MASARYK UNIVERSITY JOURNAL OF LAW AND TECHNOLOGY

VOLUME 17 | NUMBER 2 | FALL 2023 | 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. (https://rowan.legal)
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 **17** | NUMBER **2** | FALL **2023**

LIST OF ARTICLES

DOI 10.5817/MUJLT2023-2-1

(UN)LOCK AND (UN)LOADED: REGULATING 3D-PRINTED FIREARMS IN THE OPEN-SOURCE ERA AFTER THE 2013 HYSTERIA*

by

DAVID TAN † AMPUAN SITUMEANG ‡ HARI SUTRA DISEMADI §

3D printing, or additive manufacturing, is a fast-evolving technology that is transforming the way humans create things. Anyone can buy a 3D printer for private usage, allowing them to produce totally personalized things in the comfort of their own homes. One 3D-printed commodity, unfortunately, is provoking a huge debate: firearms. Any person may build a completely functional firearm only with a 3D printer, the necessary designs and filament. Thus, bypassing governmental licensing, registration, and fabrication regulations. A surge of scholarships appeared

* The authors extend their sincere gratitude to the anonymous reviewers and editors for their thoughtful comments, feedbacks, and suggestions on an earlier draft of this article. This article benefited immensely from those who had devoted their thoughts and views with the authors on the subject. A part of this research was financially supported by Batam International University (Grant No. 010/LPPM/KP-UIB/IV/2023). This article was also written as part of an independent research conducted by the lead author during postgraduate study at the Dickson Poon School of Law, King's College London with funding from the British Government's Chevening Scholarship. Chevening Scholarship is the UK government's global scholarship program, funded by the Foreign, Commonwealth and Development Office (FCDO) and partner organizations. Any opinions expressed and policies advocated in this material are the authors' and do not necessarily reflect the views of the Foreign, Commonwealth & Development Office (FCDO), the funder or the institution which the author(s) is affiliated with. The usual disclaimers apply.

† David Tan, Assistant Professor in law, Faculty of Law, Batam International University, Batam, Indonesia; Doctoral student, School of Law, Pelita Harapan University, Tangerang, Indonesia; Law & Technology LLM student, the Dickson Poon School of Law, King's College London, University of London, England, United Kingdom of Great Britain and Northern Ireland (under the auspices of the British Government Chevening Scholarship); email: david.tan@uib.ac.id.

‡ Assistant Professors in law, Faculty of Law, Batam International University, Batam, Indonesia; email: ampuan.situmeang@gmail.com.

§ Assistant Professors in law, Faculty of Law, Batam International University, Batam, Indonesia; email: hari@uib.ac.id.

nine years back, alerting people about the dangers of 3D-printed firearms. Following the widespread hysteria, this work offers commentary on the issue of 3D-printed firearms, as well as lessons learnt for a better regulatory framework for these firearms. To establish effective regulatory oversight over illicit ownership and usage of 3D-printed guns, existing law may have to be enhanced. Furthermore, any prospective regulations will almost definitely be closely scrutinized in order to strike a balance between public security concerns and personal liberty. Additionally, many conceivable technological regulations would be unfeasible and would contradict the public interest objective of safeguarding technological development. To better control 3D-printed guns while preserving basic freedoms and technological development, a three-pronged approach has been proposed.

KEY WORDS

3D Printing Technology, 3D-Printed Guns, Additive Manufacturing, Firearms, Ghost Gun, Regulation

1. INTRODUCTION

Three-dimensional (3D) printing, often known as additive manufacturing, is a fast-evolving technology that poses new legal implications. Among the most challenging issues is determining how to control 3D-printed guns responsibly.[1] Anybody with a 3D printer now has the ability to transform a digital design into an operational lethal firearm, circumventing various gun control regulations.[2] Regardless of the fact that 3D printing technology has been around since the 1980s, recent technological breakthroughs and lower costs have rendered these devices more affordable to everyday users.[3] Since the market for 3D printers is still so nascent, it is still yet to be effectively governed, and the legal ramifications of 3D-printed items have not been adequately assessed by the judiciary.[4] It is uncertain why 3D printing technology has not really been covered by current regulative frameworks up to this point. The far more likely answer is that the technology is not quite developed, and that it would be several years before it becomes a viable alternative to conventional production. Nonetheless, a number of recent advancements indicate that the technology may become feasible sooner than

1 For the purpose of this article, any firearm manufactured with any 3D-printed component that serves to the firearm's operation, regardless of the material used, is considered a 3D-printed gun. See McCutcheon, C. (2014) Deeper than a Paper Cut: Is It Possible to Regulate Three Dimensionally Printed Weapons or Will Federal Gun Laws Be Obsolete Before the Ink Has Dried? *Journal of Law, Technology and Policy*, 2014 (2), p. 227.

2 McCutcheon, C. (2014) *op. cit.*, p. 221.

3 McCutcheon, C. (2014) *op. cit.*, p. 223.

4 Berkowitz, J. (2018) Computer-Aided Destruction: Regulating 3D-Printed Firearms Without Infringing on Individual Liberties. *Berkeley Technology Law Journal*, 33 (1), p. 53.

expected.[5] As 3D printers are becoming more widely accessible, there is fear that users may utilize these devices to get around the law.[6]

Anybody with a 3D printing machine and Internet connection may make guns in their own houses, eliminating the need for license, registration and background checks.[7] There are currently minimal regulations concerning the ownership or production of 3D-printed guns. Thus far, 3D-printed weapons have largely sparked concerns about intellectual property, such as patent, trademark and intellectual property theft.[8] Nonetheless, once the technology has become more widely available, it will surely thwart existing gun-control measures and public safety concerns.[9] With tens of thousands of firearm-related violence annually,[10] 3D-printed firearms should be evaluated in the light of their potential to increase that numbers. Although it is unlikely that many people would manufacture their own weapons, 3D printers will help to increase the number of illicit weapons on the market and offer offenders with a novel way to get weaponry.[11] In addition, unskilled users may injure themselves when trying to manufacture and discharge a badly crafted firearm.[12] Nevertheless, regulators must be cautious not to let the innovation of 3D printing divert attention away from the real issue: public safety and preventing misuse of technology, while not stifling with technological innovation.[13] This is especially true for 3D printing, which has the potential to revolutionize many industries, from manufacturing, medicine to gunsmithing. However, there are potential risks associated with the technology, such as the potential for misuse, which regulators must be aware of in order to ensure public safety. Regulatory oversight is important for safety, but it must not stifle innovation. Governments must ensure that regulatory actions are reasonable and do not prevent the development of 3D printing technology for beneficial uses. It is similar to navigating a narrow path between two cliffs; too far to either side and one

5 Christopher, G. (2015) 3D Printing: A Challenge to Nuclear Export Controls. *Strategic Trade Review*, 1 (1), pp. 18-19.

