide for Thinking Humans (2019), that "We humans tend to overestimate AI advances and underestimate the complexity of our own intelligence."[36] Moreover, an overview on the current advancements in AI indicates that the market of HRs

[32] Hiroshi Ishiguro Laboratories. *Robots.* Available at: http://www.geminoid.jp/en/robots.html [Accessed April 2, 2020].

[33] *Hollywood just cast a robot actress in a $70 million movie "Erica" will be the first robot lead actress.* Available at: https://futurism.com/the-byte/hollywood-cast-robot-actress-movie [Accessed April 2, 2020].

[34] *Softbank robotics. Pepper.* Available at: https://www.softbankrobotics.com/emea/en/pepper. [Accessed April 1, 2020].

[35] *Softbank robotics*. Available at: https://www.softbankrobotics.com/emea/en/company. [Accessed April 1, 2020].

[36] Mitchell, M. (2019). *"Artificial Intelligence," "The Accusation," "Frankissstein," and "Red at the Bone."* Available at: https://www.newyorker.com/magazine/2019/11/04/artificial-intelligence-the-accusation-frankissstein-and-red-at-the-bone [Accessed April 1, 2020].

in particular is expected to flourish in terms of qualitative importance and quantitative and social impact on individuals interacting with them. Not only the market, academic institutions has been occupied following up with these advancements. Recently in the beginning of 2021, Oxford launched its "Institute for Ethics in AI," which aims to "bring together world-leading philosophers and other experts in the humanities with the technical developers and users of AI in academia, business and government."[37] Stanford did similar already in 2019 by launching "The Stanford Institute for Human-Centered Artificial Intelligence (HAI)", whose goals is "The mission of HAI is to advance AI research, education, policy and practice to improve the human condition."[38]

A brief recap

It is clear that as technologies are fast evolving, the distinction between AI and robotics blur constantly. Perhaps having no absolute definition of "robot", when the AI-human-socio-cyber-physical-etc. mix is becoming so entangled and complex. Thus, AI embodied in robots, the meaning of robots might be shifted.

3. THE GENESIS AND FUTURE OF PRIVACY & THE ROLE OF HUMANOID ROBOTS

Here is a recent scenario of our fictional story:

This is Pandora. She is a perfect and most sophisticated HR. And this is Kyllo, her owner. The relationship between the two becomes also deeper and more complex, and over time Kyllo expects Pandora to know what is right and what is wrong and what is private and what is not.

Is this a veridical, an illusory or a hallucinatory experience and, accordingly, relationship? Does such a relationship enshrine privacy--sensitive sides, and if yes, which ones specifically? This is an extreme and rather a fantasized example of relationship between humans and machines. However, this scenario does not mean that it is divorced from reality.

In this part, I distinguish between relevant concepts of privacy and the legal right to privacy. The aim is to create a *Two-Pillar Structure* and analyze different clusters of privacy, already identified in the literature and on which this Article intends to build. Part of the Article's original

[37] Institute for Ethics in AI. [Accessed August 10, 2020]. https://www.schwarzmancentre.ox.ac.uk/ethicsinai.

[38] The Stanford Institute for Human-Centered Artificial Intelligence (HAI). Available at: https://hai.stanford.edu/about [Accessed August 10, 2020].

contribution lies in the *Two-Pillar Structure*. HRs have alarming privacy implications on the virtual and physical environments; thus, the *Two-Pillar Structure* examines physical and non-physical (informational) privacy. For each cluster, I will briefly but concisely indicate the main relevant legal provisions on privacy at the international level. I will mention where and in what context these clusters overlap. Although these clusters of privacy may have some overlaps and are intrinsically intertwined and often coincide, they will be looked at and analyzed individually. This is an important approach to understand the effects which HRs generate in relation to privacy. The *Two-Pillar Structure* discussion will be complemented by a rather short, *Two-Pillar Structure Plus* section. This section examines further human rights implications generated by HRs but still associated with the right to privacy.

To provide further analysis, I introduce, in the following part, how privacy, as a philosophical and legal concept, has been conceptualized. While I consider the various philosophical and legal definitions of privacy within my initial discussions and which I find them constructive, I am not concerned with these definitions *per se*. Rather, what is important is what specific elements of privacy are impacted by HRs and in what context(s). In any event, although the term is conceptualized mostly by, or, at least, in conversations with, prominent philosophers on the field of privacy, such as John Locke and Immanuel Kant, my approach is human rights-focused particularly upon the information as a substantial and constitutive element of the right to private life. I trace the concept of privacy by adopting a non-reductionist account of the concept. That means that privacy is valuable in itself, and its value and importance are not derived from other considerations.[39] The benefits of this approach are two-fold; (a) privacy is not conflated with data-protection, but the former's understanding paves the way for conceptualizing the latter, and (b) privacy helps to form a privacy-sensitive framework for a responsible and human-rights based development of HRs.

3.1 PRIVACY AS A CONTROVERSIAL LEGAL AND PHILOSOPHICAL CONCEPT

In this section, the idea is to find a philosophical answer to the question 'What is Privacy?'. I imagine that this step is crucial if one wants to build

[39] See for example Rössler, B (2004) The *Value of Privacy*. Polity; 1st ed.

a point of departure for questioning a legal definition of privacy and to investigate how courts and legislature employ the concept to identify intrusions upon the right to privacy. Next, it considers some debates within the discussions of privacy. This is important because, although, the term "privacy" is universally known, it is often seen as a disarray and unstable concept. It does not have a universal definition.[40] Having said that, the upcoming conversations provide sophisticated insights into understanding what constitutes privacy. They also lead us to connect yesterday's with today's image of privacy. Both the former and the latter are based dominantly on a Western liberal ideology.

From the point of view of social and other sphere domains of life, privacy is a curious value. Younger and older generations *in general*, even in the current era of digital information, are still careful about who access to their private personal information.[41] This is particularly true in the information society in which information, as many argue, *inter alia*, Floridi (2011) (cited in Richardson 2016, 146), is related to "who we are", as autonomous persons.[42] What is interesting in the dominant discussions on privacy is that, although we are mindful of what is and is not private for us (think of the public debates following Edward Snowden's revelations),[43] privacy is still a studied topic in the literature. This is surprising, since privacy (or secrecy) is an extremely well-investigated field in legal scholarship. Although it is frequently invoked in political and legal, discussions, and more than anything else in relation to our life in the digital age, the concept of privacy is in its core philosophical. The concept tells us about human nature and human needs to engage in activities that are exercised in a private sphere. Perhaps, the earliest text that directly discusses the distinction between the personal and public spheres is the first book of Aristotle's *Politics*. In addition to outlining the distinction in clear

[40] See various opinions on the definition of privacy in, for example, Nissenbaum, H. (2010) *Privacy In Context: Technology, Policy, And The Integrity Of Social Life.* Stanford University Press.

[41] Van den Hoven, J, Blaauw, M. Wolter, P. and Warnier, M (2020). *Privacy and Information Technology, The Stanford Encyclopedia of Philosophy,* Edward N. Zalta (ed.),. https://plato.stanford.edu/archives/sum2020/entries/it-privacy.

[42] Richardson, J. (2016) *Law and the Philosophy of Privacy*. Routledge. (1st edit) p. 146. See also Balkin, Jack M., Information Power: The Information Society from an Antihumanist Perspective (2006). Available at *SSRN*: https://ssrn.com/abstract=1648624 or http://dx.doi.org/10.2139/ssrn.1648624.

[43] See some key discussions on privacy, following Snowden's revelation Lyon, D. (2013) *Surveillance, Snowden and Big Data. Big Data & Society.* Rotenberg, M (2015). *Privacy in the Modern Age: The Search for Solutions*. Scott, J. (Edit), Horwitz, J. (Editor). The New Press.

terms, it is still helpful by providing a sophisticated understanding of "privacy" and a useful starting point, since it has consistently performed as a point of reference for later debates on privacy. Aristotle makes a distinction between the *oikos* – private family life or best translated as household – as a distinct sphere of life, and the *polis* – the public realm of the political community. The former is, for Aristotle, the basic unit of the latter and, in addition, its existence is necessarily determined by the latter. Aristotle states that:

> "*.....Thus also the city-state is prior in nature to the household and to each of us individually…...It is clear therefore that the state is also prior by nature to the individual; for if each individual when separate is not self-sufficient, he must be related to the whole state as other parts are to their whole, while a man who is incapable of entering into partnership, or who is so self--sufficing that he has no need to do so, is no part of a state, so that he must be either a lower animal or a god.*"[44]

In various academic arenas, privacy is believed to be a very complex and contextual concept. Which means in certain contexts people might be concerned about their privacy but in others they might not. It is also believed that privacy is of the concepts that have not, and perhaps will never capture a universal recognition in terms of definition or understanding. This is also linked to the speed of technological development with affects various social, economic, and legal domains in our society. The rapid evolution of Information and Communication Technologies (hereinafter ICT), AI, robotics, and other technologies make it difficult to anticipate with certainty their impacts on our societies, including the social and legal interests of individuals. Consequently, it is also difficult to specify precisely and non-controversially the contours of the very concept of privacy. The absence of a definition or common understanding does and should not, however, refrain us from offering a reasonably solid conceptualization of privacy for the purposes of a legally binding understanding of the concept.

[44] Aristotle (1944) in 23 Volumes, Vol. 21, translated by H. Rackham. Cambridge, MA, Harvard University Press; London, William Heinemann Ltd. 1944. 1.1253a.

In the age of the digital world and rapid technological transformation, privacy, both as a value and a human right, has moved to the center of attention of academic scholarship that focuses on legal and social science. Many academic works on privacy have so far followed the "traditional method".[45] By applying this method, they tried to articulate the features that separate privacy from other values. They tried to see what is unique about privacy and next how to characterize it. Some of them looked "for sets of necessary and sufficient elements that single out privacy as unique with regard to other concepts".[46] However, this approach is arguably not the most successful. Perhaps because privacy encompasses a vast range of values and principles, e.g., freedom of thought, right to personality, control of information, solitude in one's home and private spaces.[47]

Several philosophers, political scientists, and legal theorists have attempted to define the concept of privacy. Solove (2004) observes that they have notoriously failed in reaching a satisfying common ground.[48] Also, Gutwirth (2002) notes that privacy is under-investigated and it "remains out of the grasp of every academic chasing it." He continues stating that privacy "still finds a way to remain elusive."[49] In a similar manner, Cohen (2013), claims that "privacy has an image problem" …and that "the recent additions of social media, mobile platforms, cloud computing, and AI--driven data mining now threaten to tip the scales entirely, placing privacy in permanent opposition to the progress of knowledge."[50] Furthermore, Helen Nissenbaum is of the idea that argues privacy, as a human value, is identified and understood through "contextual integrity". Nissenbaum refers to the idea that sharing of information that is not the problem *per se*. For her, the problem is by sharing of information outside of "socially agreed contextual boundaries." In this sense, people who complain about "the violation of their privacy generally understand that sharing

[45] See for example Cannataci, J. A. (2016) The *Individual and Privacy*, Routledge, V.1

[46] See generally, Solove, D. J (2002). Conceptualizing privacy. *Calif. L. Rev.*

[47] Article 8 - Right to respect for private and family life, home and correspondence - of the ECHR jurisprudence covers various aspects of privacy. See Council of Europe's Guide on Article 8 of the European Convention on Human Rights (31 August 2020). https://www.echr.coe.int/documents/guide_art_8_eng.pdf.

[48] Solove, D. J. (2004) The *Digital Person Technology and Privacy in the Information Age.* NYU press. P. 2.

[49] Gutwirth, S (2002) *Privacy and the information age*. Lanham, MD: Rowman & Littlefield. p 30

[50] Cohen, J. E. (2013) What Privacy is for, *126 HARV. L. REV.* 1904, 1907

of information is crucial to social life and that their real concern is the inappropriate and improper sharing of information".[51]

Some scholars have developed "essentialist" or "unitary" theories of privacy. [52] They attempted to identify the core of privacy and how privacy, as a single concept, is different from other concepts. While on the other hand, others have adopted a "reductionist" approach. [53] With this approach, they attempted to use privacy as an instrument to discover other human rights and values such as human liberty and autonomy.

Other scholars refuted the way that privacy is defined through a "conceptual core".[54] They hold that privacy can be identified by "developing pluralistic accounts of privacy interests or forms of intrusion to identify "cluster[s] of problems" that share family resemblances.[55]

Privacy and Technology

Various academic literature holds that the concept of privacy is about responding to the developments that come along, essentially, ICT, and other types of technologies. Looking at the intersection between privacy and technology, scholars started already in 1890s to look at the impacts of technology on privacy. The emergence of portable photography and its use in our society kicked out the discussions on this relationship. Historical legal texts trace the expression "right to privacy" to Samuel Warren and Louis Brandeis.[56] Warren and Brandeis summarized privacy as the right of the individual to "be let alone" and expanded the notion of data protection beyond the fundamental right to privacy. "The right to be let alone" late became the most definition referred to when discussing privacy and the right to privacy in legal texts. It could be argued also that there is no single legal text on privacy that does not mention Warren and Brandeis's summary of the right to privacy.

Back time when Warren and Brandeis wrote their opinions on privacy, the technology of photography was used to collect data and information about individuals without their consent, and they phrased privacy not as a philosophical concept only but also, legally as the "right to be let alone"[57]

---

[51] Nissenbaum, H (2004) Privacy as Contextual Integrity, *Washington Law Review*, 79:1, 101-139.

[52] Solove, D. J. (2002) Perspectives in privacy in information privacy law. *90 Cal. L. REV.* 1087. p. 44.

[53] Solove (2014), 4, at 14.

[54] Thomson, J. J. (1975) The Right to Privacy, *4 PHIL. & PUB. AFF.* 295, 312-13.

[55] Cohen, 3, at 1907-08.

[56] Warren, S. and Brandeis, L. D. (1890) The Right to Privacy, *Harvard Law Review.*

[57] I*bid,* 43, at 193.

which courts should understand privacy as an individual's freedom to solitude. This in turn inspired significant interest in and attention to privacy not only in the US legal system but internationally as well.

Additionally, in a famous technology-privacy--related case, *Olmstead v. United States* (1928), Brandeis called for establishing and safeguarding a right to privacy, describing such a right as "the most comprehensive of rights and the right most valued by civilized men."[58] In addition to his Article, several scholars argue that Brandeis's dissent in *Olmstead* undoubtedly was fundamental in the making of the law of privacy, both domestically and internationally, as hailed by a multitude of scholars and on subsequent theories of privacy. However, we might be misled if we insist that the formulation of privacy as a "right to be let alone" is sufficient. Martin Scheinin offers an opinion on it, noting that the phrase merely describes an attribute of privacy. For him, an understanding of privacy as merely "being let alone" fails to provide a comprehensive understanding of what privacy really is. For him, the right to privacy is largely about "making a choice". Scheinin asserts that the right to privacy is about "the ability to preserve the private sphere" and that "it depends heavily on the attributes of individual's social environment." He would claim that privacy involves one's relationship to society; in a world without others, claiming that one needs privacy would not make much sense.[59]

I tend to favor the idea that even when we are exercising our right to privacy, we are somehow and in one way or another connected to the outer world. We are influenced by others and our privacy is defined by our social relationships. To put it in Aristotelian words, we are, as social animals, caught in a natural web of necessity.

In a similar way to Scheinin's interpretation of privacy, William Prosser noted, in his famous California Law Review article 'Privacy', that Warren and Brandeis saw privacy as "public disclosure of embarrassing private facts about the plaintiff."[60] He disapproved and criticized this narrow vision of privacy rights and claimed that these rights must go beyond physical intrusion. In his own words, he divided privacy rights into four categories: "Intrusion upon a person's seclusion or solitude, or into his private affairs;

---

[58] *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

[59] *Ibid, Scheinin.* Scheinin, M. (2009) *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism,* A/HRC/13/37.

[60] Prosser, L. W., (1960) Privacy, *California Law Review* 48 383, 388–89.

Publicity placing one in a false light in the public eye; and Appropriation of one's likeness for the advantage of another."

Finally, one can claim that Louis Brandeis and Alan Westin provided the most important understanding of privacy. This understanding influenced the way various jurisdictions in various countries see privacy. Many claims also that every country adopted their understanding of privacy. Moreover, Westin's 1967 classic Privacy and Freedom enriched very significantly the philosophical and legal groundwork for the academic discussions on the intersection between technology and privacy as well as personal freedom as an integral element of privacy and is considered a foundational text in the field of privacy law.[61] The US Supreme Court went along with Westin's views stating that "understanding privacy encompass the individual's control of information concerning his or her person" in one of it is famous judgments.[62]

3.2 TYPOLOGY OF PRIVACY: THE TWO-PILLAR STRUCTURE AND TWO-PILLAR STRUCTURE PLUS

In this sub-section, my aim is to discuss important academic literature on privacy. Whereas it is not possible (and also not of present interest, considering this Article's limited scope) to discuss many of the privacy-related existing classificatory academic works. Believing that this will assist in making sense of how such classifications can become relevant to the topic at hand.

3.2.1 CLUSTER ONE: NON-PHYSICAL (INFORMATION) PRIVACY

3.2.1.1 SUB-TYPE: INFORMATION PRIVACY

The informational dimension of privacy is strongly and most directly affected by humanoid robots (HRs). There are some academic claims which states that it is all about information and how our information is impacted.

Natural human-machine (robots called machines also) interaction is an emerging field on a large scale, particularly regarding HRs. These robots can execute various tasks, from controlling other smart devices at home to reporting about the weather, news, appointments, supporting music streaming and sending notifications to family members in case of an emergency. To provide this vast array of functionalities, robots, be it HS or other types, are empowered with different technological equipment

[61] Westin, A. F (1968) Privacy and Freedom, *25 Wash. & Lee L. Rev.* 166.

[62] DOJ v. Reporters Comm. for Free Press, 489 U.S. 749 (1989).

such as sensors and cameras. These robots use supporting cloud services and connected social media platforms. As a result, these robots inevitably effect and relate to privacy.[63] Similar to mobile phones or computers, HS are connected with the clouds to which the transfer data of the environments they are serving, or they are installed at. These set of data is about general and private information that are related to the environments and the individuals interacting with them. From the type of music and movies to the type of product purchase these individuals prefer.

Consequently, the relevance of HRs to the discussion of information privacy is clear. In light of the revelations regarding mass surveillance, interception and data collection, the General Assembly of the United Nations recognized the human rights relevance to digital privacy by adopting the Resolution 68/167 titled "The right to privacy in the digital age".[64] In that resolution, the General Assembly affirmed that "the rights held by people offline must also be protected online" and called upon all States to respect and protect the right to privacy in digital communication. The resolution reaffirmed the human right to privacy, according to which "no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, and the right to the protection of the law against such interference."[65]

For the purpose of this Article, I consider that the right to privacy in the Declaration and the General Assembly Resolution has an informational aspect.

3.2.1.2 SUB-TYPE: PRIVACY OF COMMUNICATION

Humanoid robots (HRs), empowered by Cyber-Physical systems (CPSs), are able to impact not only the virtual but also the physical sphere. Consequently, HRs can create a disquieting impact on the privacy of communication. No wonder that the right to privacy encompasses privacy of communication which refers to individuals' anonymity and confidentiality. It is not necessarily HRs violate this right, they could empower it.

---

[63] For further discussion of the human rights implications presented by AI and robotics, see Ford, M (2015) *Rise of the robots: Technology and the threat of a jobless future.* Basic Books, New York.

[64] The right to privacy in the digital age - Report of the Office of the United Nations High Commissioner for Human Rights. Resolution 68/167. (2018).

[65] *Ibid. The* right to privacy in the digital age - Report of the Office of the United Nations High Commissioner for Human Rights. Resolution 68/167. (2018).

Individuals who create intimate relationships with their HRs (sex robots are the most obvious example) and share sensitive information with them, put themselves in a particularly vulnerable situation vis-à-vis the HRs (by being hacked or damaged remotely, for example). It might be argued that the states have a higher responsibility to protect individuals because of the particular vulnerability that is involved. This type of privacy can be claimed under Article 8 of the UDHR.