6 Ferguson, C. (2013) *3-D Printed Guns Are a Boon for Criminals*. [online] Atlanta: CNN. Available from: `https://edition.cnn.com/2013/05/07/opinion/ferguson-printable-gun/index.html` [Accessed 25 April 2022]

7 McCutcheon, C. (2014) *op. cit.*, p. 221.

8 Berkowitz, J. (2018) *op. cit.*, p. 54

9 McCutcheon, C. (2014) *op. cit.*, p. 220.

10 Little, R. (2014) Guns Don't Kill People, 3D Printing Does? Why the Technology Is a Distraction from Effective Gun Controls. *Hastings Law Journal*, 65 (6), p. 1506.

11 McCutcheon, C. (2014) *op. cit.*, p. 237.

12 There are many other serious social consequences of firearms ownership that are unrelated to criminality, like the alarmingly high frequency of accidental gun-related injuries. See Stevenson, D. (2021) Going Gunless. *Brooklyn Law Review*, 86 (1), p. 184.

13 Little, R. (2014) *op. cit.*, p. 1510.

will fall off the edge. Regulatory actions must be balanced to provide enough protection without choking off the beneficial advances that 3D printing can bring. Therefore, finding the balance between protecting the public while still allowing innovators to explore technology's full potential is the key. Hence, the debate over merely removing digital data for 3D printing firearms off the Internet has little practical significance.[14] However, it raises the question of whether and how gunsmithing by means of 3D printing should be governed. This paper will examine the topic of 3D printing and its prospects for regulatory action. This will include an overview of the technology, its potential applications, and its potential security implications. Next, this paper's topic will also allow for examining existing regulatory approaches. From a legal and technological perspective, the paper's topic will then move towards discussion on what strengthens the raison d'être for regulating or non-regulating 3D printers. The ultimate aim of this paper is to explore the appropriate regulatory responses for 3D printing technology, in order to ensure its potential benefits are realized, while mitigating any potential security risks. Whilst this paper is theoretical in nature and therefore not bound by any particular jurisdiction, it aims to provide overall assessments that will be useful for policymaking. However, this paper was never meant to be the "overarching" and "one-size-fits-all" panacea, and to ensure effectiveness, further contextual and empirical research is definitely needed.

Unlike previous scholarships, the novelty of this paper lies on its focus on coming up with solutions that strikes a careful balance between preserving public safety and rights on the one hand, while avoiding unnecessary controls on 3D printing technology that would stifle the industry on the other. The concerns of clients of this technology, as well as the interests of other players in the technology, like 3D printer makers, government agencies, and hosting platforms, are considered. Furthermore, lessons learnt from several scholarships in response to the 2013 3D-printed gun hysteria,[15] as well as

[14] Jacobs, J.B. and Haberman, A. (2017) 3D-Printed Firearms, Do-It-Yourself Guns, & the Second Amendment. *Law and Contemporary Problems*, 80 (2), p. 137.

[15] When the downloadable designs (or digital design files) to build a 3D-printed firearm, called "the Liberator," were posted onto the world wide web by the US-based firm, Defense Distributed in 2013, it drew a lot of public and law enforcement interest. The new tech shocked the public, reaching more than 100,000 downloads within the first 24–48 hours, well before the US Department's Directorate of Defense Trade Controls (DDTC) advised the files' withdrawal from the Internet based on the pretext that the Liberator may be in breach of the Arms Export Control Act. See Daly, A. et al. (2021) 3D Printing, Policing and Crime. *Policing and Society*, 31 (1), p. 40; On the other hand, Hassan argues in his commentary that 3D-printed firearms are not a serious societal concern. As a result, alarmist reports about 3D-printed firearms may be perceived as a disservice to the wonderful influence that 3D printing is doing for our society—hence, an unwarranted manufactured hysteria. See Hassan,

current circumstances, are considered to provide up-to-date analysis on the subject matter.

This paper focuses on the challenge 3D-printed firearms poses to policymakers, with emphasis on the lesson learned from several scholarships in response to the 2013 3D-printed gun hysteria. It also suggests a way for the legal system to govern 3D-printed firearms with minimum interference to people's freedom and without impeding technological progress. Part II explains why 3D printing is vital for development, how it works, how anyone might use it to make weapons for themselves, and how 3D printers may revolutionize the way guns are procured, compromising or perhaps even rendering obsolete the archaic regulatory regime. Part III examines the present regulatory regime for 3D-printed guns and explains why the collision of technology and existing legal systems throughout the world provokes fearful regulatory response. Part IV explains why regulation is still the best step to take, elucidates the case against regulating 3D printers, and proposes a three-pronged approach that is deemed by far the most practical way of regulating 3D-printed guns while maintaining individual liberty and technological progress. Finally, Part V highlights and emphasizes the need to embrace 3D printing technology with minimal regulatory actions, while ignoring proposal for regulations requiring strict controls on 3D printers.

2. THE PROLIFERATION OF 3D-PRINTED FIREARMS: HOW TECHNOLOGY IS MOVING FASTER THAN THE LAW

3D printing technology, according to U.S. President Barack Obama in 2013, has the "potential to change the way we create practically anything."[16] 3D printing has already been revolutionizing several industries: the National Aeronautics and Space Administration (NASA), for example, uses this technology to make parts for its spaceships.[17] They has even launched 3D printers into space onboard its spacecraft in case a component fails and has to be replaced swiftly.[18] At Boeing, about 200 distinct parts for ten separate aircraft models are manufactured using 3D printers.[19] Furthermore,

K. (2020) Three-Dimensional Printed Hysteria. *3D Printing and Additive Manufacturing*, 7 (2), p. 47.

16 Blackman, J. (2014) The 1st Amendment, 2nd Amendment, and 3D Printed Guns. *Tennessee Law Review*, 81 (3), p. 483.

17 McCutcheon, C. (2014) *op. cit.*, p. 221.

18 Lewis, A. (2014) The Legality of 3D Printing: How Technology Is Moving Faster than the Law. *Tulane Journal of Technology and Intellectual Property*, 17, p. 304.

19 Willcocks, L., Venters, W. and Whitley, A. (2014) *Moving to the Cloud Corporation: How to Face the Challenges and Harness the Potential of Cloud Computing*. Hampshire: Palgrave Macmillan UK, p. 187.

this technology is utilized on a daily basis in the healthcare industry to make products such as hearing devices, prosthetics, orthopedic implants, and dental fillings.[20] Surgeons could even construct replicas of a patient's body to rehearse surgery before it is executed using this technology. The 3D printing technology permits a relatively pleasant production process that is both more efficient and waste-free than existing conventional production techniques.[21] Numerous critics, however, are worried that as 3D printing technology is becoming more widely used, certain people would exploit it to advance illicit activities.[22] The laws are left behind technological progression. Therefore, the capacity to successfully control 3D-printed firearms is at the top of this list of concerns.[23]

2.1. 3D PRINTING OR ADDITIVE MANUFACTURING

Additive manufacturing[24] is the catch-all term for 3D printing and its related technologies.[25] What sets 3D printers apart from earlier technologies would be that they enable people to recreate anything efficiently and quickly.[26] 3D printing is a fabrication technique that involves the process of construction by assembling tiny sheets of solid or liquid substances in

[20] Jensen-Haxel, P. (2012) 3D Printers, Obsolete Firearm Supply Controls, and the Right To Build Self-Defense Weapons Under Heller. *Golden Gate University Law Review*, 42 (3), pp. 451-452.

[21] McCutcheon, C. (2014) *op. cit.*, p. 222.

[22] Although the advantages of having a 3D printer are enormous, the potential of a 3D printer to quickly transform a CAD file into a lethal item, such as a gun, allows printer availability to the regular populace, especially those with malicious intentions, a national security issue. See McMullen, K.F. (2014) Worlds Collide When 3D Printers Reach the Public: Modeling a Digital Gun Control Law after the Digital Millenium Copyright Act. *Michigan State Law Review*, 2014 (1), pp. 196-197.

[23] McCutcheon, C. (2014) *op. cit.*, pp. 235-237.

[24] Additive manufacturing is not the same as subtractive manufacturing. The former creates objects by depositing material layer-by-layer, whereas the latter creates objects by removing material layer-by-layer. Thanks to their overlapping variety of applications, additive and subtractive manufacturing technologies are frequently utilized together, despite their key distinctions. A computer numerical control (C.N.C.) milling, is an example of computerized subtractive manufacturing. This method does what 3D printing cannot: it makes an object by subtracting materials instead of adding them.

[25] Christopher, G. (2015) *op. cit.*, p. 19.

[26] In general, 3D printing outperforms conventional manufacturing techniques in terms of efficiency and speed, particularly for smaller and customizable runs of production. One can argue that a 3D printer may construct objects more slowly than a conventional manufacturing line. However, there are more things that may go wrong with conventional manufacturing processes, whenever one takes into account human mistake and mechanical issues that could halt production. The molds are necessary for conventional methods of production like the injection molding process in order to produce parts. It may take 1-2 months to create these molds from scratch. Contrarily, the creation of a finished product using 3D printing is sped up starting with the conception or conceptualization phase to a working prototype and final product in just a matter of a couple of days. Here, it is obvious that the pace is exceptional and much quicker than conventional manufacturing methods. See Kinsley, K., Brooks, G. and Owens, T. (2014) International Legal and Ethical Challenges Related to the Use and

a horizontal cross-section manner in successive layers to create an actual 3-dimensional object based on a digitized blueprint.[27] A 3D printer bears a striking resemblance to inkjet or LaserJet printers—which is a standard 2D printer. However, rather than dispensing ink onto a paper, a 3D printer deposits substances such as metals, plastics, powders, glass and rubber-like substances onto a base, layer after layer, to create an object.[28] Succinctly, 3D printing in layman's terms is the technique of manufacturing a three-dimensional version of a digital file (CAD file) by using some sort of deposited material.[29] This technique differs from typical "subtractive" manufacturing, that involves cutting or machining raw materials to produce objects.[30] While there are many different types of 3D printers on the market nowadays, they all operate in the same way.

To start, a computer-aided design (CAD) file, which serves as a digitized blueprint for the intended product, is required.[31] A CAD file can be created by utilizing 3-D modeling software or by scanning[32] the outline, contours and features of the physical object.[33] The CAD files are prepared in a standardized format that may be altered and read using a variety of software programs. In preparation for printing, software programs are often used to segment the data into a sequence of layers.[34] To manufacture an object, a 3-D printer reads commands from a digital file—usually a CAD file—and executes the file's

Development of 3D Technology in the U.S. and China. *Journal of Knowledge Management Economics and Information Technology*, 4 (1), p. 2.

27 Nielson, H. (2015) Manufacturing Consumer Protection for 3-D Printed Products. *Arizona Law Review*, 57 (2), p. 610.

28 Wilbanks, K. (2013) The Challenges of 3D Printing to the Repair-Reconstruction Doctrine in Patent Law. *George Mason Law Review*, 20 (4), p. 1152.

29 Tran, J.L. (2015) The Law and 3D Printing. *UIC John Marshall Journal of Information Technology & Privacy Law*, 31 (4), p. 508.

30 Couch, J. (2016) Additively Manufacturing a Better Life: How 3D Printing Can Change the World Without Changing the Law. *Gonzaga Law Review*, 51 (3), pp. 519-520.

31 The data which the 3D printer requires to make the final product is included in an electronic file called a computer-aided design ("CAD") file, which guides the 3D printing process. See Sharpe, M. (2019) Products Liability in the Digital Age: Liability of Commercial Sellers of Cad Files for Injuries Committed With a 3D-Printed Gun. *American University Law Review*, 68 (6), pp. 2301-2302.