3.2.1.3 SUB-TYPE: PRIVACY OF BEHAVIOR AND ACTION

The right to privacy is strongly encompassed different dimensions of privacy. For example, it is related to individuals' ability to resist "behavioral manipulation", "protection of sensitive information", "protection of personal matters such as religious and sexual practices", "autonomy and self-determination", to name a few. Being independent from others (individuals, state apparatus, tech companies…etc.) contributes to "the development and exercise of autonomy and freedom in thought and action".[66]

HRs, through their use for anticipating and guiding behavior and action enabled by detection of emotions (affective computing), and for assessing individuals, may negatively affect an individuals' right to make independent decisions. Clarke (1979) notes that "there is a special element included in the privacy of personal behavior, whereby people have a right to private space to carry out particular activities."[67] In this regard, DeCew notes that privacy "is not merely limited to control over information. Our ability to control both information and access to us allows us to control our relationships with others. Hence privacy is also connected to our behavior and activities."[68] Although not referring specifically to robots or HRs, Lawrence Lessig argues that "combinations of computer hardware and software could constrain and direct human behavior".[69]

For our purpose, I consider that the right to privacy includes a set of human behavior that are essential part of private life protected. Of course, this set of human behavior requires protection from any violation.

---

[66] Nissenbaum, H (2010) *Privacy in Context: Technology, Policy and the Integrity of Social Life.* Stanford CA: Stanford University Press.

[67] Clarke, R (1979). *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*. http://www.rogerclarke.com/DV/Intro.html.

[68] Wagner, J. D. (2015) The Feminist Critique of Privacy: Past Arguments and New Social Understandings, in *Social Dimensions of Privacy: Interdisciplinary Perspectives.* (Beate Roessler & Dorota Mokrosinska eds. 3.4.

[69] Lessig, L (1999) *Code: And Other Laws of Cyberspace* .1st ed. pp. 88–89.

3.2.1.4 SUB-TYPE: PRIVACY OF THOUGHTS AND FEELINGS

Humanoid robots (HRs) influence individuals' privacy of thoughts and feelings. This is true because HRs are engaged in digital and physical manifestations. Concerning this specific discussion, Finn et al., in their *typology of privacy* (2013) note that "the privacy of thoughts and feelings can be distinguished from the privacy of the person, in the same way that the mind can be distinguished from the body."[70]

HRs, supported by latest technological techniques such as algorithms, are declared, as several studied mentioned previously suggest, to be more humanistic. In other words, they are similar to humans in terms of appearance and actions. This has been declared also by one of the leading scholars in human robotics such as Hiroshi Ishiguro.[71]

The way HRs look and behave may eventually make it possible (or at least easier in comparison to other non-human like technologies) to access individuals' thoughts and feelings.[72] In the view of Finn et al., privacy of thoughts and feelings "protects what is perhaps the least controversial, most consistent and unwavering dimension of privacy, the individual thoughts and feelings which until now were almost entirely imperceptible to others unless individuals chose to share them".[73]

3.2.2 CLUSTER TWO: PHYSICAL PRIVACY

3.2.2.1 SUB-TYPE: PHYSICAL PRIVACY

Another dimension of privacy worth mentioning is physical privacy. Regarding this one, the physical embodiment of HRs is what makes them a unique type of technology compared to, for example, merely virtual technologies such as Chatbots. Because of the cumulative effect of their hardware, operating system, and software, they can interact with their environment and have physical impacts on physical spaces. In addition to this, Calo notes that, "their *programmability* and *interactivity* and their ability to physically reach out into the world in an autonomous fashion enable

---

[70] Finn, R. L., Wright, D. and Friedewald, M. (2013). "Seven types of privacy", in Gutwirth, S. Leenes, R., De Hert, P. and Poullet, Y. (eds.), *European Data Protection: Coming of Age,* Springer, Dordrecht, p 4.

[71] *Author's interview with Ishiguro* (Feb 8, 2021). The interview is available online at the YouTube channel: "Conversation with Nobel Minds" https://www.youtube.com/channel/UChOFP5qUDU9Y6Y_u_bDZt4A [Accessed on 18 May 2020].

[72] Subramanian, R (2017) Emergent AI, Social Robots and the Law: Security, Privacy and Policy Issues. *Journal of International Technology and Information Management* ,Volume 26| Issue 3, 97

[73] *Ibid,* Finn et al, 18.

robots to survey individuals across places and gain access to personal rooms, which was impossible at this scale before".[74]

Scholars often make a clear distinction between physical and non--physical privacy and consider them as distinct forms of privacy. Here I support the conclusion of Blok and others who argue that "informational privacy should not be put alongside relational, spatial, and communicational privacy, but rather should be seen as the other side of the coin." All (more or less) "physical types of privacy lie on one side, and informational privacy on the other".[75] I reiterate that in the case of HRs, equipped with technological sophistication, the distinction between these two kinds of privacy may be far less important to the privacy protection than it seemed before, because the boundaries between these two kinds will increasingly blur the more technological innovation advances.

3.2.2.2 SUB-TYPE: PRIVACY OF LOCATION AND SPACE

"*Privacy of location and space"* refers to the idea that individuals should be free in physical spaces with the freedom of navigating without being watched or monitored. This type of privacy is known also as "Spatial privacy". Spatial privacy may be easily perceived as one of the cornerstones of privacy protection, since it points directly to individuals' *right to solitude and a right to privacy in spaces*.[76] Home is here a most characteristic notion associated with this type of privacy. For example, the ECtHR, in *Niemietz v Germany*, considered "business premises" as a space that sometimes also falls under the notion of "home", if what happens there is linked to someone's private life.[77] Many of the international treaties, e.g., UDHR, considered in this article protect the home, but one might also argue that they protect all other places, e.g. a car or an office, to name a few.[78] These physical places are where individuals enjoyed their privacy.

In addition to the ability to move around rooms, kitchens and other small private spaces, HRs may come with programming that enhances their capacity for stealth movement.[79] A potential privacy intrusion here may involve a HR invading the privacy of a person's intimate life. This can occur,

[74] Calo, M, R (2014) Robots and Privacy," in *Robot Ethics: The Ethical and Social Implications of Robotics* (Patrick Lin, George Bekey, and Keith Abney, eds.) 4.

[75] Bok, S. (1983) *Secrets: On the Ethics of Concealment and Revelation* 10-11. Oxford University Press, cited in Koops, B. K, Newell, B. N., Timan, T. Škorvánek, I. Chokrevsk, T. Masa G. (2017) A *Typology of Privacy.*

[76] Clarke *ibid.*

[77] See ECtHR 16 December 1992, *Niemietz v Germany*, App. 13710/88.

[78] ECHR (art. 8), art. 12 of the UDHR. See also EU (art. 7). For general discussion on this issue, see Wright, F & Friedewald, 4.

for example, when a HR with cameras, looks through a bedroom window and taking photographs or recording voices. This scenario can happen where a HR is either acting autonomously or being remotely controlled. There are clear indications of potential overlaps with other aspects of privacy, for example with the informational privacy of people in places being scanned.

This type of privacy links strongly to social privacy (to be discussed right below). The concept of physical space is seen part of a community or a family. Westin states that this type of private space (or, in his own term, "intimate zone") is not limited to one person or two persons or to an intimate relationship. In his understanding, the concept refers to the intimate relationship of an individual with his or her family, friends or neighbors.[80]

3.2.2.3 SUB-TYPE: SOCIAL PRIVACY

The integration of humanoid robots (HRs) in the private spheres might affect the person's right to social life/social privacy. Social privacy is also termed "private social life" or "privacy of association" in different legal texts. In this regard, Article 8 of the ECHR - Right to respect for private and family life, home and correspondence - protects the right to identity and personal development, which includes the right to establish and develop relationships with other human beings and the outside world. This fact has been relevant in *Munjaz v. United Kingdom*, in which the ECtHR stated that the right to privacy also protects "the right to establish and develop relationships with other human beings and the outside world."[81] In another important decision, the ECtHR stated that, "[r]espect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings.[82]

3.3 TWO-PILLAR STRUCTURE PLUS

Along the *Two-Pillar Structure of* Physical and Non-Physical (information) Privacy discussed so far, one can position other relevant objectives that attached to privacy in the context of HRs. My aim is to demonstrate that

[79] Calo, R (2014) Robots and Privacy," in *Robot Ethics: The Ethical and Social Implications of Robotics* (Patrick Lin, Bekey, G and Keith Abney, eds.) 4.

[80] Westin, A, F (1968) Privacy and Freedom. *25 Wash. & Lee L. Rev.* 166, https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20.

[81] *Munjaz v. United Kingdom*, 30 Eur. Ct. H.R. (2012)

[82] *Niemietz v. Germany*, 10 Eur. Ct. H.R. (1992).

an enhanced *Two-Pillar Structure Plus* enables observing further implications to human rights as generated by HRs.[83]

The right to reputation is an important privacy aspect that is potentially undermined by HRs. Cloud computing enables HRs to interact with their surroundings and interact with individuals in private spaces. By facilitating the distribution of data, HRs can facilitate the spread of information which consequently generates impacts, positive or negative, o the reputation of individuals. Looking at human rights treaties, one can see the right to reputation being recognized as an important part of privacy and its protection.

Again, this should not be seen as an exclusive privacy-related list of rights and values that are relevant in the context of the deployment of HRs. Future work demands an extension of this section to consider, for instance, the right to personal autonomy, the right to the security of the person, the right to personality and so forth.

4. CONCLUDING REMARKS

Privacy is more than one single idea, it is multifaced concept. The Article attempted to demonstrate that privacy as a multidimensional concept that matters to older and younger generations. The Article also suggested that this multidimensionality is useful to evaluate the impacts of HRs on individuals. The case study discussion above demonstrated the potential impact of HRs potentially upon different types of privacy. The Article argued that it might, at some point in the future, challenge the very traditional physical and non--physical dimensions of privacy and the current list of clusters must always be ready to expand as, it seems, new technologies, e.g., HRs, emerge and will constantly challenge privacy.

To analyze these distinctive privacy challenges generated by HRs, the Article provided various theoretical perspectives relevant to privacy and human-machine interaction. It is worth noting, however, that as innovation in robotics proceeds, the categorization of the various dimensions of privacy

[83] In a relevant matter, the European Commission's *Ethics Guidelines for Trustworthy AI*, for instance, accord "a foundational role to human rights law in the age of AI. The Guidelines support an approach to AI ethics based on the fundamental rights enshrined in the EU Treaties, the EU Charter and international human rights law. Respect for fundamental rights, within a framework of democracy and the rule of law, provides the most promising foundation for identifying abstract ethical principles and values, which can be operationalized in the context of AI." European Commission 2019, 9.

presented does not necessarily provide the only comprehensive and adequate framework of privacy.

Lastly, the Article contended that new and emerging technologies, particularly HRs with their cumulative effect of hardware (human-like appearance) and software, have introduced novel privacy threats. I also think that the *Two-Pillar Structure* and *Two-Pillar Structure Plus* are sufficiently flexible to accommodate potential new developments that are likely to take place in the rapidly evolving field of technology.

ACKNOWLEDGEMENT

This paper is a contribution to the Cyberspace conference in Brno, Czech Republic and it is a part of my doctoral research project I pursue at the European University Institute in Florence, Italy. I would like to thank individuals working for the Masaryk University Journal of Law and Technology, including the editor Jakub Harašta for giving me the opportunity to present my doctoral research at the conference and for publishing this paper.

Many wonderful people have been so generous to contribute to this paper and to my doctoral research project in general. I have benefited a lot from valuable reflections made by Prof. Giovanni Sartor (EUI/Uni. Of Bologna), Prof. Marc Rotenberg (Georgetown Uni./CAIDP), Prof. Ben Shneiderman (Uni. Of Maryland) Prof. David Gunkel (Northern Illinois Uni.) Prof. Sofia Ranchordas (Uni. Groningen), Dr. Bethany Shiner (Uni. Of Oxford/Middlesex), judge George Aeon, Dr. Mikko Häkkinen (Laurea), and Isabele Rodrigues (UFPE).

LIST OF REFERENCES

[1] Allen, L, A (2011) *Unpopular Privacy: What Must We Hide?* New York: Oxford University Press.

[2] *Aristotle (1944) in 23 Volumes, Vol. 21*, translated by H. Rackham. Cambridge, MA, Harvard University Press; London, William Heinemann Ltd.

[3] Asimov, I (1950) Liar. In *Astounding Science Fiction*, Reprinted in "I, Robot".

[4] Balkin, J. M. (2016) Information Fiduciaries and the First Amendment. *UC Davis Law Review.* Vol. 49, No. 4.

[5] Bekey, G (2017) *Autonomous Robots: From Biological Inspiration to Implementation and Control.* Paperback.

[6] Bryson, J. J (2009) Robots should be slaves. *Artificial Models of Natural Intelligence University of Bath*, BA2 7AY, United Kingdom.

[7] Calo, R (2012) Robots and Privacy. In Patrick Lin, George Bekey, Keith Abney (Eds.), *Robot Ethics: The Ethical and Social Implications of Robotics* (1st ed.) Cambridge, MA: MIT Press.

[8] Calo, R (2014) Robots and Privacy, in *Robot Ethics: The Ethical and Social Implications of Robotics.* Patrick Lin, Bekey, G and Keith Abney, eds.

[9] Calo, R (2015) Robotics and The Lessons Of Cyberlaw, 103 *Calif. L. Rev.* 1.

[10] Cannataci, J. A. (2016) *The Individual and Privacy,* Routledge, V.1.

[11] Cerka, P. et al, (2015) Liability For Damages Caused By AI, *Computer Law &Security Review.*

[12] Cohen, J. E. (2013) What Privacy is for, 126 *HARV. L. REV.* 1904, 1907.

[13] Darling, K (2012). *Extending legal protection to social robots: The effects of anthropomorphism, empathy and violent behavior towards robotic objects.*

[14] Fong, T., Nourbakhsh, I., and Dautenhahn, K (2002) A survey of socially interactive robots. *Robotics and autonomous systems,* 42, no. 3-4.

[15] Fosch-Villaronga. E., Millar, C. (2018) Cloud Robotics Law and Regulations, *Challenges in the Governance of Complex and Dynamic Cyber-Physical Ecosystems.*

[16] Koops, B. K, Di Carlo, A. Nocco, L. Cassamassima, V. Elettra, S (2913) Robotic technologies and fundamental rights. *International Journal of Technoethics.*

[17] Gavison, R (1980) Privacy and the Limits of Law, 89 *YALE L.J.*

[18] Gunkel, D. J (2018) *Robot Rights.* Massachusetts Institute Of Technology.

[19] Gutwirth, S (2002) *Privacy and the information age* (Lanham, MD: Rowman & Littlefield, 30.

[20] Lessig, L (1999) *Code: And Other Laws of Cyberspace* 1st ed.

[21] Minsky, M (1969) *Semantic information processing*. Cambridge, MA: MIT Press.

[22] Nissenbaum, H (2004) Privacy as Contextual Integrity, *Washington Law Review,* 79:1.

[23] Nissenbaum, H (2010) *Privacy in Context: Technology, Policy and the Integrity of Social Life.* Stanford CA: Stanford University Press.

[24] Richardson, J. *Law and the Philosophy of Law.* Routledge. 2016.

[25] Prosser, L. W., (1960) Privacy. *California Law Review.*

[26] Richards, N. M., Smart, W. D (2013) *How Should the Law Think About Robots?*

[27] Rössler, B (2004) *The Value of Privacy.* Polity; 1st ed.

[28] Sartor, G. (2017). Human Rights and Information Technologies. *The Oxford Handbook of Law, Regulation and Technology.*

[29] Scheinin, M. (2009) *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/13/37.*

[30] Snow, C. P (2993) *The two cultures: and a second look*. Cambridge Univ. Press, Cambridge.

[31] Stuart, R., and Norvig, P. (1995) *Artificial Intelligence: A Modern Approach.*

[32] Subramanian, R (2017) Emergent AI, Social Robots and the Law: Security, Privacy and Policy Issues. *Journal of International Technology and Information Management.*

[33] Syamimi, S., Yussof, H., Ismail, L. I., Mohamed, S., Hanapiah, F. A., and Zaharid, N. I (2012) Initial Response in HRI- a Case Study on Evaluation of Child with Autism Spectrum Disorders Interacting with a Humanoid Robot NAO. *Procedia Engineering (IRIS).*

[34] Szabolcsi, R (2014) The Birth of the Term Robot. *AiMT Advances in Military Technology* Vol. 9, No. 1.

[35] Turing, A. M. (1950) Computing Machinery and Intelligence, *Mind, New Series*, Vol. 59, No. 236.

[36] Wagner, J. DeCew (2015) The Feminist Critique of Privacy: Past Arguments and New Social Understandings, in Social Dimensions Of Privacy: *Interdisciplinary Perspectives.* (Beate Roessler & Dorota Mokrosinska eds.).

[37] Warren, S. and Louis D. Brandeis, L. D. (1890) The Right to Privacy, *Harvard Law Review 4.*

[38] Westin, A. F (1968) Privacy And Freedom, *25 Wash. & Lee L. Rev.*

[39] William, R (1999) *The International Dictionary of AI*. The Glenlake Publishing Company.

DOI 10.5817/MUJLT2021-2-6

AI-BASED LEGAL TECHNOLOGY: A CRITICAL ASSESSMENT OF THE CURRENT USE OF ARTIFICIAL INTELLIGENCE IN LEGAL PRACTICE

by

JANA SOUKUPOVÁ [*]

In recent years, disruptive legal technology has been on the rise. Currently, several AI-based tools are being deployed across the legal field, including the judiciary. Although many of these innovative tools claim to make the legal profession more efficient and justice more accessible, we could have seen several critical voices against their use and even attempts to ban these services. This article deals with the use of artificial intelligence in legal technology and offers a critical reflection on the current state of the art. As much as artificial intelligence proved that it could improve the legal profession, there are still some underlying risks connected to the technology itself, which may deem its use disturbing.

KEY WORDS

Legaltech, Legal Technology, Artificial Intelligence, Provision of Legal Services, Robojudge

1. INTRODUCTION

In the past years, the use of disruptive technologies has found its way into the legal profession. Legal technology, or shortly "legaltech", refers to implementing various innovative technologies in the legal profession.[1] Claims about better, cheaper, and faster services have become the leading marketing claims of many such services. These technological improvements

[*] soukupovaj@prf.cuni.cz, Ph.D. student at Centre for Legal Skills, Charles University, Faculty of Law, Prague, Czech Republic.

[1] Corrales, M., Fenwick, M., Haapio H. and Vermeulen, E. (2019) Tomorrow's Lawyer Today? Platform-Driven LegalTech, Smart Contracts & the New World of Legal Design. *Journal of Internet Law,* 22 (10), p. 6.

did not only affect the private sector of legal services but have found their way into the field of the judiciary in some jurisdictions. This can be illustrated by an Estonian project, which aims to develop artificial intelligence (AI) software that would decide certain claims[2] or by the infamous COMPAS software used in the United States to calculate the possibility of recidivism.[3] The market currently offers many software tools whose aim is to improve the quality and effectiveness of the provision of legal services while using some of the presently popular technologies such as blockchain or AI. Although the former surprisingly found its use in areas such as a notary[4], the latter has become popular across all legal fields. As a result, we can see many tools based on artificial intelligence whose aim is to help lawyers with drafting contracts, legal research, or perform due diligence. For example, Kira Systems provides a software based on machine learning called Kira which is designed to extract data, clauses and other provisions from documents.[5] Likewise, Casetext developed an AI research tool called CARA A.I. that reviews cases included in legal documents..[6] Simultaneously, there are attempts to develop a software capable of predicting the court's decisions or tools to assist the judges with decisions on the cases. An example of this is a product offered by Lex Machina which works as a legal analytics tool for predicting litigation outcomes.[7] Finally, there has been a rise in services that are aimed at the general public to provide them with better access to justice such as LegalZoom or DoNotPay.[8]

As a result of these technological opportunities, AI-based legaltech has a great potential of structurally changing all aspects of the law – starting

---

[2] Niller, E. *Can AI Be a Fair Judge in Court? Estonia Thinks So.* [online] Wired. Available from: https://www.wired.com/story/can-ai-be-fair-judge-court-estonia-thinks-so/ [Accessed 26 February 2021].

[3] Liu, H., Lin, C. and Chen, Y. (2018) Beyond State v. Loomis: Artificial Intelligence, Government Algorithmization, and Accountability. *International Journal of Law and Information Technology,* 27(2), pp. 122-141.

[4] Kaczorowska, M. (2019) Blockchain-based Land Registration: Possibilities and Challenges. *Masaryk University Journal of Law and Technology*, 13 (2), pp. 339-360.