32 Activists Nora al-Badri and Jan Nikolai Nelles provide perhaps the greatest illustration of this. They strolled into Berlin's Neues Museum, where they have been scanning a 3,000-year-old bust of Egyptian Queen Nefertiti using mobile scanners concealed underneath their coats and scarves to produce a CAD file. They later utilized the scan to create a 3D-printed replica of the bust, which was gifted to American University in Cairo before making the CAD file available under a Creative Commons license. See Lewis, D. (2016) *Thanks to Sneaky Scanners, Anyone Can 3D Print a Copy of Nefertiti's Bust.* [online] Washington, D.C.: Smithsonian Magazine. Available from: `https://www.smithsonianmag.com/smart-news/thanks-sneaky-scanners-anyone-can-3d-print-copy-nefertitis-bust-180958213/` [Accessed 6 May 2022].

33 Nielson, H. (2015) *op. cit.*, p. 613.

34 Christopher, G. (2015) *op. cit.*, p.19.

computerized pattern.[35] After that, the 3-D printer interprets the CAD file and "prints" the product by releasing a selection of filaments, like plastic, ceramics, metal, or perhaps even food in small amounts onto a flat surface. The 3-D printer creates a product by layering filament horizontally on top of one another until product is completed.[36] Each subsequent layer will vary from the last in proportion to the object being created. [37] The layers are fused altogether and the object is further solidified once they have been set.[38] Despite claims to the contrary, a typical 3D printer cannot build an object with multiple parts—like a firearm. Rather, every component must be printed separately and then assembled afterward.[39]

Although this technology is still very much in infancy, others hope it may usher in a new market revolution in which people regain control of the means of production.[40] Despite all the hype, conventional manufacturing processes still outnumber 3D printing. In general, the size of what can be made with 3D printers is confined by the available motion and consequently the size of the 3D printer. Aside from size limitations, 3D printing is too slow for large-scale manufacturing and too pricey for many everyday users.[41] The everyday and ordinary users would still find using a 3-D printer challenging without training, hence aficionados now lead the sector.[42] Individuals obtain a hefty 3-D printer with the goal of creating intricate objects, however the only thing they manage to create is something simple and inexpensive that takes hours to finish—and would have cost a fraction of the price if bought conventionally. Accordingly, the ordinary user would find it difficult to manufacture anything other than ornamental things since objects take forever to print, use a lot of material, and need sophisticated assembly—which frequently requires non-3-D printed components.[43]

[35] Nielson, H. (2015) *op. cit.*, p. 613.
[36] *Ibid*.
[37] Wilbanks, K. (2013) *op. cit.*, p. 1152.
[38] *Ibid*.
[39] Sharpe, M. (2019) *op. cit.*, p. 2303.
[40] Jensen-Haxel, P. (2015) A New Framework for a Novel Lattice: 3D Printers, DNA Fabricators, and the Perils in Regulating the Raw Materials of the Next Era of Revolution, Renaissance, and Research. *Wake Forest Journal of Law & Policy*, 5 (2), p. 232.
[41] Couch, J. (2016) *op. cit.*, pp. 520-521.
[42] Nielson, H. (2015) *op. cit.*, p. 613.
[43] The few who grasp the technology, on the other hand, may print inventive, and practical things, such as to duplicate replacement parts for damaged appliance components in the household that are difficult to come by or are prohibitively expensive. See *Ibid*.

2.2. POTENTIAL SECURITY IMPLICATIONS WHEN GUNS ARE DEMOCRATIZED IN THE OPEN-SOURCE ERA: COMPUTER-AIDED DESTRUCTION AND THE UNTRACEABLE GUN CRISIS

Although 3D printing technology is innovative, it cannot be deemed completely novel in the legal sector.[44] It simply expands the range of opportunities and allows the creation of almost any shape possible. While the technology within that domain did not offer completely new stuff, the legal perspective is finding it very difficult to cope, rarely finding appropriate legal analogies.[45] Furthermore, regardless of the fact that we have been discussing this subject matter for several decades, there is a perpetual lack of decent literature on the subject.[46] Even though legal concepts extend to 3D printing in about the same way they do to other innovations, 3D printing seems to have a distinctive ability to disrupt the legal status quo.[47] The majority of the legal disruptions caused by 3D printing will most likely be inadvertent. People who 3D print objects may be unaware of their legal rights and duties. However, 3D printing without oversight may become so prevalent—and reproducing items with 3D printers may potentially become so ubiquitous.[48]

The possibility to construct difficult-to-detect, untraceable firearms is the biggest issue for criminal justice when it comes to 3D printing.[49] Since the 3D printing community is based on free open-source precepts, people may browse various file hosting websites to get CAD files. Each individual files on the open-source archives, on the other hand, are a major source of concern since they may be downloaded and modified by anybody.[50] This notion

---

[44] For a brief overview of some relevant papers, as well as a discussion of the history of regulation and proposed solution, check e.g. Tran, J.L. (2015) *op. cit.*, p. 510.

[45] Loutocký, P. (2019) 3D Printing and Beyond: Intellectual Property and Regulation. Mendis, D.; Lemley, M.; Rimmer, M. (Eds.). *Masaryk University Journal of Law and Technology*, 13 (1), pp. 123-124.

[46] Yanisky-Ravid and Kwan suggest that the judicial system was and continues to be caught off guard by technological developments. This does not, in their perspective, imply that 3D printing should introduce novel notions; nonetheless, some legal frameworks must adapt to the changing environments. See Yanisky-Ravid, S. and Kwan, K. S. (2017) 3D Printing the Road Ahead: The Digitization of Products When Public Safety Meets Intellectual Property Rights—A New Model. *Cardozo Law Review*, 38 (3), p. 921.

[47] Actual models, prototypes, templates, machining components, and production parts may all be created with 3-D printing. It is used by design and production companies for consumers, industry, healthcare, and military product parts. All of these are achieved by democratizing and dismantling the existing supply chain network. See de Jong, J.P.J. and de Bruijn, E. (2013) Innovation Lessons From 3-D Printing. *MIT Sloan Management Review*, 54 (2), p. 44.

[48] Yanisky-Ravid, S. and Kwan, K. S. (2017) *op. cit.*, p. 927.

[49] Beyer, K. E (2014) Busting the Ghost Guns: A Technical, Statutory, and Practical Approach to the 3-D Printed Weapon Problem. *Kentucky Law Journal*, 103 (3), p. 446.

[50] An open-source is like a peer-to-peer file sharing platform that allows people to download and upload digital files to a social platform for other users to access and modify. Computer

spread swiftly in the fast-changing world of 3D printing, enabling people to improve the relevant technology at a faster pace.[51] Irrespective of their intentions, users can obtain and utilize CAD files and blueprints for firearms and explosive components. An innocuous object might be altered to serve nefarious purposes. The best thing is that downloading and editing these files is now mostly unrestricted thanks to "free" nature of open-source. The proliferation of "ghost guns"—firearms that are functionally undetectable, untraceable and frequently missing a serial number—threatens to jeopardize gun control and tracking attempts.[52] In 2013, two Daily Mail journalists used a £1,700 3D printer to build a plastic firearm and managed to transport it onboard a Paris-bound Eurostar train service from London at St. Pancras International Station. Despite its plastic construction, the firearm was capable of shooting a lethal 0.38-calibre projectile.[53] In July 2013, Israeli journalists obtained the CAD files for semiautomatic 3D-printed firearms and smuggled them to Prime Minister Benjamin Netanyahu's speech at the Knesset (Israeli Parliament). The metal firing pin was left inside the firearm, and it missed detection by security sensors. In fact, the journalists were able to get past Knesset security twice.[54] This has proven that security checks with metal detectors will be ineffective if potential criminals were to manufacture plastic weapons and smuggle them into secure public areas like airports or government buildings.[55] This understandably caused instant alarm on a global scale, with realistic concerns regarding the ease with which this new sort of weaponry may be easily concealed to facilitate an assassination

programmers are thought to have started the open-source trend by exchanging free knowledge with other computer users. These programmers were encouraged to provide this "free" knowledge alongside vast communities of other programmers, allowing many individuals to edit, enhance, and recreate various variants from the same source software. The word "free" relates not just to zero-cost transactions, but mostly to programmers' opportunity to modify their own programs. See Staed, K.C. (2017) Open Source Download Mishaps and Product Liability: Who Is to Blame and What Are the Remedies? *Saint Louis University Public Law Review*, 36 (1), p. 184.

[51] Lara, S.S. (2019) The iTunes of Downloadable Guns: Firearms as a First Amendment Right. *Catholic University Journal of Law and Technology*, 28 (1), p. 85.

[52] Eichner, A.W. (2020) Crime in the Age of Printable Guns: Methodologies and Obstacles to Prosecuting Federal Offenses Involving 3D-Printed Firearms. *Vermont Law Review*, 45 (2), p. 216.

[53] Murphy, S. (2013) *How Mail On Sunday "Printed" First Plastic Gun in UK Using a 3D Printer-and Then Took It on Board Eurostar without Being Stopped in Security Scandal.* [online] London: Dailymail. Available from: `https://www.dailymail.co.uk/news/article-2323158/How-Mail-On-Sunday-printed-plastic-gun-UK--took-board-Eurostar-stopped-security-scandal.html` [Accessed 10 May 2022].

[54] Captain, S. (2013) *Journalists Smuggle 3-D Printed Gun into Israeli Parliament.* [online] New York: NBC News. Available from: `https://www.nbcnews.com/technolog/journalists-smuggle-3-d-printed-gun-israeli-parliament-6c10570532` [Accessed 10 May 2022].

[55] Beyer, K.E. (2014) *op. cit.*, p. 446.

attempt or airplane hijacking.[56] The components for ghost guns can be acquired or constructed without going through a background check, making them appealing to restricted users and those who would otherwise fail these checks.[57] There seems to be a good chance that ghost guns will be employed in the future to support illegal acts. Lawmakers and academics fear that as 3D-printing technology progresses, the size and shape of printed guns will render detection unfeasible.[58] Furthermore, during times of emergency, the circulation of ghost guns is anticipated to escalate. Since the widespread of COVID-19, internet sales of untraceable and undetectable firearm parts and 3D printers have surged, according to the Giffords Law Center.[59]

The National Ballistic Intelligence Service (NABIS) of the United Kingdom stated that the 3D-printed firearm was indeed a workable lethal weapon, but only effective for three to four discharges (presuming one could find appropriate ammunition), as the polymer parts started to crack and distort with repetitive discharges, causing the "firearm" to blow up in the holder's hand.[60] However, now, the technology of 3D-printed guns has progressed. The capacity to manufacture polymer bullets compatible with 3D plastic firearms, for example, has increased the desire to oversee 3D printing of firearms.[61] Furthermore, a blueprint for a multi-use 3D-printed Glock is now openly available for download from the Internet.[62]

While illegal weapons are widely available, obtaining one requires contacting a third party. Manufacturing a 3D gun, on the other hand, may be done in full anonymity and secrecy. Furthermore, the firearm can be simply destroyed by remelting the plastic, leaving no sign of its existence. While authorities can track down firearms and, relying on projectile identification, perhaps correlate a firearm to a specific projectile and hence a crime scene, this opportunity is not available in the case of 3D gun-related crimes. When a 3D plastic firearm is destroyed, investigators could only look for 3D printers. It would be difficult to connect a suspect to a crime through firearm use

[56] Lewis, A. (2014) *op. cit.*, p. 309.
[57] Talbot, T. and Skaggs, A. (2020) Regulating 3D-Printed Guns Post-Heller: Why Two Steps are Better than One. *Journal of Law, Medicine and Ethics*, 48 (4), p. 99.
[58] Talbot, T. and Skaggs, A. (2020) *op. cit.*, p. 100.
[59] Pucino, D. (2020) *Ghost Guns: How Untraceable Firearms Threaten Public Safety*. [online] San Francisco, CA: Giffords Law Center. Available from: `https://giffords.org/lawcenter/report/ghost-guns-how-untraceable-firearms-threaten-public-safety/` [Accessed 12 June 2022].
[60] Daly, A. et al. (2021) *op. cit.*, p. 41.
[61] Leon, K.N. (2019) Beyond the Single-Use Plastic Gun: The Need to Make 3D-Printed Gun Laws Shatterproof. *Houston Law Review*, 57 (2), pp. 462-463.
[62] Hanrahan, J. (2019) *3D-Printed Guns Are Back, and This Time They Are Unstoppable*. [online] San Francisco, CA: WIRED. Available from: `https://www.wired.co.uk/article/3d-printed-guns-blueprints` [Accessed 6 May 2022].