[5] What is Kira. [online] Available from: https://kirasystems.com/how-kira-works/. [Accessed 5 June 2021].

[6] CARA A.I. [online] Available from: https://casetext.com/cara-ai/. [Accessed 5 June 2021].

[7] What we do. [online] Available from: https://lexmachina.com/about/. [Accessed 5 June 2021].

[8] Marchant, G. (2017) Artificial Intelligence and the Future of Legal Practice. The *SciTech Lawyer*, 14 (1), p. 23.

with legal education and ending with legal practice and judiciary.[9] However, as opportunities grow, so does the critical response. Therefore, some authors such as Wendel, Sandvik, Yu or Pasquale pointed out the risk of new malpractice[10], legal and technical black box connected to the use of AI[11] or the all-embracing US-centrism.[12] Another debate focuses on the barrier some of these services have to face in the form of statutes dealing with the unauthorized provision of legal services.[13] Simultaneously, there is an ongoing debate on the use of artificial intelligence in the justice field and the right to a fair trial.[14]

As mentioned above, AI is capable of making significant changes in all areas of law. It is, however, known to have certain flaws, such as its lack of transparency and explainability, possible biases deriving from potentially flawed data, or highly techno "salvationist"[15] narratives in its advertisement. This article addresses these risks connected to AI-based legaltech. The aim of this article is not to discourage the use of the new disruptive technologies but merely to offer a few points for reflection. While providing these points, I would like to stress that we should not uncritically embrace *all* AI-based legaltech in *all* possible areas of law and legal practice. Rather, we should examine the risks connected to each specific use as these risks might manifest differently with distinct AI tools and their distinct use. If a legal drafting tool makes a mistake, the consequences might be less severe than if a robojudge misjudges a piece of evidence. Hence, we should

---

[9] McGinnis J. and Pearce, R. (2014) The Great Disruption: How Machine Intelligence Will Transform the Role of Lawyers in the Delivery of Legal Services. *Fordham Law Review*, 82 (6), p. 3042.

[10] Sandvik, K. (2021) *Is Legal Technology a New "Moment" in the Law and Development Trajectory?*. [online] Antipode Online. Available from: https://antipodeonline.org/2019/12/04/legal-technology-law-and-development/ [Accessed 26 February 2021].; Marchant, G. (2017) Artificial Intelligence and the Future of Legal Practice. The *SciTech Lawyer*, 14 (1), p. 23.

[11] Liu, H., Lin, C. and Chen, Y. (2018) op. cit., pp. 134-136.; Wendel, B.W. (2019) The Promise and Limitations of Artificial Intelligence in the Practice of Law. *Oklahoma Law Review*, 72 (1), pp. 27-29.; Pasquale, F. (2019) A Rule of Persons, Not Machine: The Limits of Legal Automation. *George Washington Law Review,* 87 (1), p. 5.; Yu, R. and Spina G.A. (2019) What's Inside the Black Box? AI Challenges for Lawyers and Researchers. [online] *Cambridge University* Press. Available from: https://www.cambridge.org/core/journals/legal-information-management/article/whats-inside-the-black-box-ai-challenges-for-lawyers-and-researchers/8A547878999427F7222C3CEFC3CE5E01#article [Accessed 29 May 2021].

[12] Sandvik, K. (2021) op. cit. Available from: https://antipodeonline.org/2019/12/04/legal-technology-law-and-development/ [Accessed 26 February 2021].

[13] McGinnis J. and Pearce, R. (2014) op. cit., p. 3057.

[14] Sourdin, T. (2018) Judge v Robot? Artificial Intelligence and Judicial Decision-Making. *UNSW Law Journal*, 41 (4).

[15] Pasquale, F. (2019) op. cit., p. 2.

be ready to know where to draw a line. Not all AI is equal when it comes to its risks and not all legal fields and services are the same.

The article consists of two main parts. The first part discusses the current concerns associated with AI and their significance for legaltech. The second part then focuses on AI's use in two particular legal areas: in the provision of legal services and in the judiciary. Specifically, the article separately explores and reflects the issues, themes, dilemmas, and impact of AI in these legal areas.

2. THE RISKY ARTIFICIAL INTELLIGENCE AND LEGALTECH

2.1 AI-BASED LEGALTECH

There have been many attempts to define what artificial intelligence is. Many scholars tried to come up with their own definition, often including terms such as the ability to learn, ability to reach any goal, consciousness, self-awareness or alternatively trying to tie artificial intelligence with the concept of intelligence or rationality.[16] Calo, for example, understands AI as

> "*a set of techniques aimed at approximating some aspect of human or animal cognition using machines.*"[17]

Scherer defined AI for his purposes as

> "*machines that are capable of performing tasks that, if performed by a human, would be said to require intelligence.*"[18]

This is just a small demonstration of how diversely AI can be grasped. Thus, for the purpose of this article, artificial intelligence will be used as a broad umbrella term to cover a vast spectrum of technology often based on algorithms capable of achieving complex goals[19], irrespective of whether the technology is based on machine learning, natural language processing, deep learning, or cognitive computing. This allows for

---

[16] Scherer, M. (2016) Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. *Harvard Journal of Law & Technology,* 29 (2), pp. 360-361.

[17] Calo, R. (2018) Artificial Intelligence Policy: A Primer and Roadmap. *University of Bologna Law Review*, 3 (2), p. 184.

[18] Scherer, M. (2016) op. cit., p. *362*.

[19] Similar solution was adopted e.g., by Sourdin in Sourdin, T. (2018) Judge v Robot? Artificial Intelligence and Judicial Decision-Making. *UNSW Law Journal*, 41 (4), p. 1116.

an extensive amount of legaltech to be covered. AI-based legaltech then refers to tools designed to achieve certain goals to improve legal services while using artificial intelligence. In practice, it may be either tools used for document revision, legal research, or even tools capable of predicting courts' decisions and the ones that are designed to assists judges with their decisions.[20] And although lawyers still might be far from being replaced by robots, it seems that artificial intelligence may do certain tasks faster as it can process large volumes of data in a matter of seconds.[21]

2.2 THE RISKS ASSOCIATED WITH ARTIFICIAL INTELLIGENCE

AI offers many opportunities, most often connected to better efficiency. However, there are still many risks and dilemmas surrounding this technology. That is why it got on the radar of so many scholars and regulatory bodies recently. For example, in 2020, the European Commission adopted White paper on artificial intelligence in which a risk-based approach toward future regulation of artificial intelligence was emphasized.[22] The following chapters explore multiple risks associated with AI-based legaltech, such as its unpredictability, algorithmic and data bias, advertisement, or lack of transparency.

2.2.1 THE BLACK BOX AND EXPLAINABILITY OF AI

One of the risks associated with artificial intelligence is undoubtedly it being a black box. That means we have become unable to understand its decision-making process.[23] In this sense, black box is a metaphor being used to describe the difficulty to explain AI.[24] Interestingly, there can be many black-box problems for different stakeholders. Thus, the question of explainability may vary from „what" to „why" depending on the stakeholder.[25] However, the core issue is the same - we cannot

[20] Corrales, M., Fenwick, M., Haapio H. and Vermeulen, E. (2019) op. cit., p. 7.

[21] Fabian, S. (2020) Artificial Intelligence and the Law: Will Judges Runs on Punchcards?. *Common Law Review*, 16 (4), p. 4.

[22] European Commission (2020) *White Paper On Artificial Intelligence - A European approach to excellence and trust*, COM(2020) 65 final, 19 February 2020. Available from: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf [Accessed 5 March 2021].

[23] Bathaee, Y. (2018) The Artificial Intelligence Black Box and the Failure of Intent and Causation. *Harvard Journal of Law & Technology*, 31 (2), p. 905.

[24] Zednik, C. (2019) *Solving the Black Box Problem: A Normative Framework for Explainable Artificial Intelligence*. [online]. Philosophy & Technology. Available from: https://doi.org/10.1007/s13347-019-00382-7 [Accessed 29 May 2021].

[25] Zednik, C. (2019) op. cit.

understand it, which means that we cannot predict and recognize its failures.[26] Additionally, it is also important to highlight that not all AI techniques are equally unexplainable. The one technique mostly connected to black box is deep learning, which was even called the "particularly dark black box".[27] This essentially means that not all AI is equally opaque. This aspect might be important in the moment we are choosing which AI we will put our trust into when it comes to decision making.

The reason why the lack of explainability of AI has become such a serious part of the discussion is simple – it is a question of trust.[28] The way AI is deployed nowadays leads to the fact that we put a lot of trust into a system that may be unpredictable or unexplainable to us. And there are calls that if we cannot properly understand AI, at least at the same level as we understand humans, we should not use it.[29] That is the reason why there is a demand for the creation of "explainable AI" that would make AI's opacity transparent.[30] This issue of trust and transparency is an important thing to consider while using in the legal field, especially in the field of justice. In this matter, Wendel writes about the core function of law which includes the need for justification for actions that may affect other's interests.[31] He even goes further stating that the core lawyering function is the connection between legal authority and the moral demand for accountability.[32] This in itself poses problems when it comes to the lack of explainability of AI.

The black box issue discussed above is sometimes referred to as the "technical black box".[33] However, is not the only black box associated with AI. AI was also called a "legal black box" in the literature. The notion of the legal black box refers to its opacity that crystallizes from its being proprietary software.[34] In other words, the algorithms and data are often

---

[26] Knight, W. (2017) The *Dark Secret at the Heart of AI.* [online] MIT Technology Review. Available from: https://www.technologyreview.com/2017/04/11/5113/the-dark-secret-at-the-heart-of-ai/ [Accessed 5 June 2021].

[27] *Ibid.*

[28] *Ibid.*

[29] Knight, W. (2017) op. cit.

[30] Zednik, C. (2019) op.cit.

[31] Wendel, B.W. (2019) The Promise and Limitations of Artificial Intelligence in the Practice of Law. *Oklahoma Law Review*, 72 (1), p. 29.

[32] *Ibid.*

[33] Liu, H., Lin, C. and Chen, Y. (2018) op. cit., pp. 134-136.

[34] *Ibid*.

protected as trade secrets.[35] Clearly, the solution here is to demand a transparent release of these algorithms.[36] This demand is particularly strong in the field of justice as transparency poses one of the core values in the justice system.[37] The problem is that a simple release of an algorithm might not bring the desired effects as will be described in the following chapter.

Both of these aspects of black box create a very paradoxical situation in the legal market. On the one hand, we see the advertisement about how the brand-new AI tools can make our lives easier, the legal practice faster, and the judicial decisions fairer. On the other, we may not really know the "how" and "why" behind it. Moreover, this could also mean that the program may function in a different way than it was initially intended.[38] That, in itself, can bear horrible consequences in the legal field, as will be demonstrated in the following chapters of this paper.

2.2.2 BIAS AND DISCRIMINATION

Another known risk connected to the use of AI is a bias that can lead to discrimination. There have been numerous cases where this issue has occurred. Amazon, for example, had to deactivate its AI used for the hiring process because it heavily discriminated against women.[39] In another known case, LinkedIn's search engine was suggesting a male version of a name if a user searched for a female.[40] Likewise, facial recognition technology, which is often based on deep learning, has become notorious for being biased on ethical, gender and racial characteristics.[41]

---

[35] Yu, R. and Spina G.A. (2019) What's Inside the Black Box? AI Challenges for Lawyers and Researchers. [online] *Cambridge University Press.* Available from: https://www.cambridge.org/core/journals/legal-information-management/article/whats-inside-the-black-box-ai-challenges-for-lawyers-and-researchers/8A547878999427F7222C3CEFC3CE5E01#article [Accessed 29 May 2021].

[36] *Ibid.*

[37] Prins, C. and van Ettekoven, B-I. (2018). Data analysis, artificial intelligence and the judiciary system. In Mak V., Tiong Tjin Tai E., & Berlee A. (Eds.), *Research handbook in data science and law*, Edward Elgar, p. 442

[38] Bathaee, Y. (2018) op. cit., p. 907.

[39] Dastin, J. (2018) *Amazon scraps secret AI recruiting tool that showed bias against women.* [online] Reuters. Available from: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G [Accessed 5 March 2021].

[40] Day, M. (2018) *How LinkedIn's search engine may reflect a gender bias.* [online] The Seattle Times. Available from: https://www.seattletimes.com/business/microsoft/how-linkedins-search-engine-may-reflect-a-bias/ [Accessed 5 March 2021].

[41] Castelvecchi, D. (2020) *Is facial recognition too biased to be let loose?.* [online] nature. Available from: https://www.nature.com/articles/d41586-020-03186-4 [Accessed 5 March 2021].

Generally, bias may appear either in algorithms or in the data.[42] Both of these biases may be complementary to each other. The algorithms are not immune to the values of their creators and at the same time they are dependent on the datasets they were provided with.[43] The risk here is that AI may emphasize all the existing bias in the code or in flawed data.[44] There is even an argument that as long as AI derives its instructions from humans, it will always be inaccurate.[45]

Moreover, the issue with bias is tightly connected to both technical and proprietary legal black box and affects more fields than law as algorithms are now being used to decide everyday economic decisions across many institutions. Yet, the institutions using them, be it a bank or state authority, do not know how the decisions were derived and people are basically left in the dark with their "why" question.[46] That is why there is such a strong call for algorithm transparency. However, there is a growing skepticism that transparency alone might not solve the issue itself until we reach explainable AI.[47] To put it simply – just knowing the code and the data might not be enough to understand the decision.

Once aware of the risks, it can only be concluded that using AI technology in the legal field can easily cause more harm than good, notably if used unaware of the risks and without any critical assessment. The risks may, however, differ. In the case of legal tools developed for attorneys to use in their practice, the outcome may simply be that different legal research tools come up with different results.[48] Although this may mean that owning a particular database may pose a competitive advantage in the legal profession, it is not an impediment to the use of AI in legal practice. Whereas in judiciary, this issue may again be against the very core values of justice system.[49]

---

[42] Therefore we either speak of algorithmic bias or data bias as described by Yu, R. and Spina G.A. (2019) op. cit.

[43] Yu, R. and Spina G.A. (2019) op. cit.

[44] *Ibid.*

[45] Davis J. P. (2019) Artificial Wisdom? A Potential Limit on AI in Law (and Elsewhere). *Oklahoma Law Review*, 72 (1), pp. 65-66.

[46] Hao, K. (2020) The *coming war on the hidden algorithms that trap people in poverty [online] MIT Technology Review.* [online] MIT Technology Review. Available from: https://www.technologyreview.com/2020/12/04/1013068/algorithms-create-a-poverty-trap-lawyers-fight-back// [Accessed 5 June 2021].

[47] Yu, R. and Spina G.A. (2019) op. cit.

[48] Up to 40% cases may be unique to each database, more in Yu, R. and Spina G.A. (2019) op. cit.

[49] Pasquale, F. (2019) op. cit., p. 5.

2.2.3 MORE TROUBLE WITH DATA

Data has become a powerful asset in the past years. It can be argued that even more powerful than algorithms themselves. This is very well illustrated by Norvig's famous quote that Google does not have better algorithms, just more data.[50] Data may, indeed, be a good helper and may give us answers to understand many underlying patterns in our daily lives. This being transformed in the field of law – data may for example help us to better understand court rulings as we can extract some patterns from them like how the judges use law literature or how often the change in case law led to the amendment in legislation.[51]

The problem is that data may be inaccurate and incomplete. It was already mentioned that faulty data may carry biases which are then projected into the result. But that is not the only issue. Data may simply be wrong. And once they are wrong, so is the outcome they produce.[52] Furthermore, one needs a huge amount of data to build their legaltech tool. This may be an obstacle for many startups to create functional legaltech tools. LexMachina was for example funded by many big technology companies such as Oracle, Microsoft, Apple or Intel.[53] Data also seem to be the reason behind the downfall of ROSS Intelligence as the company was sued by Westlaw for scraping Westlaw's database.[54] This demonstrates that some AI risks do not lie directly within the AI, but are connected to the environment it creates on the market.

There are two final remarks I would like to make. First, data do not know the context and do not know the story. Data can be wrongly used in a different context than they were collected for.[55] Here is where

---

[50] This quote can be found in Cleland, S. (2011) *Google's "Infringenovation" Secrets* [online] Forbes. Available from: https://www.forbes.com/sites/scottcleland/2011/10/03/googles-infringenovation-secrets/?sh=5e00d3c930a6 [Accessed 5 June 2021]. It was also repeated by Schneider, G. (2018) European intellectual property and data protection in the digital-algorithmic economy; a role reversal(?). Journal of *Intellectual Property Law & Practice*, 13 (8), p. 231.

[51] Prins, C. and van Ettekoven, B-J. (2018) op.cit., p. 435.

[52] This issue is often referred to as „garbage in, garbage out". For more detailed assessment see Davis J. P. (2019) op. cit., pp. 65-66.

[53] Katz, D. (2012) Quantitative Legal Prediction--or--How I Learned to Stop Worrying and Start Preparing for the Data-Driven Future of the Legal Services Industry. *Emory Law Journal*, 62 (4), p. 940.

[54] Lancaster, Alaina. *Judge Rejects ROSS Intelligence's Dismissal Attempt of Thomson Reuters Suit Over Westlaw Content*. [online] Law.com. Available from: https://www.law.com/therecorder/2021/03/29/judge-rejects-ross-intelligences-dismissal-attempt-of-thomson-reuters-suit-over-westlaw-content/ [Accessed 5 June 2021].

[55] Prins, C. and van Ettekoven, B-J. (2018) op.cit., p. 439.

the context and decisions come into play. As was mentioned – simple algorithmic and data transparency may not be sufficient. Hence, if we want to understand the code, we must look for far more than the data itself.[56] Second, there is a privacy issue with data. The moral question here is whether client's data or court party's data can or even should be used to feed these algorithms and who then own this data.[57] Although this topic is slightly out of the scope of this article, it is still one piece of a puzzle of the data controversy.

2.3 THE MARKETING NARRATIVES SURROUNDING AI

There is one final note to make about the risks associated with AI-based legaltech and that is a reflection of their marketing strategies. We may notice that the one thing the legaltech tools have in common is the narrative surrounding them, which often revolves around promises on improved lawyering, higher performance and better access to justice.[58] For instance, Ravell has quite a textbook claim which states that they "build data-driven tools that help lawyers be better, faster, and more persuasive."[59] We must therefore make a careful look at these services and evaluate whether they can truly deliver what they claim. Some of these tools may be targeted at professionals who may take their claims a bit more reserved. Others, such as chatbots or automated legal documents services, are designed for the general public which might fall for these claims much more easily, especially when the price points may differ drastically from attorneys. This is not to say that all legaltech designed for the public cannot deliver great service and help those truly in need. However, it is still a business being offered in a competitive environment. And there already has been a case where these claims went too far when the company claimed to deliver service in a quality equal to an attorney.[60]

It is also true that AI has a big potential to bring great benefits into legal practice because it can help lawyers with their research, contract analysis

---

[56] Pasquale, F. (2020) Revisiting the Black Box Society by rethinking the political economy of big data. *Big Data & Society*, 7 (2) , p. 3.

[57] Prins, C. and van Ettekoven, B-J. (2018) op.cit., p. 445.

[58] Sandvik, K. (2021) op. cit. Available from: https://antipodeonline.org/2019/12/04/legal-technology-law-and-development/ [Accessed 26 February 2021].

[59] *Our Story.* [online] Available from: https://home.ravellaw.com/who-we-are. [Accessed 5 June 2021].

[60] The case at hand is a German case involving Wolters Kluwer and their service SmartLaw. More detailed analysis can be found in the following chapter.

or draft review while observing patterns humans would simply overlook.[61] These benefits could even transform the legal profession and open debates about new set of skills lawyers should have. We must, however, take a very realistic look at what it can really do to not fall into a trap of unrealistic expectations. Reading some of the advertising claims can awaken very utopistic pictures of the legal profession's future. This is why it is important to understand both advantages and disadvantages of AI-based technology.

3. PROVISION OF LEGAL SERVICES IN THE CONTEXT OF THE NEW TECHNOLOGIES

Currently, the market offers dozens of legaltech tools and services which are based on AI, mostly natural language processing tools based on machine learning. These services also have different target groups as some such as Kira or Case Mine are offered to assist lawyers and others like LegalZoom or JustFix to help the public with access to justice. The latter category seems to be the one that sparks the most controversies, as these services have been challenged with unauthorized practice of law.[62] This is the reason why I will focus on them. As many of these services are becoming more and more autonomous, the question arises whether they could be considered a provision of legal services or not. Additionally, an important point to reflect is that these services are still a business in their nature. Thus, they may not be as salvationist as they tend to present themselves.