and ownership if the perpetrator also destroyed any cache, buffer files on the printer and computer, and wiped all of his online presence during data download.[63]

From the aforementioned, the present regulations are inadequate to clearly control 3D-printed firearms due to ambiguities and lack of enforceability.[64] Simply requiring licensing and transfer registration of 3D-printed firearms does not address enforceability issues. Simply said, if 3D-printed firearms are to be distributed illicitly, certain gunsmiths and gun aficionados will just refuse to comply.[65] A complete ban on 3D-printed firearms is impractical, and even if it were to happen, such restrictions and rules would be hard to execute.[66] In addition, efforts to regulate online file sharing may also be futile.[67]

2.3. GUNSMITHING OPERATIONAL FIREARM FROM THE COMFORT OF YOUR HOME: HOW TECHNOLOGY DISRUPTS THE ARCHAIC LAW ENFORCEMENT FOCUSING ON TRADITIONAL SUPPLY CHAIN

Thus far, our laws have gradually evolved to address the issues that 3D printers provide, but the advancement of technology continues to surpass that of the law. The rise of 3D printing has implications–at least technically–for a variety of archaic legal frameworks that are affected by its operation and use. The regulation of guns is one of the most notable of these areas of legislation, owing to the manufacturing of firearm components created through the 3D printing technology.[68] Other regulations that pertain to 3D printing's uses and applications include intellectual property, product safety, medicinal regulation, and data protection. With the growing popularity of 3D printing among consumers and businesses, it is conceivable that new legal frameworks will be exposed to the innovation.[69] These regulations may appear to be rather distinguishable, having little in common other than their applicability to 3D printing. They do, nonetheless, embrace two aspects in this interaction with 3D printing: the structure of these

[63] Walther, G. (2015) Printing Insecurity? The Security Implications of 3D-Printing of Weapons. *Science and Engineering Ethics*, 21 (6), p. 1441.

[64] Leon, K.N. (2019) *op. cit.*, p. 446.

[65] Jacobs, J.B. and Haberman, A. (2017) *op. cit.*, p. 146.

[66] Osborn, L.S. (2013) Regulating Three-Dimensional Printing: The Converging Worlds of Bits and Atoms. *San Diego Law Review*, 51 (2), p. 579.

[67] Langvardt, K. (2016) The Doctrinal Toll of Information as Speech. *Loyola University Chicago Law Journal*, 47 (3), p. 794.

[68] Daly, A. (2016a) Don't Believe the Hype? Recent 3D Printing Developments for Law and Society. In: Dinusha Mendis, Mark Lemley and Matthew Rimmer (eds.) *3D Printing and Beyond*. Cheltenham: Edward Elgar Publishing, p. 350.

[69] *Ibid.*

legislation and their enforcement. Both of these challenges are fueled by 3D printing's democratization of manufacturing and the ability for people to make goods in their homes and workplaces, bypassing existing gatekeepers and control nodes.[70]

In contrast to the earlier kinds of centralized manufacturing in the Fordist period, 3D printing is a modern technology that is "democratizing" production.[71] Current gun control regulations were created for a Fordist period of mass production,[72] in which centralized companies produce goods that are subsequently sold in stores and purchased in their entirety by customers. Most of these goods were simply too complicated for the common person to create himself, and/or the expense of manufacturing machines was far too costly for these people. Law enforcement in the Fordist mindset is based on the idea that manufacturing takes place through centralized institutions and that goods are supplied through well-defined distribution networks, ending in a retail outlet where the customer makes the final sale. As a result, the law may be enforced at multiple locations throughout the distribution network against these identified parties.

This scheme is severely disrupted by consumer fabrication of goods via 3D printing, when these supply chains, with their control nodes, are bypassed.[73] The gap between post-Fordist decentralized manufacturing and current legal frameworks is highlighted by 3D printing. In general, current legal frameworks are based on the assumptions of centralized manufacturing and distribution of manufactured goods via a traceable distribution network to a passive end-consumer. In this case, law and its enforcement frequently lag behind the emerging technology.[74] However, bear in mind that although the "decentralization and democratization" which 3D printing (conceivably) involves is a departure from the status quo, there was

[70] Daly, A. (2016a) *op. cit.*, pp. 350-351.
[71] Daly, A. et al. (2021) *op. cit.*, p. 39.
[72] Fordism is a word coined to characterize the mass-production strategy spearheaded by the Ford Motor Company in the early twentieth century. In 1922, Henry Ford claimed that mass production had become the "new Messiah" as he marveled at his company's successful Highland Park facility. Although Henry Ford is not given credit with inventing the notion of mass manufacturing, he is recognized with revolutionizing the industrialized period by fragmenting operations and standardizing parts, allowing for the assembly line and mass manufacturing. See Richardson, M. (2016) Pre-Hacked: Open Design and the Democratisation of Product Development. *New Media and Society*, 18 (4), p. 657.
[73] Daly, A. (2016a) *op. cit.*, p. 351.
[74] Daly, A. et al. (2021) *op. cit.*, p. 40.

also a "reintermediation" trend including actors related to the process, like 3D printing filesharing providers.[75]