3.1 CHATBOTS, AUTOMATED LEGAL DOCUMENTS AND THE PROVISION OF LEGAL SERVICES

DoNotPay, a so-called "robot lawyer", is a chatbot that started as a service that provided help with appealing parking tickets. Currently, it can help customers contest almost anything – insurance claims, driving tests or cancelled flight tickets.[63] What is interesting about the service is that it was not created by a lawyer. The founder was 17 years old when he first started this app that currently runs on the famous IBM Watson.[64] DoNotPay is an example that AI creates new opportunities for people to get their legal matter resolved without talking to a lawyer. In essence, it is not a bad thing

[61] Yu, R. and Spina G.A. (2019) op. cit.

[62] McGinnis J. and Pearce, R. (2014) op. cit., p. 3057.

[63] Information available from the introduction page of DoNotPay, section Features. Available from: https://donotpay.com. [Accessed 5 March 2021].

since legal services may be expensive, which may discourage many people from seeking legal advice. As Moradian points out, legaltech comes most for those who cannot afford standard legal services.[65] And this is exactly what DoNotPay claims to be their mission.[66] What may become an issue is the expectation these people have when using such services. If we look at the advertisement of DoNotPay a bit more carefully, we can observe that it allows people to "fight corporations, beat bureaucracy and sue anyone at the press of a button."[67] Moreover, they list "sue anyone" as one of their features.[68] Although wrapped in the "cheaper and better alternative to a lawyer" narrative, this sue anyone button might become hazardous when in hands of consumers. As much appealing as it is, consumers may be left in the dark about their actual chances with their claim or about the potential risks associated with this service based on AI.

Advertisement is not the only controversy connected to DoNotPay and similar services. Given their nature, these services have drawn the attention of many Bar Associations and raised a question about what a provision of legal services is. The reason is simple – a consumer or a company provides these services with information or documents and an algorithm gives them an answer or a full legal document. In the US, a platform called LegalZoom has faced multiple suits regarding the unauthorized provision of legal services. Although the service is a mere automated document preparation, it very nicely illustrates some tendencies towards these services and raises questions concerning whom the restriction on the unauthorized practice of law is meant to protect.[69] The reasons behind these claims may not be just the protections against unqualified legal advice, but it may serve as an anti-competition measure.[70] LegalZoom's services are also not that different from

---

[64] Krieger. M. (2019) *Stanford student's quest to clear parking tickets leads to "robot lawyers.* [online] The Mercury News. Available from: https://www.mercurynews.com/2019/03/28/joshua-browder-22-builds-robot-lawyers/ [Accessed 5 March 2021].

[65] Moradian, J. (2020) A New Era of Legal Services: The Elimination of Unauthorized Practice of Law Rules to Accompany the Growth of Legal Software. *William. & Mary Business Law Review*, 12 (1), p. 249.

[66] Terms of Service, section Introduction and Overview. [online] Available from: https://donotpay.com/learn/terms-of-service-and-privacy-policy/ [Accessed 5 June 2021].

[67] Information available from the introduction page of DoNotPay, section Features. Available from: https://donotpay.com. [Accessed 5 June 2021].

[68] *Ibid.*

[69] Shipman, C. (2019) Unauthorized Practice of Law Claims Against LegalZoom—Who Do These Lawsuits Protect, and is the Rule Outdated?. *Georgetown Journal of Legal Ethics*, 32 (4), p. 940.

[70] Shipman, C. (2019) op. cit., p. 944.

the one many chatbots offer as they generate documents, and their system contains responses from their clients, which in the actual suit was used by the North Carolina Bar Association to demonstrate that their service is similar to a lawyer interviewing a client.[71] This case also led to a creation of a new law in North Carolina that ultimately stated that the practice of law

> "*does not include the operation of a Web site by a provider that offers consumers access to interactive software that generates a legal document based on the consumer's answers to questions presented by the software*."[72]

Recently, there has been an interesting case in this area in Germany. This case has not only brought up the question of the nature of these services but the claims they make in their advertisement. Hamburg Bar Association sued a platform SmartLaw for the same reasons as LegalZoom was sued in the US – unauthorized provision of legal services. SmartLaw works as a generator of legal documents based on a Q&A system. It was precisely the fact that the platform used a Q&A system that has become the core issue in the dispute. The Bar argued that since the system does not offer simple templates to fill but creates the contracts specifically tailored to the customer based on answers concerning the subject matter, it amounts to an individual examination of a case that constitutes a provision of legal services.[73] The Bar also had a problem with the service's allegedly misleading advertisement as many claims about the quality "being the same as from an attorney" was made.[74] Unfortunately, we still do not have a final verdict at this point as the first two instances reached an opposite decision, so the final decision now remains to the supreme court. However, if we look at both decisions closer, it is interesting to see how the courts' approach toward the Q&A system differs. In the first instance, the court concluded that the provision of such a system amounts to the individual examination of the case because the platform generates the documents on a more individualized matter and thus offers a tailored solution to the customer.[75] The second instance, however, considered that the software's programming always predetermines the final result, so the finalized legal document is still

---

[71] Shipman, C. (2019) op. cit., p. 946; *LegalZoom.com, Inc. v. N.C. State Bar* (2014), No. 11CVS15111, WL 1213242, North Carolina Business Court.

[72] Shipman, C. (2019) op. cit., p. 947.

[73] 33 O 35/19, LG Köln, 8.10.2019.

[74] *Ibid.*

[75] *Ibid.*

routinized.[76] Both courts, however, agreed that the advertising was misleading as it may create unrealistic expectations.

Regardless of the SmartLaw case final result, there are a few points we may take from this and other similar disputes. First, as much as it can be argued at this point that automated responses do not provide any individual examination of the case, this might not be true in the future with the current technological development. It is going to be very interesting to see where the technical development will go as these chatbots and other similar services become "smarter". We may even take a wild guess that at some point, they will be truly capable of making a genuinely individual examination of a case that even might amount to legal reasoning.

Second, these claims often come from bar associations which may indicate that the dispute is not solely about the protection of the consumers, but there are some competitive aspects in play.

Finally, as these services are primarily offered as a cheaper and more accessible alternative to a lawyer, we must further debate about their role in our society and what advantages and disadvantages they bring. As already mentioned, one of the issues with the SmartLaw case was the misleading advertisement of the whole service. Similarly, DoNotPay has its whole advertisement build around a "sue anyone" button on your phone. That is why we should take a very cautious approach to all those claims about quality being on par with an attorney or surpassing even. If we take a look at all the risks associated with AI, the result is that a code may simply be flawed – with bias or wrong data. Therefore, these chatbots and other similar services are very reliant on the datasets they were created with. Furthermore, if a chatbot is not sufficiently "trained" in a certain matter, a blind trust by a laic public may lead to the client's harm.[77] Another risk may be the fact that the service might not be subject to any confidentiality or conflict of interest rules.[78] These risks then go against

[76] I-6 U 263/19, Oberlandesgericht Köln, 19.6.2020.

[77] It should be noted that the general public might not be the only one who can fall victim to the unrealistic expectations the advertisement may create. This leads to the general issue that if the AI-based legaltech is not provided with sufficient data, it may later fail to deliver appropriate level of services. This brings us back to the fact that context matters when it comes to data or that different tools may come up different results based on their algorithm or datasets. Hence, different tools may lead a lawyer to different problematics and different cases. This may play a role in the delivery of their service. This, however, leads to another debate that would be more focused on the ethical aspect of legal practice and possibly a need for a change in law curriculums.

[78] Moradian, J. (2020) op. cit., p. 256.

the general narrative about better access to justice, for which many of these services are created.

One final note on this topic should be made. Although the points mentioned above are inclining toward the critical view of these services, they still play an important role in the development of the legal profession. The points simply lead to the question we should ask ourselves – are these issues sufficiently adverse that we should fight for the ban of such services? My answer would be a no as they still provide a cost-effective alternative to the general public, so their overall benefit outweighs the negatives. What should be handled is the level of transparency of these services. They should only offer what they can deliver and not create unrealistic narratives about their nature.

4. AI AND THE JUSTICE SYSTEM

There is an Israeli study about what affects judges' verdicts which concluded that judges deliver much harsher decisions when they are hungry.[79] This study has become somewhat famous when it comes to debates about fairness in human-judges' decisions. The reason is quite simple. The outcome of the study and many other examples through history led to the sentiment that robojudges could eradicate all human biases, be it intentional or accidental, and make sure that everybody is equal under the law.[80]

This sentiment soon became overshadowed by the findings concerning the algorithmic and data bias. As mentioned, AI should not be automatically deployed in all areas of law. And judiciary is a particularly sensitive branch to put our trust into a black box. Moreover, even impartially, which is what made this deployment so appealing, seems to be a myth. As long as there is a bias in the code and the data, the decisions may be flawed. This risk was well demonstrated by the recent case in the US, State v. Loomis. The defendant, Eric Loomis, was sentenced based on the outcome provided by the software called COMPAS that concluded a risk assessment on Loomis. This assessment determined that Loomis was at high risk of recidivism. Based on this assessment, the defendant was

[79] Danzinger, S., Levav J. and Avnaim-Pesso, L. (2011) Extraneous factors in judicial decisions. *Proceedings of the National Academy of Sciences of the United States of America,* 108 (17).

[80] Tegmark, M. (2018) *Life 3.0: Being Human in the Age of Artificial Intelligence,* Penguin Books, p. 105.

sentenced to six-year imprisonment and five-year extended supervision.[81] The decision later served as a controversial point and led to a debate about these algorithms' nature and their accuracy. The issue concerning COMPAS become even more severe after a non-profit organization, ProPublica, conducted a study in which they observed 7000 defendants that COMPAS marked as high risk only to find out that just 20 per cent of them committed a relapse. Moreover, the study found out grave racial disparities – black defendants were falsely labelled as high risk, almost twice the rate as white defendants.[82]

This is not to say that AI cannot help the judiciary and make it more efficient. Generally, AI can be used in two ways in the judiciary – either as an independent adjudicating entity or as an assisting tool for a judge.[83] AI can also make the judicial proceedings faster and thus more effective the same way other AI tools help attorneys in their practice.[84] AI may very well work as a supportive tool since the tools offered for practicing attorneys can be deployed in the judiciary as well.

However, once we focus on more complex tools that are not designed to simply draft or review documents but are designed to actually make certain predictions or even decisions, we stand before the important question – should we put our trust in them? And would it make justice *fairer*? Or even – *just fair*? In my opinion, and given the risks of AI, the technology has still not reached that level of transparency (or explainability) that an AI tool should be used to make crucial decisions in the field of justice. The issue of discrimination, algorithmic bias, legal and technical black box lead to many doubts about whether any use of artificial intelligence would not undermine the right to a fair trial.[85] Moreover, some studies found out that humans tend to blindly trust machines, although they know they might be faulty.[86] This could be particularly dangerous as many would not even question the outcome of these algorithms, which is exactly what happened in the Loomis case.

---

[81] Liu, H., Lin, C. and Chen, Y. (2018) op. cit., pp. 126-129.

[82] Angwin J. and Larson J., Machine Bias. *Propublica*. 23 May 2016. Available from: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [Accessed 10 March 2021].

[83] Dymitruk, M. (2018) The Right to a Fair Trial in Automated Civil Proceedings. *Masaryk University Journal of Law & Technology*, vol 13 (1), p. 29.

[84] Dymitruk, M. (2018) op. cit., pp. 36-37.

[85] Liu, H., Lin, C. and Chen, Y. (2018) op. cit., p. 137.

[86] Dymitruk, M. (2018) op. cit., pp. 31-32.

Of course, humans are biased, too. They are prone to emotions, and they have bad days.[87] However, is replacing one bias with another for the sake of effectivity something we should desire? As Fabian notes,

> *"At this point of our evolution and their development, we must not forget that judging requires not only knowledge of the law and case evidence, but also the empathetic ability to understand the emotions and motivations underlying human behaviour "*[88]

This is something we should bear in mind while implementing the algorithms into our justice system. Because deep underneath, a "human" understanding, empathy and capability of critical thinking is something a person might be looking for in our justice system along with the objectivity, once they are put on a trial. This may be particularly important when it is necessary to moderate too harsh a provision of law. And that is something the AI does not possess at the moment.

5. CONCLUSION

At the most general level. AI-based legaltech represents the conflict of whether to advance law further through the use of new disruptive technologies or whether to choose a "safe" path and remain conservative under the weight of possible risks. This paper discussed the present use of AI-based legaltech while addressing several critical points connected to the risks associated with artificial intelligence. At present, we can see several AI-based tools deployed in the legal profession. Some of them are research and review tools designed to help lawyers in their profession; others are chatbots and automated legal document generators created to provide cheaper access to law and justice. The technological innovations did not even miss the judicial field as there are attempts to apply AI-based technological solutions even in this field. Furthermore, despite the fact that AI-based legaltech can improve the legal profession, there are still many concerns that need to be addressed and further dealt with to make the present technological solutions more transparent.

The first part of this article focused on several issues concerning artificial intelligence, such as the technical and legal black box, algorithmic and data bias and discrimination. In the second part, the paper addressed the specific

[87] Fabian, S. (2020) op. cit., p. 5.
[88] Fabian, S. (2020) op. cit., p. 6.

issues that arise from the application in the sphere of the provision of legal services and deployment in the judiciary. Many of the tools have drawn the attention of several stakeholders. Either be it academics or regulatory bodies who point out certain risks or bar associations, which are trying to delineate where the provision of legal services starts under the disguise of protection. Therefore, services such as LegalZoom in the US or SmartLaw in Germany have faced being sued for the unauthorized provision of legal services.

As demonstrated in the article, artificial intelligence could make the legal profession more efficient. The aim of this article was not to discourage lawyers or consumers from using legaltech but to merely state certain risks for them not to overly rely on the technology. All the remarks made showed that artificial intelligence could be a valuable tool; however, it must be used cautiously. The technology bears many risks which must be addressed before we put our blind trust into them.

LIST OF REFERENCES

[1] Angwin J. and Larson J., Machine Bias. *Propublica*. 23 May 2016. Available from: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [Accessed 10 March 2021].

[2] Bathaee, Y. (2018) The Artificial Intelligence Black Box and the Failure of Intent and Causation. *Harvard Journal of Law & Technology*, 31 (2).

[3] Calo, R. (2018) Artificial Intelligence Policy: A Primer and Roadmap. *University of Bologna Law Review*, 3 (2).

[4] Castelvecchi, D. (2020) *Is facial recognition too biased to be let loose?.* [online] nature. Available from: https://www.nature.com/articles/d41586-020-03186-4 [Accessed 5 March 2021].

[5] Cleland, S. (2011) *Google's "Infringenovation" Secrets* [online] Forbes. Available from: https://www.forbes.com/sites/scottcleland/2011/10/03/googles-infringenovation-secrets/?sh=5e00d3c930a6 [Accessed 5 June 2021].

[6] Corrales, M., Fenwick, M., Haapio H. and Vermeulen, E. (2019) Tomorrow's Lawyer Today? Platform-Driven LegalTech, Smart Contracts & the New World of Legal Design. *Journal of Internet Law*.

[7] Danzinger, S., Levav J. and Avnaim-Pesso, L. (2011) Extraneous factors in judicial decisions. *Proceedings of the National Academy of Sciences of the United States of America*, 108 (17).

[8] Dastin, J. (2018) *Amazon scraps secret AI recruiting tool that showed bias against women.* [online] Reuters. Available from: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G [Accessed 5 March 2021].

[9] Davis J. P. (2019) Artificial Wisdom? A Potential Limit on AI in Law (and Elsewhere). *Oklahoma Law Review*, 72 (1).

[10] Day, M. (2018) *How LinkedIn's search engine may reflect a gender bias*. [online] The Seattle Times. Available from: https://www.seattletimes.com/business/microsoft/how-linkedins-search-engine-may-reflect-a-bias/ [Accessed 5 March 2021].

[11] DoNotPay. *Features*. [online] Available from: https://donotpay.com [Accessed 5 March 2021].

[12] Dymitruk, M. (2018) The Right to a Fair Trial in Automated Civil Proceedings. *Masaryk University Journal of Law & Technology*, vol 13 (1).

[13] European Commission (2020) *White Paper On Artificial Intelligence - A European approach to excellence and trust,* COM(2020) 65 final, 19 February 2020. Available from: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf [Accessed 5 March 2021].

[14] Fabian, S. (2020) Artificial Intelligence and the Law: Will Judges Runs on Punchcards?. *Common Law Review*, 16 (4).

[15] Hao, K. (2020) The *coming war on the hidden algorithms that trap people in poverty*. [online] MIT Technology Review. Available from: https://www.technologyreview.com/2020/12/04/1013068/algorithms-create-a-poverty-trap-lawyers-fight-back// [Accessed 5 June 2021].

[16] Kaczorowska, M. (2019) Blockchain-based Land Registration: Possibilities and Challenges. *Masaryk University Journal of Law and Technology*, 13 (2).

[17] Katz, D. (2012) Quantitative Legal Prediction--or--How I Learned to Stop Worrying and Start Preparing for the Data-Driven Future of the Legal Services Industry. *Emory Law Journal*, 62 (4), p. 940.

[18] Knight, W. (2017) The *Dark Secret at the Heart of AI.* [online] MIT Technology Review. Available from: https://www.technologyreview.com/2017/04/11/5113/the-dark-secret-at-the-heart-of-ai/ [Accessed 5 June 2021].

[19] Krieger, M. (2019) *Stanford student's quest to clear parking tickets leads to "robot lawyers.* [online] The Mercury News. Available from: https://www.mercurynews.com/2019/03/28/joshua-browder-22-builds-robot-lawyers/ [Accessed 5 March 2021].

[20] Lancaster, Alaina. *Judge Rejects ROSS Intelligence's Dismissal Attempt of Thomson Reuters Suit Over Westlaw Content.* [online] Law.com. Available from: https://www.law.com/therecorder/2021/03/29/judge-rejects-ross-intelligences-dismissal-attempt-of-thomson-reuters-suit-over-westlaw-content/ [Accessed 5 June 2021].

[21] LegalZoom.com, Inc. v. N.C. State Bar (2014), No. 11CVS15111, WL 1213242, North Carolina Business Court.

[22] Liu, H., Lin, C. and Chen, Y. (2018) Beyond State v. Loomis: Artificial Intelligence, Government Algorithmization, and Accountability. *International Journal of Law and Information Technology*, 27 (2).

[23] Marchant, G. (2017) Artificial Intelligence and the Future of Legal Practice. The *SciTech Lawyer*, 14 (1).

[24] McGinnis J. and Pearce, R. (2014) The Great Disruption: How Machine Intelligence Will Transform the Role of Lawyers in the Delivery of Legal Services. *Fordham Law Review*, 82 (6), p. 3042.

[25] Mokhtarian, E. (2018) The Bot Legal Code: Developing a Legally Compliant Artificial Intelligence. *Vanderbilt Journal of Entertainment and Technology Law*, 21 (1).

[26] Moradian, J. (2020) A New Era of Legal Services: The Elimination of Unauthorized Practice of Law Rules to Accompany the Growth of Legal Software. *William. & Mary Business Law Review*, 12 (1).

[27] Morse, S. C. (2019) When Robots Make Legal Mistakes. *Oklahoma Law Review*, 72 (1).

[28] Niller, E. Can AI Be a Fair Judge in Court? Estonia Thinks So. [online] *Wired.* Available from: https://www.wired.com/story/can-ai-be-fair-judge-court-estonia-thinks-so/ [Accessed 26 February 2021].

[29] Pasquale, F. (2019) A Rule of Persons, Not Machine: The Limits of Legal Automation. *George Washington Law Review,* 87 (1).

[30] Pasquale, F. (2020) Revisiting the Black Box Society by rethinking the political economy of big data. *Big Data & Society*, 7 (2), p. 3.

[31] Poppe, E. (2019) The Future Is Complicated: AI, Apps & Access to Justice. *Oklahoma Law Review*, 72 (1).

[32] Prins, C. and van Ettekoven, B-J. (2018). Data analysis, artificial intelligence and the judiciary system. In Mak V., Tjong Tjin Tai E., & Berlee A. (Eds.), *Research handbook in data science and law*, Edward Elgar.

[33] Sandvik, K. (2021) *Is Legal Technology a New "Moment" in the Law and Development Trajectory?*. [online] Antipode Online. Available from: https://antipodeonline.org/2019/12/04/legal-technology-law-and-development/ [Accessed 26 February 2021].

[34] Scherer, M. (2016) Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. *Harvard Journal of Law & Technology*, 29 (2).

[35] Schneider, G. (2018) European intellectual property and data protection in the digital-algorithmic economy; a role reversal(?). Journal of Intellectual Property Law & Practice, 13 (8).

[36] Semmler, S. and Zeeve, R. (2017) Artificial Intelligence: Application Today and Implications Tomorrow. *Duke Law & Technology Review*, 16.

[37] Shipman, C. (2019) Unauthorized Practice of Law Claims Against LegalZoom—Who Do These Lawsuits Protect, and is the Rule Outdated?. *Georgetown Journal of Legal* Ethics, 32 (4).

[38] Sourdin, T. (2018) Judge v Robot? Artificial Intelligence and Judicial Decision-Making. *UNSW Law Journal*, 41 (4).

[39] Tegmark, M. (2018) *Life 3.0: Being Human in the Age of Artificial Intelligence*, Penguin Books.

[40] Wendel, B.W. (2019) The Promise and Limitations of Artificial Intelligence in the Practice of Law. *Oklahoma Law Review*, 72 (1).

[41] Wischmeyer, T. (2020) Artificial Intelligence and Transparency: Opening the Black Box. In Wischmeyer, T. and Rademacher T. (Eds.), Regulating Artificial Intelligence, Springer.

[42] Yu, R. and Spina G.A. (2019) What's Inside the Black Box? AI Challenges for Lawyers and Researchers. [online] *Cambridge University Press.* Available from: https://www.cambridge.org/core/journals/legal-information-

management/article/whats-inside-the-black-box-ai-challenges-for-lawyers-and-researchers/8A547878999427F7222C3CEFC3CE5E01#article [Accessed 29 May 2021].

[43] Zednik, C. (2019) Solving the Black Box Problem: A Normative Framework for Explainable Artificial Intelligence. [online] *Philosophy & Technology*. Available from: https://doi.org/10.1007/s13347-019-00382-7 [Accessed 29 May 2021].

[44] 33 O 35/19, LG Köln, 8.10.2019.

[45] I-6 U 263/19, Oberlandesgericht Köln, 19.6.2020.

DOI 10.5817/MUJLT2021-2-7

CYBER SECURITY: LESSONS LEARNED FROM CYBER-ATTACKS ON HOSPITALS IN THE COVID-19 PANDEMIC[1]

by

JAN KOLOUCH[*], TOMÁŠ ZAHRADNICKÝ[**], ADAM KUČÍNSKÝ[***]

The article deals with the issue of cyber security, specifically the security of medical facilities. The introduction summarizes and briefly analyses the cyber-attacks demonstrated on Czech health care facilities in the period from 12/2019 to 1/2021, together with the procedures adopted by the responsible authorities. The article also newly presents the current regulatory requirements for cyber security of hospitals. In the context of past attacks and based on analysis of attacks, current legislation and events, the article will provide an opinion on whether the requirements for cyber security of hospitals are set sufficiently or whether this area should be revised. At the same time, measures will be recommended to strengthen the cyber security of hospitals.

KEY WORDS

Critical Infrastructure Protection, Legal Framework, Cyber Security, Cyber-attack, CSIRT, CERT, Healthcare

[1] This article was supported by the European Regional Development Fund "CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence" (No. CZ.02.1.01/0.0/0.0/16_019/0000822).

[*] jan.kolouch@cesnet.cz, CESNET a.l.e., Prague; jan.kolouch@law.muni.cz, CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence (C4e), MUNI, Brno.

[**] tomas.zahradnicky@vse.cz; Department of Systems Analysis, Faculty of Informatics and Statistics, Prague University of Economics and Business, Prague.

[***] a.kucinsky@nukib.cz; Department of Cybersecurity Regulation, the National Cyber and Information Security Agency, Brno.

1. INTRODUCTION

The article provides a summary of significant publicly known cyber-attacks on Czech hospitals that occurred in the period from 12/2019 to 1/2021. This period is also significant that due to the SARS-CoV-2 virus pandemic (hereinafter referred to as "COVID-19"), hospitals, or rather medical facilities, are subject to significantly higher requirements than in the normal period. There are problems with the capacity of medical facilities and the staffing shortage in these facilities. Capacity is often compensated by temporary changes in hospital structures and restrictions on non-acute care, while staffing shortages are partially offset typically by the services of volunteers and medical students called etc.

Following the analysis of cyber-attacks from the above period, the reaction of stakeholders in the field of cyber security will be described. The procedure of the National Cyber Information Security Agency (hereinafter also "NCISA") will be described, as well as the regulatory requirements for cyber security of hospitals and their changes since the beginning of 2021.

In the context of cyber attacks conducted at the healthcare sector in the Czech Republic, the article will provide a framework and recommendations for improving the legal and technical aspects of cyber security in that sector. Based on this framework, it will be possible to verify whether the existing cyber security requirements for healthcare facilities are sufficiently set. Another output of the article will be information on whether the area of cyber security in the healthcare sector should be revised, and if so, proposals for specific adjustments will be made. At the end of the article, recommendations and proposals of measures that can help strengthen the cyber security of medical facilities will be presented.

Based on the Czech Republic's approach to healthcare cyber security, recent law changes, and authors' own analysis, the authors demonstrate possible risks and pitfalls implementing a minimal cybersecurity standard and legislation in other countries.

2. SIGNIFICANT CYBER SECURITY INCIDENTS IN THE HEALTHCARE SECTOR IN THE CZECH REPUBLIC

Cyber-attacks on medical facilities are not a new problem. In the USA, the first cyber-attacks on these facilities combining phishing and

ransomware appeared already in 2016.[2] Outside the USA, there have been cases of attacks in many other countries, including the Czech Republic. Since December 2019, the Czech Republic has been affected by cyber-attacks at ICT infrastructure of numerous medical facilities, some of which have crippled their normal operation for up to several weeks and caused extensive damage.

Medical facilities are currently heavily dependent on ICT infrastructure. In practice, this has shown, among other things, that medical facilities are currently unable to function fully without ICT infrastructure and provide services for which they are primarily established. The dysfunction or unavailability of information and communication technologies and services related to them can, in extreme cases, endanger the lives of patients[3]. Such a strong dependence on ICT infrastructure poses a significant risk.

The risk of the successful attack can often be minimized by organizational and technical measures after analysis of previous attacks.

Based on a detailed analysis of the cyber-attack performed on 11th December 2019 at the Rudolph and Stephanie Regional Hospital in Benešov (HBEN), which we presented in the article Cyber Attacks on Czech Hospitals in the Covid-19 Pandemic[4], we analyzed other similar attacks carried out on the territory of the Czech Republic at the time when a state of emergency was declared on the basis of the COVID-19 pandemic for a significant part of the year. The attacks and their resolution will be studied, and an opinion will be offered on whether the current regulatory requirements are sufficient or whether they should be amended and if so how.

The following table provides a chronological listing of significant publicly known cyber-attacks targeting medical facilities in the Czech Republic between 12/2019 and 1/2021. The table is presented to demonstrate ransomware attacks in healthcare in a relatively short time frame during the COVID-19 pandemic.

---

[2] *Ransomware: See the 14 hospitals attacked so far in 2016*. [online] Available from: https://www.healthcareitnews.com/slideshow/ransomware-see-hospitals-hit-2016?page=1 [Accessed 10 May 2017] also: *Three US hospitals hit by ransomware*. [online] Available from: https://www.bbc.com/news/technology-35880610 [Accessed 10 May 2017].

[3] Deutsche Welle (2020). *German police probe 'negligent homicide' in hospital cyberattack*. [online] Available from: https://p.dw.com/p/3ieQl [Accessed 19 February 2020].

[4] Kolouch, J., Zahradnický T. and Kučínský A. (2021) *Cyber Attacks on Czech Hospitals in the Covid-19 Pandemic.* Unpublished manuscript.

Target of the Attack	**Detection**	**Malware**	**Impact**	**Damages Est.**
The Rudolph and Stephanie´s Regional Hospital in Benešov (444 beds)	11. 12. 2019	Emotet TrickBot Ryuk	Decommissioning Malfunction of some ICT services	CZK 59 million
University hospital Brno (1889 beds)	12. 3. 2020	Defray777	Decommissioning Unavailability of patient data.	Hundreds of milion of CZK
The Psychiatric hospital in Kosmonosy (600 beds)	27. 3. 2020	Dewar	Encryption of shared storage, domain and application disks. Loss of part of the backups.	Unknown
The Hospital for long-term illnesses in Horažďovice (140 beds)	January 2020	Buran	Unauthorized use, damage and deletion of data.	CZK 150 000

Table 1: An overview of successful publicly known attacks at Czech hospitals in 2019-2021

For the purposes of this article, especially for the purpose of introducing a minimal security standard (cf. Section 7), we have decided to briefly summarize each of the attacks from the technical point of view.

The Rudolf and Stefanie's Hospital in Benešov (HBEN). In the case of the attack on HBEN, the Microsoft office document containing macros was opened after the initial phishing email. A user overrode the warning by hitting the "Enable Content" button, the malicious macro within

the document executed further executing a PowerShell script which in turn downloaded the Emotet trojan from the Internet, running it, and starting off the first stage of the infection. There are other possibilities for Emotet installation such as running a stand-alone infected script or by downloading its executable directly by accessing a malicious link in e-mail. TrickBot was used to conduct reconnaissance and to ultimately deliver Ryuk (ransomware). Ryuk is a common final payload for banking Trojans (like TrickBot). Research from SonicWall[5] claims that Ryuk represented a third of all ransomware attacks so far in 2020.

The University Hospital in Brno (HBRNO) was infected with the Defray777 malware. The Defray malware family first appeared in 2017, targeting the Education and Health Care sector[6] and since then has undergone a number of modifications. The most widely occurring infection with Defray777 today comprises of launching Vatet Loader, performing Cobalt Strike attack, and ultimately deploying Defray777. The attack begins with a phishing e-mail with an attachment in the form of a Microsoft Office document containing an embedded OLE Packager Object. According to Trend Micro[7], phishing emails are now well-crafted — for an attack targeting a hospital, the phishing email was from a "hospital IT manager" and the malicious files were disguised as patient reports. If the victim clicks on the OLE file, the attack was initiated launching the Vatet Loader[8]. The Vatet Loader launches the Cobalt Strike attack to perform reconnaissance and spread laterally over the network and to provide remote access to the network. Once the malware operator decides, the attack ends by deploying Defray777. After running Defray777, the listed processes will end, and data encryption will begin. Data on local disks and attached network storage is encrypted by a combination of AES and RSA algorithms. The decryption key for the AES cipher is encrypted by the RSA algorithm

[5] Wadhwani, S. (2020) *Cyber World's Most Fearsome Ransomware Is Ryuk: SonicWall*. [online] Available from: https://www.toolbox.com/security/threat-reports/news/cyber-worlds-most-fearsome-ransomware-is-ryuk-sonicwall/. [Accessed 19 February 2020].

[6] Proofpoint, Inc. (2020) *New Defray Ransomware Targets Education and Healthcare Verticals*. [online] Available from: https://www.proofpoint.com/us/blog/threat-insight/new-defray-ransomware-targets-education-and-health-care-verticals. [Accessed 19 February 2020].

[7] Trend Micro Incorporated (2017) *Defray Ransomware Sets Sights on Healthcare and Other* Industries. [online] Available from: https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/defray-ransomware-sets-sights-on-healthcare-and-other-industries. [Accessed 19 February 2020].

[8] Tracey, R. and Schmitt, D. (2020) *When Threat Actors Fly Under the Radar: Vatet, PyXie and Defray777*. [online] Available from: https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/. [Accessed 19 February 2020].

and sent to the control server under the control of the attacker. After the encryption is completed, the user is asked to pay a ransom for decrypting his data.

The Psychiatric Hospital in Kosmonosy (HKOS). The attack began again with a phishing campaign, this time to launch the Dewar ransomware. This ransomware belongs to a group of malware called Phobos[9]. The initial infection can occur through the insecure Remote Desktop port[10] or through phishing. In the case of phishing, Dewar is distributed as e-mail attachments containing, for example, executable files, archives, Microsoft Office files and PDF documents, or javascript code. After the initial infection, lateral spreading occurs, for which operators can use a variety of methods. The infection ends with a ransom notice after all document files are encrypted. The effects of Dewar ransomware are very similar to those of Defray777.

The Hospital for long-term illnesses in Horažďovice (HHOR). This hospital was attacked by Buran ransomware, which is a development of the older VegaLocker ransomware. Buran[11] spreads through phishing, a publicly accessible Remote Desktop interface, and through the vulnerability of the out-of-date Microsoft Internet Explorer. After it runs and ensures the persistence in the Microsoft Windows operating system registries, privilege escalation tools such as Mimikatz[12] may run to obtain administrator-level access. With administrator privileges, operational logs are deleted, the Windows Event Log service is turned off, and restore points and any local backups are deleted. Finally, the encryption of user data on local disks and attached network storage is started while the decryption key is sent to the control server. Finally, the user is left with a file with ransom requests for decrypting his data. Fortunately, there was no massive spread of this malware at the hospital.

---

[9] Elshinbary, A. (2020) *Deep Analysis of Ryuk Ransomware*. [online] Available from: https://n1ght-w0lf.github.io/malware%20analysis/ryuk-ransomware/. [Accessed 19 February 2020].

[10] *Ibidem.*

[11] Mundo, A. (2019) *Buran Ransomware; the Evolution of VegaLocker*. [online] Available from: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/buran-ransomware-the-evolution-of-vegalocker/. [Accessed 19 February 2020]. Sette, N. (2020) *Malware Analysis – Buran Ransomware-as-a-Service*. [online] Available from: https://www.kroll.com/en/insights/publications/cyber/malware-analysis-buran-ransomware-as-a-service. [Accessed 19 February 2020].

[12] Delpy, B. and Le Toux, V. (2020) *Mimikatz*. [online] Available from: https://github.com/gentilkiwi/mimi-katz/releases. [Accessed 19 February 2020].

All of the above-mentioned attacks have a common factor which is the usage of phishing and ransomware. However, this is not a new, unknown and as yet unpublished phenomenon. Examples include historically older sources – ransomware attacks Defray (years 2016 and 2017)[13], WannaCry (2017)[14], etc.

Given the relatively well-known "modus operandi" of attackers (ie. the use of phishing campaigns and ransomware), the relatively high success rate of their own attacks is surprising. On the other hand, it should be borne in mind that the medical facilities, and in particular the staff of these facilities at the time of the COVID-19 pandemic, are primarily involved in recovering and rescuing as many patients as possible and their caution in relation to phishing e-mails and defective attachments is reduced, among other things, due to mental and physical exhaustion. Another factor increasing the success of these attacks is the way in which temporary staff is recruited in a state of emergency in the form of volunteering and work duty[15]. Employees recruited in this way pose a significant risk, as they may have access to the ICT of the healthcare facility, but they do not always have sufficient computer security habits.

When we compare the presented ransomware attacks to similar attacks in other countries, the average downtime of 15 days and the breadth of damage[16] applied to the Czech attacks as well.

This section summarized publicly known attacks using a combination of phishing and ransomware in the Czech Republic between 9/2019 and 1/2021. This is not an isolated problem and hundreds of similar attacks have already taken place on the world stage. Furthermore, the success of pandemic attacks is increasing due to the strain that causes users to lose vigilance when opening malicious attachments, as well as the potentially insufficient training of temporary staff. In addition to the hospitals

[13] Trend Micro Incorporated (2017) *Defray Ransomware Sets Sights on Healthcare and Other Industries*. [online] Available from: https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/defray-ransomware-sets-sights-on-healthcare-and-other-industries. [Accessed 19 February 2020].

[14] Landi, H. (2019) *Report: 40% of healthcare organizations hit by WannaCry in past 6 months*. [online] Available from: https://www.fiercehealthcare.com/tech/lingering-impacts-from-wannacry-40-healthcare-organizations-suf-fered-from-attack-past-6-months. [Accessed 19 February 2020].

[15] In case of crisis resolution, most countries have a possibility to summon physical persons for work duty for necessarily long time. In the Czech Republic, the work duty institute is defined in article 2 (d) of the Act No. 240/2000 Coll., On Crisis Management.

[16] Davis, J. (2020) *Ransomware Causes 15 Days of EHR Downtime, as Payments Avg $111K*. [online] Available from: https://healthitsecurity.com/news/ransomware-causes-15-days-of-ehr-downtime-as-payments-avg-111k. [Accessed 19 February 2020].

themselves, law enforcement agencies and anti-virus companies, the National Cyber and Information Security Agency (hereinafter referred to as "NCISA") also participated in resolving the impacts of the cyber security incidents described above.

3. NCISA'S ROLE IN CYBER INCIDENT HANDLING

After a brief analysis of significant cyber-attacks on medical facilities, we will describe how NCISA was involved in solving not only the cyber security incidents described above. It is the central administrative body for cyber security, including the protection of classified information in the field of information and communication systems and cryptographic protection[17]. As a regulator, NCISA determines and enforces the fulfillment of obligations in the field of cyber security of defined bodies and persons, and at the same time has the capacity to resolve cyber security incidents, especially through its organizational unit, which is the Government CERT (Computer Emergency Response Team).

NCISA actively participated in resolving incidents targeting the health sector in 2019 and 2020. Both HBEN and HBRNO had the staff directly at the scene of the incident. At the same time, in response to the attacks and their secondary threat, they did the following:

1. issued a reactive measure in March 2020[18],
2. in April 2020, they issued a warning[19] against attacks on organizations in the Czech Republic, especially hospitals.

Reactive Measure (RM) is a measure defined within article 13 (1) of Act No. 181/2014 Coll., On Cyber Security (hereinafter referred to as "ACS"). According to this article "*NCISA issues a decision ordering to take reactive measures to deal with a cyber security incident or to secure information systems or electronic communications networks and services from the cyber security incident, which is the first act in a case.*" RM is a measure the state can issue to involve state bodies into a cyber-attack resolution. From the EU legislative perspective, the Directive (EU) 2016/1148

[17] The National Cyber and Information Security Agency (2021) *About NÚKIB.* [online] Available from: https://www.nukib.cz/en/about-nukib/. [Accessed 19 February 2020].

[18] The National Cyber and Information Security Agency (2020) *NCISA issued a reactive measure for select health care subjects*. [online] Available from: https://www.nukib.cz/cs/infoservis/aktuality/1418-nukib-vydal-reaktivni-opatreni-pro-vybrane-subjekty-ve-zdravotnictvi/. [Accessed 19 February 2020].

[19] The National Cyber and Information Security Agency (2020) *Cyberattack threat at the hospitals and other significant targets in the Czech Republic.* https://www.nukib.cz/cs/infoservis/aktuality/1425-hrozba-kybernetic-kych-utoku-na-nemocnice-a-jine-vyznamne-cile-cr/. [Accessed 19 February 2020].

Of European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (hereinafter referred to as "NIS") states that "*digital service providers should be subject to light-touch and reactive ex post supervisory activities justified by the nature of their services and operations*."[20] The NIS directive also states in article 8 (5) that member States shall ensure that the competent authorities have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them and thereby to fulfil the objectives of the NIS directive.

If we compare the possibilities declared by the NIS directive and the ACS to national authorities, we must conclude that the ACS empowers NCISA with much more proactive capacity to handle some cyber incidents than is required by the NIS directive. In our opinion, the Czech legislation can be an inspiration for other states as well, especially in the case when the revision of the NIS directive is being prepared.