Another spectrum of law-disrupting 3D printing that is impacting the archaic law enforcement mechanisms in its sense that tends to rely heavily on the traditional supply chain can be seen from the intersection between 3D printing innovation and intellectual property protection. The challenges with intellectual property are now influencing the actual world. Although counterfeit products have traditionally been a source of concern, many of them remain dependent on huge production plants—particularly in less developed nations. [76] In theoretical terms, every design might be subject to a specific type of intellectual property protection, making any method of duplication potentially illegal. Since the 3D printing method is digitized in nature, it has become simpler nowadays to "steal" a product's design and subsequently produce it in small quantities. [77] Instead of buying the genuine product, consumers can now digitize genuine products and manufacture copies for themselves. They can subsequently upload the scanned file to the Internet—which means anybody can readily access it and manufacture as many copies of the product as they like. Additionally, regardless of whether individuals are inadvertently violating intellectual property rights, the readily accessible nature of the Internet and advancements in communications technology have made it possible for proprietors to take advantage out of the content for free. [78] To make matters worse, the materials that were downloaded may effortlessly be redesigned and reuploaded to the Internet, which makes intellectual property owners to have an exceptionally tough time tracing the root of the violation and making law enforcement extremely challenging. The simplest kind of intellectual property law infraction occurs when an individual creates, utilizes, distributes, proposes to sell, or exports the protected property without the appropriate permission. Anybody who manufactures a protected product using a 3D printer is immediately breaching the intellectual property rights given that the manufacture was done without permission. The owner

[75] Such actors may include 3D printing or CAD filesharing providers, print-on-demand service providers, and the producers of 3D themselves springing up as possible control nodes. See Daly, A. (2016a) *op. cit.*, p. 350.

[76] Kietzmann, J., Pitt, L. and Berthon, P. (2015) Disruptions, Decisions, and Destinations: Enter the Age of 3-D Printing and Additive Manufacturing. *New Media and Society*, 58 (2), p. 213.

[77] Chan, H.K. et al. (2018) The Impact of 3D Printing Technology on the Supply Chain: Manufacturing and Legal Perspectives. *International Journal of Production Economics*, 205, p. 158.

[78] Assuming it is being used for private or academic purposes, it might be permissible. The digitally produced material could nevertheless be released on the marketplace for monetary benefits. See *Ibid*.

of the intellectual property might theoretically bring a lawsuit against these individuals. But this approach might be pretty unworkable in practice. Firstly, it might be challenging for the owner of the intellectual property to pinpoint these violators due to how dispersed the 3D printers could potentially be. Secondly, irrespective of whether the legitimate owner of the intellectual property names the violators—who are likely to be internationally dispersed—the owner might nonetheless still need to bring individual lawsuits against each violator due to joinder rules[79] or specific jurisdictional requirements. At the end of the day, the owner of the intellectual property would also potentially file a lawsuit against a prospective customer—which is not good for business.[80] Looking at a policy standpoint, lawmakers, and policymakers face challenging difficulties as a result of the widespread expectation that entrepreneurial customers (prosumers) are going to create products of their own. If intellectual property infringements were left unscathed, intellectual property is going to turn less significant, [81] violation will continue to be a serious concern, and commercialization methods are going to shift drastically. Hence, the fight for the protection of traditional intellectual property rights for digital goods is going to become incredibly challenging. Another example would be the concern about standards, i.e., how will society manage them, or alternatively, what are the possible risks that the absence of standardization presents? as well as who checks, supervises, and guarantees the quality of the printed products?[82]

3. SCRUTINIZING THE LAWS OF 3D-PRINTED FIREARMS UNDER TODAY'S OUTLOOK: IS THE GENIE ALREADY OUT OF THE BOTTLE?

Technology helps our lives.[83] Even though 3D printers now has produced a diverse range of products, unforeseeable risks associated with this far-reaching innovation will surely provide issues. A number of these concerns will be complicated by the lack of an adequate legal framework to address them. Moreover, most of these concerns may fall within

[79] For a well-discussed elaboration on the joinder rules, see Taylor, D.O. (2013) Patent Misjoinder. *New York University Law Review*, 88 (2), p. 662.

[80] Holbrook, T.R. and Osborn, L.S. (2015) Digital Patent Infringement in an Era of 3D Printing. *The UC Davis Law Review*, 48 (4), p. 1333.

[81] Jiang, R., Kleer, R. and Piller, F.T. (2017) Predicting the Future of Additive Manufacturing: A Delphi Study on Economic and Societal Implications of 3D Printing for 2030. *Technological Forecasting & Social Change*, 117, p. 91.

[82] Kietzmann, J., Pitt, L. and Berthon, P. (2015) *op. cit.*, p. 213.

[83] Weinberger, V.P., Quiñinao, C. and Marquet, P.A. (2017) Innovation and the Growth of Human Population. *Philosophical Transactions of the Royal Society B: Biological Sciences*, 372 (1735), pp. 1-2.

the scope of current legislation, notably in terms of gun control and information restriction. Technological improvements, on the other hand, will undoubtedly continue to raise new and difficult concerns. [84]

Every innovation brings with it a head-on collision with current legal systems around the world.[85] Instead of astonishment and enthusiasm, our legislative and regulatory reactions to technological innovations typically portray apprehension and irrationality.[86] Many people are fearful of technology. Some people even despise it—thus, the label 'luddite'.[87] People use the availability heuristic to create risk estimates while sifting through unknown or unfamiliar threats.[88] In this scenario, the human mind tends to construct a proxy estimate of the likelihood of an occurrence based on how easily preceding instances can be recalled from stored recollections.[89] The availability heuristics may be a useful tool to predict and traversing the hazards of everyday lives.[90] However, most of those heuristics and prejudices that contribute to systemic technological threat misconception were unconsciously institutionalized in clichés like "better safe than sorry," "the devil you know is better than the angel you don't," and "you can't teach an old dog new tricks."[91] Succinctly, how can we safeguard ourselves against ourselves? One thing is certain. Although the status quo may be pleasant, development is necessary to retain our global leading role and wellbeing.

According to data from the Small Arms Survey (SAS), a non-profit research initiative based at the Graduate Institute of International and Development Studies in Geneva, Switzerland, there is a positive correlation between wealth and firearm ownership. Firearms are more common in higher-income nations. While obtaining a 3D printer is still extremely costly, firearms would most probably be manufactured in wealthy nations, that

---

[84] Cosans, J. (2014) Between Firearm Regulation and Information Censorship: Analyzing First Amendment Concerns Facing the World's First 3-D Printed Plastic Gun. *American University Journal of Gender Social Policy and Law*, 22 (4), p. 920.

[85] Ma, V.C.K. (2017) 3D Printing and the Law. *Intersect: The Stanford Journal of Science, Technology, and Society*, 11 (1), p. 1.