The issuance of the reactive measure is an act by which NCISA can order selected addressees to do something and/or refrain from doing so. This is to increase the security of the systems, and thus prevent or resolve a cyber security incident. From the point of view of resolving a security incident, this is the reactive power of NCISA, which can, with this institute, correct the security of information or communication systems if the condition of response to the incident is met. It should be added that NCISA may issue such a measure only in relation to those systems and entities affected by the Cyber Security Act, and the administrators of these systems are then obliged to notify the NCISA of the implementation of the measure and the manner of its implementation.[21]

Reactive measures may be issued on the general basis by measures of the general nature or by the decision pursuant to the Administrative Procedure Code. A measure of the general nature is issued if the number of addressees is not limited or not specified[22] and takes effect immediately by posting on the official notice board of NCISA[23]. Its efficiency is therefore significantly accelerated compared to the standard state. The decision according to the Administrative Procedure Code is addressed to a specific administrator(s) of critical information infrastructure systems, essential

[20] Recital 60 NIS.
[21] Article 13 (4) ACS.
[22] Article 13 (3) ACS.
[23] Article 15 ACS.

service, or a significant information system. The fact that this authorization of NCISA is to respond to acute threats or incidents is emphasized by the fact that the appeal filed against the decision has no suspensive effect.

Reactive measures responding to attacks on medical facilities were issued on 17th March 2020 and were addressed to those medical facilities that fall under the ACS as operators of the essential service. In the conditions of the Czech Republic, there were a total of 16 medical facilities.

The reason for issuing this specific reactive measure was both the attacks on HBEN and HBRNO and the effort to minimize the risk of similar incidents in the future, i.e. securing ICT systems against cyber security incidents.

The reactive measure in question required the addressees to perform a total of 20 specific actions divided into 4 sets according to the time frame for their fulfillment. At the same time, it contained the legitimacy of non--performance of any of the acts, in such a way that the act is not necessary to perform if its performance would cause a greater impact than the incident itself. A methodology was issued for the reactive measure, which specified it, stated the objectives of individual actions and recommendations for their implementation. The content of the reactive measure can be described as follows:

1. *without delay:*

Avoid interconnection of systems except when necessary. Interconnection between systems allows an attacker from one system to access another system. For each connection, it is therefore necessary to consider whether it is absolutely necessary and, if not, not to allow such a connection at all. We assume that all connections are a-priori prohibited and whitelisting, not blacklisting techniques, are employed to allow connections only when necessary and always to the smallest possible extent.

Avoid communication to the Internet except when necessary. If a system can communicate to the Internet without restrictions, an attacker can download data to/from it and/or attack it from anywhere if it is directly accessible from the Internet. It is therefore advisable to use restrictive firewall settings and not allow outgoing communication to the Internet. If the system already needs to communicate to the Internet, such as some

modalities, it is appropriate to use egress filtering (i.e. outbound filtering) and allow access only to a whitelisted set of IP addresses.

Separate the network of medical devices from the rest of the network. Specialized medical devices (modalities) often need to communicate to the Internet. However, these modalities may be obsolete, without new updates, and therefore vulnerable. Such devices must be isolated from the rest of the medical device's network by being allocated to a separate network segment. A more suitable solution seems to be to create one isolated network segment for each modality. Furthermore, it is appropriate not to allow communication in between the modality network(s) and other networks except for the absolutely necessary individual cases, which will be determined by whitelisting.

Change the passwords of privileged accounts. The password change was forced due to the installation of malware on the computer system. As such, malware could intercept, among other things, already used user's passwords. A privileged account allows access to and control of critical systems. This account allows to bypass standard security mechanisms and manipulate sensitive data stored in ICT systems and applications. These are usually administrator accounts for software and hardware operated within the organization, administration scripts, user and application accounts, accounts for social networks, etc.

Report to the NCISA the current IP ranges. The aim of this action is usually to obtain data to facilitate the investigation of the incident and possible further attacks. At the same time, ranges are an important source of data for checking whether they are not present in the investigated malicious communication. NCISA can also perform vulnerability scans and provide other services upon request. Therefore, it is necessary to report a list of both public IPv4 and IPv6 address ranges.

2. *within 2 days:*

Move backups offline and check the functionality of backups. If the backup is offline, it cannot be attacked by a remote attacker with a ransomware attack. Therefore, it is important to have at least part of the backups offline. It is also important to verify that the recovery from the backup works correctly.

Do not delete data on cyber security incidents. Most hardware and software record data about their activities in operational records (logs). For example, logs can contain IP addresses, usernames, timestamps, and other

information that may be important in resolving cyber security incidents. This data should have sufficient retention so that it can be used to obtain more detailed information in the event of an incident.

Check sent indicators of compromise. NCISA sends compromise indicators (IOC) to selected subjects. These most often take the form of IP addresses, the occurrence of which should be checked in the operational records. If an IOC address appears in the records, it cannot be ruled out that one of the systems has been compromised and further steps need to be taken to verify the potential attack.

Alert employees to the risk of phishing. Phishing is very sophisticated today, so it is necessary to periodically train and check employees. Phishing does not have to take the form of a fake, trusted-looking e-mail that is written in good Czech, for example from a supervisor. These can be, for example, lost keys with the hospital logo and a USB stick on which the malware is located. Bare insertion of the stick into a computer can start off the infection. Therefore, it is necessary to periodically train and test employees so that they do not open unknown attachments, connect unknown devices to the computer, and do not share any login details (social engineering) with anyone. In case of suspicion and finding of the device or an attempt to obtain login information, for example by phone, employees should be trained to contact a designated employee.

3. *within a week:*

Verify that backups are separated so that even a privileged administrator cannot delete them. An attacker could use software tools to gain the access to a privileged administrator account, as well as the right to delete any file, including backups. Therefore, you must verify that even the highest--privileged account does not have permission to delete and/or overwrite backups. This can usually be solved by using local accounts instead of accounts located in the Active Directory.

Disable the use of unsigned macros if possible. Much of the malware spreads through infected Microsoft Office documents and takes the form of macros. They can be enabled by the user to start the first phase of the infection. Macros can be digitally signed with the private key to the Microsoft Authenticode digital code signing certificate, making them trusted. To prevent random users from running unsigned macros, it is a good idea to disable this organization-wide through the Administrative

Templates files and the Office Customization Tool for Microsoft 365 Apps and Enterprise, Office 2019, and Office 2016 in the Active Directory domain.

Check network segmentation and control between segments. Proper network segmentation and well-set segment interconnection rules can greatly reduce the impact of ransomware infection. The network should therefore be divided into segments, with intersegment communication being a priori denied. Only communication that is necessary and to the least extent possible should be allowed by whitelisting.

Tighten endpoint security policies (ban on running unapproved applications, unsigned PowerShell, etc.). The Microsoft Windows operating system allows you to list applications that the user can run through Group Policy in the form of whitelisting. It is also advisable to disable unsigned scripts for Microsoft PowerShell on this system. Whitelisting of running applications also offers other operating systems, and especially on mobile devices that connect to the LAN (tablets and mobile phones), this is important because these devices are often neglected.

If business continuity management is not implemented – develop business continuity plans at least for key systems. Business continuity management allows you to foresee potential threats and provides plans for their solution. There should be offline plans for key systems that can be used in the event that the system becomes infected with malware and becomes unavailable.

Perform a vulnerability scan in systems accessible from outside the organization. NCISA offered to perform the scan. A periodic scanning of vulnerabilities on public IP addresses allows the organization to verify that unwanted services are not exposed to the Internet, and that systems are properly updated and do not contain known vulnerabilities.

4. *within 2 weeks:*

Deploy antivirus on all relevant devices. Deployment of an antivirus solution on all relevant devices, including client stations, file and mail servers. Antivirus and antimalware software is a necessary security layer today and is not the domain of the Microsoft Windows operating system alone.

Consider deploying updates after testing them. Deploying system updates can be problematic in an enterprise environment due to concerns about breaking system functionality by applying a patch. Nevertheless, it is important to prioritize security patches.

Note that patches can be tested before deployment. Whether a patch should break something, if it is not available, or if it cannot be applied, it is important to consider isolating the non-patched system from the surrounding network.

At the time of the issuance of the reactive measure, it is necessary to consider as essential or critical steps those that have the shortest time interval given for their fulfillment.

In this context, the change of passwords of privileged accounts (measures responding to the situation in the already compromised network), prevention of network interconnection and disconnection of unnecessary services from access to the Internet (measures against possible attacks) can be emphasized.

The section described the role of NCISA in solving cyber security incidents. It described how the reactive measure was being issued, including the specific steps taken by NCISA in response to the HBEN incident. The framework of the actions of the reactive measure issued on 17th March 2020 was also presented. In the next section we will summarize long-term recommendations for dealing with ransomware attacks and compare them with the recommendations of the US Cyber security & Infrastructure Security Agency and its warning AA 0-302 A[24].

4. LONG-TERM RECOMMENDATIONS FOR HANDLING RANSOMWARE ATTACKS IN THE HEALTHCARE SECTOR

In the long run, ensuring cyber security is a range of individual measures that are often mutually supportive and interlinked. If we limit ourselves to measures responding to ransomware attacks, it is necessary to recommend at least from the above-mentioned and detailed measures:

Regular staff training. The attackers focus on the weakest point in the organization. The weakest point means usually people, i.e. users and administrators. It is important to constantly increase security awareness through introductory and periodic training. To maintain awareness and vigilance, it is also advisable to conduct testing, for example, through internal phishing campaigns, which can both verify the effectiveness of security training and keep users alert.

[24] Cybersecurity & Infrastructure Security Agency (2020) *Alert (AA20-302A) Ransomware Activity Targeting the Healthcare and Public Health Sector* [online] Available from: https://us-cert.cisa.gov/ncas/alerts/aa20-302a. [Accessed 19 February 2020].

Significant network segmentation. Network segmentation is a key measure to limit the spread and thus the amount of data affected in the event of a ransomware attack. Network segmentation allows to include, for example, classic users or modalities into various segments. Modalities have a much longer lifetime than traditional ICT equipment and often run on platforms that are no longer supported. If network segmentation is missing, an attacker can move virtually unrestricted in the organization, causing much larger damage. Individual segments can then have differently set permissions and options for where they connect and who accesses them[25].

Minimize the use of administrator accounts. The use of privileged accounts should be restricted on the basis of the principle of minimum privileges. Thus, privileged rights should be granted only to those who absolutely need them, and at the same time privileged accounts should be used only when absolutely necessary. The need to grant a privileged authorization to each specific account should be assessed periodically and, if the condition of necessity ceases, the authorization should be revoked. If the privileged account is compromised by ransomware, a significantly greater amount of damage can be expected.

Backup, regularly test backups, keep backups offline. Backup is a basic and effective measure against the effects of ransomware. Backing up your organization's data from ransomware may not protect it, but it can repair the damage. Backups work if done correctly. NCISA recommends the following backup rules:

- Rule 3 – 2 – 1 = At least 3 copies on 2 different devices, of which 1 outside the organization.
- Inactive backup = At least one or more backups shall be inactive (offline) at one time. Consistently deploy identity management and access control for cloud backups.
- Recoverability and recovery plan = Backups shall be tested and usable for recovery.

Regularity and existence of a backup plan = Backups shall be created regularly[26].

Have business continuity plans (BCMs) and test them. Even the best security is not 100% guarantee that an incident will not occur. In addition

[25] Donovan, F. (2019) *How Network Segregation, Segmentation Can Stop Ransomware Attacks.* [online] https://hitinfrastructure.com/features/how-network-segregation-and-segmentation-can-stop-ransomware-attacks. [Accessed 19 February 2020].

to preventive measures, it is also necessary to think about reactive measures. In particular, it is necessary to have a functional recovery plan, which will clearly define the individual systems and their prioritization with regard to the impact on the achievement of organizational goals, deadlines and responsibilities for individual actions and, last but not least, procedures for system recovery. It is advisable to test these plans regularly to ensure that they are up-to-date, functional and usable in a crisis situation. Requirements for continuity plans can be found, for example, in the Cyber Security Ordinance or in IEC/ISO 22301[27].

Regularly check applications accessible from the Internet and evaluate whether they are still necessary. Organizations often have services open to the Internet. It is completely logical, because through these services, users, administrators or suppliers can access the ICT environment. Attackers can try to break into these services and gain access to the system. It also happens that organizations have historical services open to the Internet, which administrators do not know or maintain for various reasons. These services become vulnerable and very dangerous because they can be used by attackers to break into the organization.

For comparison, we present a set of recommendations issued by the Cyber security & Infrastructure Security Agency (hereinafter referred to as "CISA"). Within the Alert (AA 0-302A) on Ransomware Activity Targeting the Healthcare and Public Health Sector[28], as an immediate response to a similar type of attack as in the Czech Republic, the recommendations were divided into levels:

- Network infrastructures
  - Patch operating systems, software, and firmware as soon as manufacturers release updates.
  - Check configuration for every operating system version for HPH organization-owned assets to prevent issues from arising

[26] The National Cyber and Information Security Agency (2020) *Ransomware: Recommendations* for Mitigation, Prevention, and Reaction. [online] Available from: https://www.nukib.cz/download/publikace/pod-purne_materialy/Ransomware%20-%20Doporuceni_pro_mitigaci_prevenci_a_reakci.pdf. [Accessed 19 February 2020].

[27] European Union Agency for Cybersecurity (2020) *Procurement Guidelines for Cybersecurity in Hospitals*. [online] Available from: https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services. [Accessed 19 February 2020].

[28] Cybersecurity & Infrastructure Security Agency (2020) *Alert (AA20-302A) Ransomware Activity Targeting the Healthcare and Public Health Sector* [online] Available from: https://us-cert.cisa.gov/ncas/alerts/aa20-302a. [Accessed 19 February 2020].

that local users are unable to fix due to having local administration disabled.
    - Regularly change passwords to network systems and accounts and avoid reusing passwords for different accounts.
    - Use multi-factor authentication where possible.
    - Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.
    - Implement application and remote access allow listing to only allow systems to execute programs known and permitted by the established security policy.
    - Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
    - Audit logs to ensure new accounts are legitimate.
    - Scan for open or listening ports and mediate those that are not needed.
    - Identify critical assets such as patient database servers, medical records, and telehealth and telework infrastructure; create backups of these systems and house the backups offline from the network.
    - Implement network segmentation. Sensitive data should not reside on the same server and network segment as the email environment.
    - Set antivirus and anti-malware solutions to automatically update; conduct regular scans.
- Ransomware Best Practices
    - Regularly back up data, air gap, and passwords protect backup copies offline.
    - Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, secure location.
- User Awareness Best Practices
    - Focus on end user awareness and training about ransomware and phishing.
    - Ensure that employees know who to contact when they see suspicious activity or when they believe they have been a victim

of a cyberattack. This will ensure that the proper established mitigation strategy can be employed quickly and efficiently[29].

If we compare the content of the reactive measure with the recommendations of NCISA and CISA, we come to a strong agreement. However, as it turns out, despite high-quality recommendations in the field of cyber security, which aim to reduce the risk of security incidents caused by ransomware attacks, these recommendations are not mandatory, except for actions of reactive measures for entities within the scope of the ACS. The following section will discuss how NCISA can proceed in the prevention of incidents in the healthcare sector.

5. NCISA'S CYBER ATTACK PREVENTION POSSIBILITIES IN THE HEALTHCARE SECTOR

Reactive measures as they are defined by the ACS cannot be applied to organizations that do not fall within the scope of the ACS[30]. Due to the fact that the ACS, and thus also reactive measures, covers only a small part of the total number of medical facilities (only 16 medical facilities in the Czech Republic fell under the ACS in 2020, as they were operators of essential service according to Article 3 (g) ACS), in response to cyber-attacks, NCISA was forced to issue recommendations for health service providers supplemented by a methodology.

16th April 2020, NCISA issued, in accordance with Section 12[31] of the ACS,

> "*Cyber Security Threat Warning, consisting in the implementation of a large-scale campaign for serious cyber-attacks on information and communication systems in the Czech Republic, especially medical systems*[32]."

---

[29] Cybersecurity & Infrastructure Security Agency (2020) *Alert (AA20-302A) Ransomware Activity Targeting the Healthcare and Public Health Sector.* [online] Available from: https://us-cert.cisa.gov/ncas/alerts/aa20-302a. [Accessed 19 February 2020].

[30] Adressees of the reactive measure are obliged subjects defined in Article 3 ACS.

[31] The institute of warnings is defined in Section 12 of the ACS as an act to be issued by the NCISA if it "*learns in particular from its own activities or at the initiative of the national CERT operator or from bodies performing activities in the field of cyber security abroad about the threat in cyber security.*"

[32] The National Cyber and Information Security Agency (2020) *Cyberattack threat at the hospitals and other significant targets in the Czech Republic.* https://www.nukib.cz/cs/infoservis/aktuality/1425-hrozba-kybernetickych-utoku-na-nemocnice-a-jine-vyznamne-cile-cr/. [Accessed 19 February 2020].

The warning is published on the NCISA website and sent to obliged subjects in accordance with the law[33].

NCISA's own findings and warnings from partners led to the issuance of a warning dated 16th April 2020, and this information raised legitimate concerns about the real threat of serious cyber-attacks on important targets in the Czech Republic, but above all on medical facility systems.

The threat of these attacks was classified as high, i.e. grade three on the four-point scale used by the NCISA. Such a threat is therefore probable to very probable (51-75%)[34].

As such, an alert does not directly impose rights or obligations, but defines the threat and its severity. Entities falling under the ACS must work with this threat and take it into account in their own risk analysis. The entities concerned must respond to these risks by applying appropriate and proportionate organizational and technical measures[35].

In the issued warning, the Agency also recommended that the following actions be taken:

- Warn users against spear phishing.
- Prevent macros from running in Microsoft Office products.
- Block unnecessary access from the external Internet to the hospital's network infrastructure.
- Implement offline backups including checks of their functionality.

The warning itself was further supplemented by a recommendation, which included other actions to increase the security of organizations[36].

This warning expired on 20th May 2020. According to the justification,

> "*the probability of the threat that was the subject of the warning decreased, i.e. intensity of the threat for which the warning was issued was reduced.* [37]"

---

[33] Article 12 (2) of the ACS.

[34] NCISA uses a 4-point threat severity scale. This scale is also used in the Cybersecurity Decree, Annex 2. Threat severity is evaluated as: 1 – low, threat does not exist or has low probability (probability 0-25 %), 2 – medium, threat is low probable to probable (26-50 %), 3 – high, threat is probable to highly probable (51-75 %), 4 – critical, threat is highly probable to more or less certain.

[35] The National Cyber and Information Security Agency (2020) *Supplementary materials*. [online] Available from: https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/. [Accessed 19 February 2020].

[36] The National Cyber and Information Security Agency (2020) *Recommended security measures to warning from 16th April 2020. Supplementary material.* [online] Available from: https://www.nukib.cz/down-load/uredni_deska/Doporuceni_k_varovani_2020-04-17.pdf. [Accessed 19 February 2020].

[37] Article 6 justification to end a warning, https://www.nukib.cz/cs/uredni-deska/.

This section stated the possibilities of NCISA in the field of prevention of cyber security incidents. Unfortunately, even the warning does not impose any obligation to take any action, so the following section will analyze the regulatory requirements in the field of cyber security in the health sector to propose adjustments that would increase the number of entities covered by ACS and further enforce a minimum-security level for this sector.

6. APPLICABLE LEGAL FRAMEWORK IN THE CYBER SECURITY WITHIN THE HEALTHCARE SECTOR

The aim of this chapter is to present the regulatory framework of cyber security and its specific impact on the health sector.

At the EU law level, we can observe ongoing significant changes based on awareness of the cyber security attack risks and insufficient security of key systems of individual member states. The security enhancement of personal data and medical data can be observed in 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, GDPR). Beside GDPR, the cybersecurity area was also codified in the NIS directive, which states that the magnitude, frequency and impact of security incidents are increasing, and represent a major threat to the functioning of network and information systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union.[38]

The NIS directive defines in article 4 an *operator of essential services* term. A subject is an *operator of essential services* if it meets criteria laid down in Article 5 (2) of the NIS directive.

According to the NIS directive, the following is required to the essential service and to the health sector particularly:

> *„in addition to the cross-sectoral factors, sector-specific factors should also be considered in order to determine whether an incident would have a significant disruptive effect on the provision of an essential service. With*

[38] *DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. [online] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN. [Accessed 20 February 2020].

regard to health sector, it could be the number of patients under the provider's care per year, provided services etc. "[39]

The Czech Republic implemented the requirements from the NIS draft into the ACS yet in 2014, that is 2 years before the NIS directive came into effect. Based on the experience NCISA earned since the ACS came into effect and increasing number of attacks, it was necessary to amend the ACS and the underlying decrees several times, including criteria for determination of the operator of essential service in health care. The experience also helps adjusting a minimal legislative standard for these operators not only in the Czech Republic, but also in other member states or during the NIS revision process.

ACS regulates:

"*the rights and obligations of persons and the competence and powers of public authorities in the field of cyber security, incorporates the relevant regulations of the European Union and regulates the security of electronic communications networks and information systems*. [40]"

The ACS does not affect all users of cyberspace, but only the entities listed in Article 3 ACS. Regarding the determination of whether a medical facility falls under the competence of the ACS, the obligatory subjects according to Article 3 (c), (d), and (f). Particularly speaking about:

(c) an operator and an administrator of a critical information infrastructure information system,

(d) an operator and an administrator of a critical information infrastructure communication system,

(f) an operator and an administrator of an information system of essential service, unless they are the operator, or the administrator specified in letters c) or d).

Ad c) and d)

Critical information infrastructure is Article 2 (b) ACS defined as an element or system of elements of critical infrastructure in the field of communication and information systems in the field of cyber security.[41]

Critical infrastructure (hereinafter also "CI") and thus also critical information infrastructure (hereinafter also "CII") is determined according

[39] Recital 28 NIS.

[40] Article 7 ACS justification to end a warning, https://www.nukib.cz/cs/uredni-deska/.

to cross-sectional and sectoral criteria in the field of cyber security in Article 2 (i), Crisis Act and further in Government Order No. 432/2010 Coll. on the Criteria for the Identification of a Critical Infrastructure Element (hereinafter also "OCID").

According to the OCID, it is a necessary precondition for the inclusion of a medical facility in a critical infrastructure that such a facility has at least 2,500 acute beds.

However, there are no medical facilities that meet this condition in the Czech Republic, and therefore, according to the current legal framework, no medical facility can be included in CI.

Regarding the connection to the CII, it is necessary to assess the fulfillment of the criteria in the sector: VI. Communication and information systems, part G – Cyber security. Five criteria are defined here, which state that a critical information infrastructure can be identified:

a) an information system which significantly or fully influences the activity of an identified element of critical infrastructure, and which is at the same time replaceable only if excessive costs are incurred or in a time period of more than 8 hours,
b) a communication system which significantly or fully influences the activity of an identified element of critical infrastructure, and which is at the same replaceable only if excessive costs are incurred or in a time period of more than 8 hours,
c) an information system which is operated by a public authority that execute public powers which contains personal data of more than 300,000 people,
d) a communication system securing the connection or interconnection of an element of critical infrastructure, with a capacity of guaranteed data transmission of at least 1 Gbit/s,
e) sectoral criteria for the identification of a critical infrastructure element specified in A to F shall be used adequately for the field of cyber security, if the protection of the element fulfilling these criteria is necessary to ensure cyber security.

If we study the criteria in more detail, we will find that the first two criteria allow to determine as CII only those systems that affect the specified

[41] The very concept of critical infrastructure is defined by Act No. 240/2000 Coll., On Crisis Management (Crisis Act), which states "*that it is a complex of elements (in our case, information and communication systems), the disruption of which could have a serious impact on security of the state, provision of the basic living needs of the population, health of persons or the economy of the state.*" See article 2 (g) Crisis Act.

element of CI, while medical facilities do not meet this condition. Of the other criteria, it is possible to apply only the criterion listed under letter e) to medical facilities, but the fulfillment of this criterion is relatively difficult to assess in reality, and it is also proven due to its uncertainty and vagueness. In addition to the sectoral criteria, NCISA must prove the fulfillment of cross-cutting criteria in the process of assessing the inclusion of a certain entity in the CII. This can be difficult in the context of healthcare facilities, as there is no inclination in healthcare legislation. It is thus difficult to prove how many potential patients will be affected by the failure of a particular medical facility. However, proving the fulfillment of cross-sectional criteria is a necessary condition for identifying hospitals and their systems as CII. At the same time, there is currently no satisfactory key in the form of sectoral criteria for identifying major healthcare facilities.

Cross-sectional criteria are an important filter for determining CII and are defined in Article 1 of the OCID. When learning an element of a critical information infrastructure, any disruption of this system must be able to cause:

a) more than 250 casualties or more than 2,500 people who needed hospitalization for longer than 24 hours,
b) economic impact with threshold value of economic loss greater than 0.5 % of GDP or,
c) impact on society with threshold value of a large limitation of necessary service provision or another serious intervention into the daily life of more than 125,000 people.

The sectoral criteria of the government regulation for determining CIs are in sector IV. Healthcare, by the Ministry of Health set up so that no medical facility meets them. From the authors' point of view, it would be logical to set these criteria to cover at least the most important players in the industry.

In this case, it is necessary to agree with the conclusions of Harasta, which he states

> *"If we state that the purpose of the legislation is to protect critical infrastructure effectively and efficiently, the current Czech legal development suggests that our statement might be wrong and misguided. The law on its operative level does not sufficiently reflect the broad definition*

on a strategic level. Cross-cutting and sectoral criteria allow us to approach certain interdependencies selectively, but not to cover them exhaustively. The broad definition of critical infrastructure as present within legal framework of EU and, as demonstrated on the case of the Czech Republic, in its member states, furthers the securitization of the issue by labeling it as influential enough to move into the realm of law and to achieve institutionalization within its framework. Since the strategic level with its broad definitions has a purpose, simplistic lower-level norms are justified to a certain extent, because they allow for administration in the issue. Therefore, a legal framework of critical infrastructure protection does not present a significant legal value that needs to be maintained – it merely mirrors the lax or active role this issue plays within policy discussions[42]."

Ad f)

Operators of essential services (OES) represent another group of obligated persons according to the ACS, under which possible medical facilities could be included. Operators of essential services represent a group of obliged subjects that were included in the ACS by a transposition amendment to the Act in 2017. This group of liable persons is determined by NCISA pursuant to Decree No. 437/2017 Coll. on the criteria for the determination of an operator of essential service (hereinafter also "DCRIT").

These criteria were defined by the DCRIT, until 31st December 2020, as follows:

a) a total of at least 800 acute care beds in the last three calendar years or
b) the status of a facility for highly specialized trauma care according to the Act on Health Services.

These special criteria for the type of entity represent the importance of the entity in the industry in terms of the size and scope of the services provided. As of 31st December 2020, only 16 medical facilities in the Czech Republic met these criteria.

In the light of the incidents described in the previous chapter, NCISA proceeded to amend the DCRIT, specifically the special criteria of the types of entity. The aim of this change was to expand the number of hospitals that

[42] Harašta, J. (2018) *Legally critical: Defining critical infrastructure in an interconnected world*. International Journal of Critical Infrastructure Protection, vol. 21, pp. 47-56. Elsevier. ISSN 1874-5482.

could be included under the ACS as OES. The criteria are therefore as follows from 1st January 2021 (changes compared to the previous version are marked in bold):

a) the total number of acute beds in the last three calendar years is at least 400, the status of a center of highly specialized traumatological, oncological, cerebrovascular, cardiovascular, complex cardiovascular or perinatological care according to the Act on Health Services,
b) provision of emergency admission according to the Act on Ambulance Service in facilities with a total number of intensive care beds in the last three calendar years of at least 40 or
c) an acute inpatient care provider with an average number of uniquely treated patients in the last three calendar years of at least 100 000 per calendar year.[43]

If at least one of the above special criteria meets the type of medical facility entity, its systems may be assessed in relation to the fulfillment of the impact criteria, which are set at Decree No. 437/2017 Coll., Annex, Sector 5. Health Care.[44]

As healthcare facilities are the controllers of a significant amount of personal data of a special category and data on health status, it is offered to meet at least criterion VI.

As of 31st December 2020, only 16 medical facilities were covered by the ACS, and only these facilities had to introduce safety measures pursuant to Sections 4 and 5 of the ACS, i.e. report contact details[45]

[43] Decree No. 437/2017 Coll., Annex 1, Sector 5. Health Care.

[44] Those criteria are:

The impact of a cyber security incident in an information system or electronic communications network on the operation of which the provision of a service depends may cause:

I. a serious limitation of the type of service which would affect more than 50,000 people,
II. a serious limitation or disruption of another essential service or a limitation or disruption of a critical infrastructure element,
III. unavailability of the type of service for more than 1,600 people which is irreplaceable in another way unless excessive costs were to be incurred,
IV. more than 100 casualties or 1,000 injured people in need of medical treatment or,
V. disruption of public safety in a significant part of the administrative territory of a municipality with extended powers, which may require rescue and liquidation operations by the integrated rescue system units, or

disclosure of sensitive data of more than 200,000 people.

[45] Providing contact information, and therefore a possibility to contact an organization, is an elementary condition for a timely warning and reaction to an imminent cyber-attack. As well as fast notification. Under current conditions, notifications and other measures in the health care sector are only enforceable with difficulties or not at all.

pursuant to Section 16 or comply with measures pursuant to Section 11 of the ACS. It should be added that the organization will be designated as an OES by a decision in administrative proceedings issued by NCISA. Thus, the mere fulfillment of the criteria does not in itself mean the obligation to follow the law immediately.

There are currently at least 232 health care providers in the Czech Republic – medical facilities with inpatient care. We list at least 232, because this number fluctuates more than usual due to the pandemic. The number of 232 was determined on the basis of information from open data published on the website of the National Register of Health Data Providers for the period 1st January 2021 – 31st January 2021[46].

Filtering according to the "*FormaPece*" (type of health care service) field was applied to the data for the occurrence of the word "*lůžková*" (accute beds) and at the same time the "*DruhZarizeni*" (facility type) field for the occurrence of the word "*nemocnice*". The number of 232 medical facilities does not include long-term care hospitals. The numbers of beds were subsequently added to the data and obtained manually from the websites of medical facilities and their annual reports. It was possible to find bed capacity online only in 153 of them.

Due to the fact that all large medical facilities have been reliably added to the list, the data insufficiency is reflected only in smaller medical facilities for which the status of operator of essential service (OES) is not assumed. Medical facilities were further divided according to their bed capacity into bins of 50 beds and the numbers of hospitals in individual bins were determined. The values of the bins were cumulatively summed from 2500 beds to zero.

The following graph shows the cumulative totals obtained indicating the number of hospitals that would meet the OES criterion if set to the number of acute beds equal to the interval of their bin. Thus, it is possible to enter in the graph the minimum number of beds that are codified in law, i.e. 2500 beds for CI, 800 beds for the OES up to and including year 2020 and 400 beds from year 2021 on. Codified values are highlighted in the graph. The gaps in between the columns in the graph were shrunk to conserve space and mean that no data was available for the given interval.

[46] *Národní registr poskytovatelů zdravotních služeb*. [online] Available from: https://opendata.mzcr.cz/data/nrpzs/narodni-registr-poskytovatelu-zdravotnich-sluzeb.csv. [Accessed 20 February 2020].

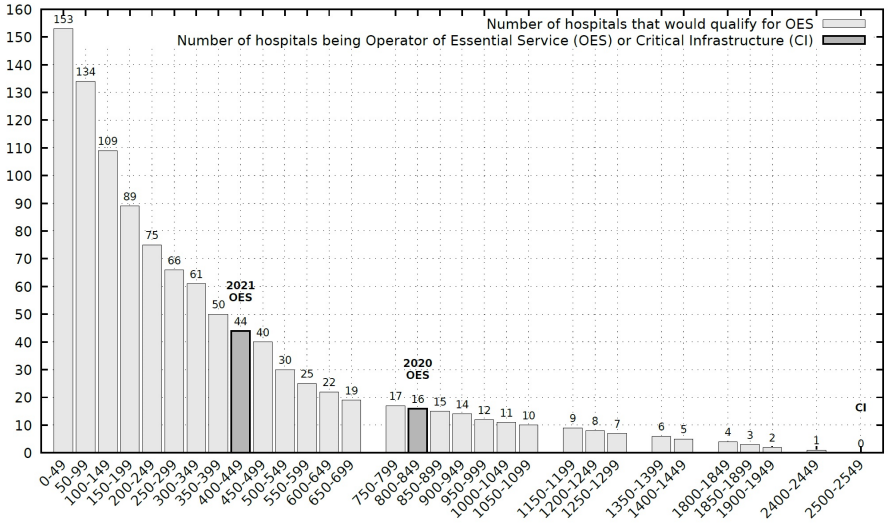

Figure 1. Cumulated number of hospitals that would qualify as operators of essential services (OES). According to the law when setting the criterion – the number of acute beds – to any number of beds from the interval under the x axis. The OES criterion was originally set to 800 beds until the end of the year 2020 and this, according to the figure above, means that there were 16 hospitals with 800 or more beds. From 1st January 2021 on the value was set to 400 beds meaning there will be an estimated total of 44 hospitals falling into the OES.

The data also revealed that adjustments to the minimum number of acute care beds from 800 to 400 beds have now included HBEN among the essential service operators with their 444 beds.

In terms of content, the issued recommendation was very similar to the reactive measure itself (see Chapter 2), but points that are not relevant for non-obligated persons were omitted (for example, the obligation to report its IP ranges to NCISA).

It is clear that NCISA, as the central administrative body for cyber security, wanted to warn other potential victims in response to the described cyber-attacks and the high level of risk of repeating these attacks. For this reason, the recommendation was issued and distributed on 18th March 2020, i.e. immediately after the issuance of the reactive measure[47].

[47] The National Cyber and Information Security Agency (2020) *NCISA issued a reactive measure for select health care subjects*. [online] Available from: https://www.nukib.cz/cs/infoservis/aktuality/1418-nukib-vydal-reaktivni-opatreni-pro-vybrane-subjekty-ve-zdravotnictvi/. [Accessed 19 February 2020].

The recommendation from NCISA as a means of legal coercion of another entity is non-binding and was sent to 85 medical facilities. These 85 medical facilities were designated by the Ministry of Health as the backbone.

This section presented an analysis of regulatory requirements in the field of cyber security for health care providers and provided a graph estimating the number of health care facilities (primary care providers) depending on the minimum number of acute beds. Based on the application of legislative requirements and analysis of available data, it was found that none of the medical facilities in the Czech Republic is part of the critical infrastructure because it does not meet the minimum number of acute beds at 2,500, although one of the hospitals is close to this limit.

It was further stated that until 31st December 2020, only 16 health care facilities met the criterion of a primary care provider and that this criterion was reduced to 400 as from 1st January 2021. Finally, a graph was presented estimating the number of health care facilities among providers of essential services with an accuracy of 50 beds.

The number of medical facilities falling under the ACS since 1st January 2021 has not yet been published, but we can estimate from the graph that there will be approximately 44 medical facilities.

The next part of the article will deal with proposals for amendments to legislation that could further contribute to the cyber security of medical facilities.

7. LEGISLATIVE MEASURES NECESSARY TO INCREASE THE CYBER SECURITY OF MEDICAL FACILITIES

If we summarize the incidents described in the first chapter of this text in terms of ICT implications, it can be stated that the confidentiality, integrity or availability of these systems may be compromised, and thus, for example, complete system control, unavailability, data theft or unauthorized modification. No data theft was detected in the attack cases described above. However, there may also be inaccessibility of information, services and malfunctions of specialized facilities, which has actually happened. The effects of a successful ransomware attack on an affected organization are often fatal in such cases. The organization ceases to function, physical damage to property can occur, and in the case of hospitals, life and health

can also be endangered. The reputational and financial implications are almost certain.

A successful attack is not out of the question even with the best preventive measures, and therefore the existence of business continuity plans is absolutely crucial for minimizing the impact of attacks and rapid recovery. From the above-described attacks i tis clear that the disruption of information systems of medical facilities has real consequences. In the Czech Republic these facilities fall under the ACS only to a very limited extent and there is no uniform and enforceable security standard for medical facilities and their ICT systems. Also, no functional communication platform has been created by Ministry of Health that could quickly, accurately and intelligibly inform about cyber-attacks outside the ACS system.

The NCISA's competences are strictly defined by the ACS.

The measures and recommendations summarized above were all meant with good intention, yet they may be difficult to implement.

After analysis of the cyber security incidents at Czech hospitals occurring during the COVID-19 pandemic and discussion with medical care cyber security experts that were unaffected by the attack, we have to conclude that there is no "collective intelligence". There is no platform on which health care providers (and other sectors) could share data on collectively, to learn from, and to acquire and apply experiences of others.

As an appropriate collective intelligence solution, authors propose to create a cyber-attack information coordinator, perhaps per sector, within NCISA or the National CSIRT team. It is a question whether these organizations are understood as a trustworthy partner for the hospitals and other sector organizations, as trust can be built by active approach to share data about attacks and by presentation of appropriate measures[48].

Despite the following text may seem highly technical, authors believe that the depth is necessary for proper definition of minimal security standards in healthcare as a key element for ensuring cyber security in the sector.

On the other hand, it can be stated that the state or territorial self--governing units should also play an important role in the protection

[48] Kolouch, J., Zahradnický T. and Kučínský A. (2021) *Cyber Attacks on Czech Hospitals in the Covid-19 Pandemic.* Unpublished manuscript.

of medical facilities. The state and its bodies are entitled to do only what is expressly permitted by law. For this reason, it was necessary to adjust the legislative framework of these powers in at least the following areas:

• **Amendment of Decree No. 432/2017 Coll. so that more medical facilities are included in the category of operators of essential services (OES)**

By changing the criteria set out in this Decree for operators of basic healthcare services, it is relatively easy to increase the number of healthcare facilities included in the ACS system. NCISA, just in response to the described attacks, has already amended this decree.

According to the available information, the described change allows for the inclusion of another 30 health care facilities in the OES system, i.e. a total of 46 health care facilities could be the operator of basic services in the health care sector.

It is therefore possible to assess whether NCISA has set the change in regulation sufficiently and whether the newly set criteria for determining the operators of basic services are adequate (see the analysis in Chapter 5).

The special criteria for the type of entity for the determination of OES in the healthcare sector are newly established as follows:

a) a total of at least 400 acute care beds in the last three calendar years,

The criterion is basically the same as in the previous version of the decree, but the number of acute beds is reduced from 800 to 400.

b) the status of a facility for highly specialized traumatological, oncological, cerebrovascular, cardiovascular, complex cardiovascular or perinatological care according to the Act on Health Services,

Compared to the previous version of the decree, there is an expansion of medical disciplines in this criterion, when in the original version only one type of center of highly specialized care was mentioned, namely trauma care.

In the Czech Republic, the status of a highly specialized care center is granted in a total of 14 medical fields[49], of which a total of 6 are in the area of cyber security regulation.

[49] A list of centres of highly specialized care in The Czech Republic – Ministry of Health of The Czech Republic.

This extension, in contrast to the original trauma care only, can be described as a step in the right direction, as it will cover other key medical disciplines and services for patients.

c) provision of emergency admission according to the Act on Ambulance Service in a facility with a total number of intensive care beds in the last three calendar years of at least 40,

This is a completely new criterion, which was not in the original version of the decree. This criterion is intended to cover medical facilities to which the emergency medical service is linked. Urgent income is regulated by Act No. 374/2011 Coll., On the ambulance service, which stipulates that it means:

> "*a specialized workplace of a provider of acute inpatient care with continuous operation, which ensures the receipt and provision of intensive acute inpatient care and specialized outpatient care to patients with sudden serious damage to health and to life-threatening patients*. [50]"

The regulation is now also focused on those medical facilities where the emergency medical service primarily transports patients with acute problems.

Acute care is defined by Act No. 372/2011 Coll., On health services and as a type of health care, the aim of which is to

> "*avert a serious deterioration in health or reduce the risk of a serious deterioration in health so that the facts necessary to determine or change individual treatment or that the patient does not end up in a condition that endangers himself or his surroundings*[51]."

In-patient care is then divided by the same law into acute in-patient care, intensive care and acute standard inpatient care[52]. The criterion thus takes into account the performance of the hospital, resp. the importance of the hospital in relation to the number of patients treated.

---

[50] Article 6 (3) Z ZZS.

[51] Černý, V. (2020). *Dostupnost intenzivní péče pro hospitalizované pacienty s COVID-19*. [online] Available from: https://www.uzis.cz/res/file/covid/20200324-cerny-cz.pdf. [Accessed 19 February 2020].

[52] Article 9 (2a, 2b) Act No. 372/2011 Coll.

The total number of medical facilities with resuscitation and intensive acute care (ARO + ICU) in the Czech Republic is 136[53]. The number of ARO beds is 823 and the number of ICU beds is 3658.

d) an acute inpatient care provider with an average number of uniquely treated patients in the last three calendar years of at least 100 000 per calendar year.

This is a completely new criterion, which was not in the original version of the decree. The aim is to include in the regulation those healthcare facilities that provide their services to a large number of patients and are therefore important for the industry in terms of the range of services provided.

• **Amendment of Government Regulation No. 432/2010 Coll. so that more medical facilities are included in the Critical Infrastructure of the state**

As mentioned above, no medical facility is and cannot be presently included in the critical infrastructure of the state.

The authors believe that setting unsatisfiable criteria does not make sense and it would be appropriate to adjust them so that the most important medical facilities fall into the CI.

For example, inspiration can be found in the version of Decree No. 437/2017 Coll., Effective between 1 February 2018 and 31 December 2020:

By lowering the criterion of 2,500 acute beds to 800 acute beds and/or the status of a trauma center, it would be possible to achieve the 16 largest medical facilities as critical infrastructure.

For the regulation of cyber security of medical facilities, resp. their inclusion under the ACS would not be a problem, because according to the principle of "higher regulation takes precedence" (expressed in Article 3 (f) ACS), such an organization could be determined as CII and reassigned into this group from the OES group. This measure would include the inclusion of some medical facilities in crisis management of the country, the possibility of emergency supplies and, in general, better emergency readiness.

• **Setting a minimum-security standard for medical facilities**

The inclusion of selected medical facilities in the regulation of the ACS as one of the obliged subjects is one of the steps to increase the protection

[53] Černý, V. (2020). *Dostupnost intenzivní péče pro hospitalizované pacienty s COVID-19*. [online] Available from: https://www.uzis.cz/res/file/covid/20200324-cerny-cz.pdf. [Accessed 19 February 2020].

of these facilities against cyber-attacks. However, due to the number, diversity and different nature of medical facilities, such regulation will not and can never cover all facilities. Meeting some ACS requirements is not realistic or effective for some health care providers (for instance, due to their size).

Nevertheless, we believe that at least the basic security of medical facilities should be taken into account. It would therefore be appropriate to set a certain minimum-security standard for medical facilities in the field of cyber security. Such a standard should be relatively simple, general given the diversity of organizations, and at the same time binding so as to ensure its widespread application.

To achieve these goals, the following basic questions need to be answered:

a) Who should define the standard?

In order to create an ideal security standard, it would be appropriate to create a working group composed of representatives of regulators, i.e. NCISA and the Ministry of Health, medical facilities, especially those to whom the standard would be addressed.

It would also be appropriate to invite representatives of security forces and the professional public to the working group (e.g. National CSIRTs, auditors operating in the healthcare sector, representatives of anti-virus companies, internet connection providers, etc.).

b) What should the standard contain?

There are a number of security standards and various methodologies for their implementation. In order to determine what a standard should contain; it is appropriate to start in particular from the person for whom such a standard is intended.

The target group of this standard is healthcare providers (especially small and medium-sized hospitals). Such organizations cannot be overwhelmed by complex analyzes that they will not be able to carry out on their own. Nor can they be given a complex management system that they will not be able to apply effectively.

The measures should therefore be simple and cover the underlying risks.

If an organization wants to devote more effort to security, it can always use the regulations on cyber security, the deployment of ISMS according to ISO 27001 or similar standards.

The Minimum Safety Standard issued by NCISA, MI and NAKIT in the middle of 2020 can serve as a basic material from which it would be possible to start, and which could be tailored to the working group by medical facilities.

> "*This document offers simplified principles, procedures and recommendations in the field of cyber security for organizations that do not fall under the regulation of Act No. 181/2014 Coll., on cyber security*[54]."

Its development and modification for the environment of medical facilities is thus directly offered.

Standard, resp. the areas and measures it should cover are also described in Chapter 2 of this article. The standard should be divided in terms of risk minimization measures into two parts – organizational and technical.

The organizational part should cover the area:

- classification of information;
- planning the implementation of security measures;
- building security awareness;
- supplier management;
- change management;
- continuity management;
- cyber security control and audit.

The technical part should cover technical safety measures in at least the following areas:

- physical security;
- control of access to information systems;
- network segmentation;
- protection against malicious code;
- cryptography;
- backup;
- protection of web applications;
- security of cloud services.

When defining measures, it must be assumed that individual organizations have different ICT architectures and therefore measures should be defined in general with possible examples of application and the standard should be technology neutral.

[54] The National Cyber and Information Security Agency (2020) *Supplementary materials*. [online] Available from: https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/. [Accessed 19 February 2020].

a) What should be a suitable carrier, or on what basis should it be required and enforced?

In order to increase cyber security and the resilience of the health sector as a whole, a minimum-security standard should be mandatory. If this is not the case, cyber security cannot be expected to be considered a priority by healthcare management. In addition, as mentioned above, a minimum-security standard for non-ACS organizations exists and can be deployed voluntarily.

If the minimum-security standard were not mandatory, in the opinion of the authors, a significant improvement of the situation cannot be expected.

As obligations can be imposed in the Czech Republic on the basis of and within the limits of the law, it is necessary that the obligation to apply a safety standard be imposed by a medical facility by law.

There are basically two options. Either the obligation will be introduced in the ACS or in another, "sectoral" law. In the opinion of the authors, enshrining a similar obligation in the ACS is inappropriate, as it would disrupt its construction and purpose. The ACS affects only selected entities in various industries and defines a set of obligations for them. If specific sectoral regulations, in addition to obliged subjects other than those defined by law, begin to be added to the ACS, this appears to be unsystematic. For example, the Energy or Atomic Act also stipulates certain obligations in the field of information security, and in some cases its addressees are also the ACS addressees.

Thus, practice shows that the ACS and other, sectoral regulations, can coexist and complement each other. It therefore seems to be a suitable model to impose the obligation to comply with the security standard in a specific sectoral law, namely in Section 16 of Act No. 372/2011 Coll., On health services and the conditions for their provision (the Health Services Act), where the conditions for granting authorization to provide health services.

This would ensure the definition of clear measures to increase cyber security and the obligation to meet them as a condition for the provision of health services.

b) Who should meet the standard?

A seemingly simple question that is not easy to answer. To solve it, it is necessary to proceed from Act No. 372/2011 Coll., On health services and

the conditions for their provision (the Health Services Act). As described above, regulation by the ACS is aimed at healthcare providers with inpatient capacity, and inclusion in the scope of the ACS is conditional on meeting special criteria of the type of entity and meeting impact criteria that filter out less important organizations that would find it very difficult to introduce mandatory regulation. The impact of the law is thus limited and a certain limitation of the scope of the addressees of the minimum-security standard, if it were mandatory, would also be necessary, because there are about 39,170 health care providers in the Czech Republic, and they are diametrically opposed entities. Due to this, it is appropriate to focus the standard on hospitals with inpatient care in a similar model as the ACS regulation is now set, but with lower limits.

c) Who will require and control compliance with the standard?

If we come to the conclusion mentioned in the previous part of the text, ie that the minimum security standard and the obligation to meet it would be a condition for the provision of health services, it would be appropriate that enforcement and control be entrusted to either the Ministry of Health as the central administrative office or, as in Section 15 of the Health Services Act,

> "*the regional authority in whose administrative district the medical facility in which the medical services will be provided is, the Ministry of Defense or the Ministry of Justice, if the health services are provided in medical facilities established by these ministries, or the Ministry of the Interior, in the case of health services provided in health care facilities established by this Ministry or in health care facilities established by the Office for Foreign Relations and Information or the Security Information Service.*"

- **Setting standards for data sharing, establishing, and operating cyber security teams in healthcare sector**

A fundamental prerequisite for assuring cyber security in healthcare is establishment of a proper communication channel for efficient and fast data sharing in between individual health care providers and the government. The Ministry of Health as the top authority for the sector should provide such a channel. Paradoxically we are in a situation that the ministry disclaims from its coordinator role claiming that the cyber security area falls under another gestion based either on the NIS directive or specific law

of a member state. In the Czech Republic, neither NCISA provides any specific communication channel that could be used by the OES operators in healthcare use to share cyber threat and attack information they are facing.

From the data sharing perspective, the subjects under the ACS are obliged to share information with the Governmental CERT team, which may based on the information issue a warning. Nonetheless, the Governmental CERT team is not specifically focused on healthcare and provides its services to all subjects under the CI or OES. It is also necessary to state that the Czech Ministry of Health has not established its own security team or a Security operations centre that could provide targeted support to healthcare providers.

As an appropriate collective intelligence solution, authors propose to create a hospital Security operation centre within a Ministry of Health. Such centre would not only act as a CSIRT/CERT team, which is often part of such a centre, but could also serve as a coordinator at both the national level and multinational level when collaborating through ENISA. Such centre would also be able to receive, test, and forward recommendations from other organizations and states[55] and should take part on forming new sector standards and recommendations.

This section analyzed the legislative measures following the attacks on hospitals in the Czech Republic in the period 12/2019 and 1/2021. The measures were evaluated and amendments to several decrees were proposed that could increase the cyber security of the healthcare sector. It was also proposed to create a sectoral platform for the exchange of security information and collective intelligence. Finally, it was proposed to introduce a minimum mandatory security standard for healthcare, which would prioritize safety from the point of view of hospital management.

8. CONCLUSION

The first part of the article analyzes the cyber incidents that took place in the period from 12/2019 to 1/2021 in health care facilities in the Czech Republic. All these incidents were caused by a combination of phishing and ransomware attacks. The use of ransomware along with phishing

[55] See also: *Procurement Guidelines for Cybersecurity in Hospitals*. [online] Available from: https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services/at_download/fullReport [Accessed 19 February 2021]. *Cloud Security for Healthcare Services*. [online] Available from: https://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services/at_download/fullReport [Accessed 19 February 2021].

as an attack vector is common and not a new phenomenon, however, as it turns out, it is still effective. The attack on the Brno University Hospital can be assessed as the most fundamental of the analyzed incidents in terms of impact. These attacks sparked debate on the cyber security and resilience of hospitals.

NCISA also paid attention to the attacks on the healthcare sector. In response to incidents, they issued, inter alia, reactive measures and warnings in accordance with the Cyber Security Act. Through these actions, NCISA sought to respond to the security situation and oblige the addressees of these measures, primarily hospitals, to ensure security and vigilance. The issued measures were aimed at introducing measures against ransomware and phishing. The article analyzes these actions, especially the mentioned reactive measures, and proposes its own recommendations in connection with them.

As it turned out, the regulation of cyber security of hospitals, resp. health care in general is not sufficient and in 2020 only 16 hospitals out of the total number of 232 hospitals in the Czech Republic were within the scope of the Cyber Security Act. In 2021, NCISA amended the criteria for classifying organizations in the healthcare sector under the act with the aim of expanding its addressees. This change is then analyzed in the article. In the opinion of the authors, another legislative change would be appropriate, namely an amendment to Government Decree No. 432/2010 Coll., which would allow hospitals to be included in critical infrastructure, as no hospital meets the current criteria, and this situation seems inappropriate.

We are convicted that the findings described by us, as well as the criteria used to determine whether a health care provider will be considered an operator of essential services can be used in countries other than the Czech Republic.

The article further discusses the issue of introducing a minimum mandatory security standard in healthcare, which does not currently exist and which would cover healthcare facilities outside the scope of the Cyber Security Act. The authors recommend the creation of such a standard so that even organizations that do not fall within the scope of the Cyber Security Act have a clear framework on how to secure their systems.

A revised standard could also be issued for some specific threats. Due to the fact that the presented article analyzes attacks that combine

a phishing campaign and ransomware, we will present a possible minimum standard related to these attacks.

LIST OF REFERENCES

[1] Cybersecurity & Infrastructure Security Agency (2020) *Alert (AA20-302A) Ransomware Activity Targeting the Healthcare and Public Health Sector* [online] Available from: https://us-cert.cisa.gov/ncas/alerts/aa20-302a. [Accessed 19 February 2020].

[2] Černý, V. (2020) *Dostupnost intenzivní péče pro hospitalizované pacienty s COVID-19.* [online] Available from: https://www.uzis.cz/res/file/covid/20200324-cerny-cz.pdf. [Accessed 19 February 2020].

[3] Davis, J. (2020) *Ransomware Causes 15 Days of EHR Downtime, as Payments Avg $111K.* [online] Available from: https://healthitsecurity.com/news/ransomware-causes-15-days-of-ehr-downtime-as-payments-avg-111k. [Accessed 19 February 2020].

[4] Davis, J. (2016) *Ransomware: See the 14 hospitals attacked so far in 2016*. [online] Available from: https://www.healthcareitnews.com/slideshow/ransomware-see-hospitals-hit-2016 [Accessed 10 May 2017].

[5] Delpy, B. and Le Toux, V. (2020) *Mimikatz.* [online] Available from: https://github.com/gentilkiwi/mimi-katz/releases. [Accessed 19 February 2020].

[6] Deutsche Welle (2020) *German police probe 'negligent homicide' in hospital cyberattack*. [online] Available from: https://p.dw.com/p/3ieQl [Accessed 19 February 2020].

[7] Donovan, F. (2019) *How Network Segregation, Segmentation Can Stop Ransomware Attacks.* [online] https://hitinfrastructure.com/features/how-network-segregation-and-segmentation-can-stop-ransomware-attacks. [Accessed 19 February 2020].

[8] Elshinbary, A. (2020) *Deep Analysis of Ryuk Ransomware.* [online] Available from: https://n1ght-w0lf.github.io/malware%20analysis/ryuk-ransomware/. [Accessed 19 February 2020].

[9] European Union Agency for Cybersecurity (2020) *Procurement Guidelines for Cybersecurity in Hospitals.* [online] Available from: https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services. [Accessed 19 February 2020].

[10] European Union Agency for Cybersecurity (2020) *Cloud Security for Healthcare Services.* [online] Available from: https://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services/at_download/fullReport [Accessed 19 February 2021].

[11] European Union Agency for Cybersecurity (2020) *Procurement Guidelines for Cybersecurity in Hospitals.* [online] Available from: https://www.enisa.europa.eu/publications/good-

practices-for-the-security-of-healthcare-services/at_download/fullReport [Accessed 19 February 2021].

[12] Harašta, J. (2018) Legally critical: Defining critical infrastructure in an interconnected world. *International Journal of Critical Infrastructure Protectio*n, vol. 21, pp. 47-56. Elsevier. ISSN 1874-5482.

[13] Kolouch, J., Zahradnický T. and Kučínský A. (2021) *Cyber Attacks on Czech Hospitals in the Covid-19 Pandemic.* Unpublished manuscript.

[14] Landi, H. (2019) *Report: 40% of healthcare organizations hit by WannaCry in past 6 months.* [online] Available from: https://www.fiercehealthcare.com/tech/lingering-impacts-from-wannacry-40-healthcare-organizations-suf-fered-from-attack-past-6-months. [Accessed 19 February 2020].

[15] Mundo, A. (2019) *Buran Ransomware; the Evolution of VegaLocker.* [online] Available from: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/buran-ransomware-the-evolution-of-vegalocker/. [Accessed 19 February 2020].

[16] Proofpoint, Inc. (2020) *New Defray Ransomware Targets Education and Healthcare Verticals.* [online] Available from: https://www.proofpoint.com/us/blog/threat-insight/new-defray-ransomware-targets-education-and-health-care-verticals. [Accessed 19 February 2020].

[17] Sette, N. (2020) *Malware Analysis – Buran Ransomware-as-a-Service.* [online] Available from: https://www.kroll.com/en/insights/publications/cyber/malware-analysis-buran-ransomware-as-a-service. [Accessed 19 February 2020].

[18] The National Cyber and Information Security Agency (2020) *Cyberattack threat at the hospitals and other significant targets in the Czech Republic.* https://www.nukib.cz/cs/infoservis/aktuality/1425-hrozba-kybernetic-kych-utoku-na-nemocnice-a-jine-vyznamne-cile-cr/. [Accessed 19 February 2020].

[19] The National Cyber and Information Security Agency (2020) *NCISA issued a reactive measure for select health care subjects.* [online] Available from: https://www.nukib.cz/cs/infoservis/aktuality/1418-nukib-vydal-reaktivni-opatreni-pro-vybrane-subjekty-ve-zdravotnictvi/. [Accessed 19 February 2020].

[20] The National Cyber and Information Security Agency (2020) *Ransomware: Recommendations for Mitigation, Prevention, and Reaction.* [online] Available from: https://www.nukib.cz/download/publikace/pod-purne_materialy/Ransomware%20-%20Doporuceni_pro_mitigaci_prevenci_a_reakci.pdf. [Accessed 19 February 2020].

[21] The National Cyber and Information Security Agency (2020) *Recommended security measures to warning from 16th April 2020. Supplementary materia*l. [online] Available from:

https://www.nukib.cz/down-load/uredni_deska/Doporuceni_k_varovani_2020-04-17.pdf. [Accessed 19 February 2020].

[22] The National Cyber and Information Security Agency (2020) *Supplementary materials.* [online] Available from: https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/. [Accessed 19 February 2020].

[23] The BBC (2016) *Three US hospitals hit by ransomware.* [online] Available from: https://www.bbc.com/news/technology-35880610 [Accessed 10 May 2017].

[24] Tracey, R. and Schmitt, D. (2020) *When Threat Actors Fly Under the Radar: Vatet, PyXie and Defray777.* [online] Available from: https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/. [Accessed 19 February 2020].

[25] Trend Micro Incorporated (2017) *Defray Ransomware Sets Sights on Healthcare and Other Industries.* [online] Available from: https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/defray-ransomware-sets-sights-on-healthcare-and-other-industries. [Accessed 19 February 2020].

[26] Wadhwani, S. (2020) *Cyber World's Most Fearsome Ransomware Is Ryuk: SonicWall*. [online] Available from: https://www.toolbox.com/security/threat-reports/news/cyber-worlds-most-fearsome-ransomware-is-ryuk-sonicwall/. [Accessed 19 February 2020].

MUJLT Official Partner (Czech Republic)

ROWAN LEGAL, advokátní kancelář s.r.o.
www.rowanlegal.com/cz/

Cyberspace 2020 Partners

Vodafone Czech Republic
www.vodafone.cz

PwC Legal
www.pwc.com

Zákony pro lidi - AION CS
www.zakonyprolidi.cz

CODEXIS - ATLAS consulting
www.codexis.cz

Notes for Contributors

Focus and Scope

Masaryk University Journal of Law and Technology (ISSN on-line 1802-5951, ISSN printed 1802-5943) is a peer-reviewed academic journal which publishes original articles in the field of information and communication technology law. All submissions should deal with phenomena related to law in modern technologies (e.g. privacy and data protection, intellectual property, biotechnologies, cyber security and cyber warfare, energy law). We prefer submissions dealing with contemporary issues.

Structure of research articles

Each research article should contain a title, a name of the author, an e-mail, keywords, an abstract (max. 1 500 characters including spaces), a text (max. 45 000 characters including spaces and footnotes) and list of references.

Structure of comments

All comments should contain a title, a name of the author, an e-mail, keywords, a text (max. 18 000 characters) and a list of references.

Structure of book reviews

Each book review should contain a title of the book, a name of the author, an e-mail, a full citation, a text (max. 18 000 characters) and a list of references.

Structure of citations

Citations in accordance with AGPS Style Guide 5th ed. (Harvard standard), examples:

Book, one author: Dahl, R. (2004) *Charlie and the Chocolate Factory*. 6th ed. New York: Knopf.
Book, multiple authors: Daniels, K., Patterson, G. and Dunston, Y. (2014) *The Ultimate Student Teaching Guide.* 2nd ed. Los Angeles: SAGE Publications, pp.145-151.
Article: Battilana, J. and Casciaro, T. (2013) The Network Secrets of Great Change Agents. *Harvard Business Review*, 91(7) pp. 62-68.
Case: *Evans v. Governor of H. M. Prison Brockhill* (1985) [unreported] Court of Appeal (Civil Division), 19 June.
Citation Guide is available from: https://journals.muni.cz/public/journals/36/download/Citationguide.pdf

Formatting recommendations

Use of automatic styles, automatic text and bold characters should be omitted.
Use of any special forms of formatting, pictures, graphs, etc. should be consulted.
Only automatic footnotes should be used for notes, citations, etc.
Blank lines should be used only to divide chapters (not paragraphs).
First words of paragraphs should not be indented.
Chapters should be numbered in ordinary way – example: "5.2 Partial Conclusions".

Submissions

Further information available at https://journals.muni.cz/mujlt/about

LIST OF ARTICLES