[86] Khasawneh, O.Y. (2018) Technophobia: Examining Its Hidden Factors and Defining It. *Technology in Society*, 54 (1), p. 94.

[87] There are countless instances of technology saving and enhancing lives, but there are also numerous cases of human mistrust of technology. Emerging technology is assumed to cause humans to continually and systemically misunderstand the risk it poses to humankind. See Calandrillo, S. and Anderson, N.K. (2022) Terrified by Technology: How Systemic Bias Distorts U.S. Legal and Regulatory Responses to Emerging Technology. *University of Illinois Law Review*, 2022 (2), p. 599.

[88] Khasawneh, O.Y. (2018) *op. cit.*, p. 94.

[89] Tversky, A. and Kahneman, D. (1973) Availability: A Heuristic for Judging Frequency and Probability. *Cognitive Psychology*, 5 (2), p. 208.

[90] *Ibid*.

[91] Calandrillo, S. and Anderson, N.K. (2022) *op. cit.*, p. 662.

already have more firearms than poorer nations. It is far too soon to say where 3D-printed firearms will emerge, but one assumption is that 3D firearms will be created by people who already have access to "regular" firearms and just want one for the curiosity instead of for practical reasons. This curiosity factor could have a serious complication of catching the attention of youngsters who want to manufacture one just to be 'cool.' If they are negligent, this could result in an upsurge of accidental discharges, especially since plastic firearms are far less reliable hence more deadly than regular firearms.[92]

A large portion of today's printing comes under the category of fun or handy trinkets rather than life-changing instruments.[93] The fourth industrial revolution is now underway. Since 3D printing is now at the center of this transformation, it is in a spot where it is being closely scrutinized. People appear to have little difficulty adapting to new ideas, but this is not the case with our legal systems. A fine example of a disruptive upstart is 3D printing. At the very least, 3D printing has the potential to render laws and legal safeguards obsolete. The 3D printing revolution is the intersection of technological possibilities and a passion to make the world a better place. Marvels may emerge from this combination, but notable change will only occur if the legal system permits it. Therefore, instead of being afraid of new technological advancements, why not regulate these innovations with a longer leash. Afterall, the protection and recognition of the law permits greater utilization and better certainty that would be beneficial to everyone.

Parallels, however, can be drawn from Web 2.0's experiences, where users partake in social creation knowingly, without much regard to regulatory framework. However, in this case users might expose themselves to repercussions beyond legal comprehension. In terms of uncertainty, it is best to let the market create (the *laissez-faire* stance).[94] Although it might seem alluring to engage in social creation without giving regulatory frameworks adequate consideration, it is crucial to be cognizant of the possible adverse legal ramifications and to abide by the laws and regulations established by

[92] Walther, G. (2015) *op. cit.*, pp. 1440-1441.

[93] Couch, J. (2016) *op. cit.*, pp. 521-522.

[94] In the example of Chinese peer-to-peer lending industry, the traditionally conservative Chinese monetary authorities, who chose a wait-and-see *(laissez-faire)* approach to promote such technological advances while minimizing onerous oversight, initially embraced and actually encouraged online peer-to-peer lending. Yet, the friendly regulatory approach gave rise to widespread Ponzi schemes or bogus financial innovations, which caused massive financial losses for many investors. To demonstrate a prompt and effective reaction, the Chinese government launched a four-year operation of tough Internet finance regulation (whack-a-mole approach), which has targeted and cracked down all P2P lending platforms in the country. See Xu, D., Taylor, C.J. and Ren, Y. (2022) Wait-and-See or Whack-a-Mole: What Is the Best Way to Regulate Fintech in China? *Asian Journal of Law and Society*, First View, pp. 9-15.

governmental bodies. Some would contend that unnecessarily stringent rules and regulations might impede creative and innovative thinking. For instance, a heavy regulatory load may cause some businesses to be reluctant to put money into new technology or commercial strategies.[95] It is crucial to remember that laws and regulations are set to safeguard both individuals and companies from harm and discourage anti-competitive behavior, despite the devil's advocate's claims to the contrary.

In relation to laws and technology, the interaction between the markets and social norms is frequently complicated and multifaceted. The introduction of cutting-edge technology and the creation of new rules and laws may both be influenced by social conventions. For instance, social standards about privacy and safeguarding data have influenced the creation of privacy safeguards like the General Data Protection Regulation (GDPR) in Europe—hence, when collecting and handling private information, businesses in Europe are required to adhere to stringent privacy rules, as compared to that of the United States that boasts a more liberal stance towards data protection.[96] Social standards may additionally have an impact on how people and businesses behave in the marketplace. For instance, the desire for environmentally friendly products and services has increased as a result of societal standards surrounding environmental responsibility. However, markets may additionally affect the creation of rules and regulations as well as social standards. Market pressures, for instance, can spur research and the creation of novel technology. Market conditions may additionally impact the creation of fresh rules and regulations by influencing political discourse and public sentiment. In a nutshell, there are many different ways that markets and social norms interface with laws and technology. Markets can impact social conventions and the creation of rules and regulations, whereas societal conventions and the acceptance of novel technologies can be influenced by cultural standards.

Predominantly, 3D printers produced the least dangerous of products.[97] Until now, the exorbitant cost of 3D printers and materials still curb its widespread use. Therefore, it is safe to say that the genie is not yet out of the bottle. However, the notable discharge of a 3D-printed firearm, on the other hand, demonstrates the increasing possibilities and hazards of this technological innovation. Given the apparent trend of decreasing

[95] Tu, K.V. and Meredith, M.W. (2015) Rethinking Virtual Currency Regulation in the Bitcoin Age. *Washington Law Review*, 90 (1), p. 307.

[96] Rustad, M.L. and Koenig, T.H. (2019) Towards a Global Data Privacy Standard. *Florida Law Review*, 71 (2), p. 372.

[97] Hearing aids and musical instruments are two examples of 3-D printed objects listed. See Jensen-Haxel, P. (2012) *op. cit.*, p. 450.

technological costs in the long run, it really is important to consider the implications of 3D printing today, before it becomes largely accessible.[98] This new innovation poses a substantial and imminent threat to public safety, indicating a justifiable reason for regulation and the urgent need to address this problem before technology outpaces the law. So, when we regulate, examining these threats and possible strategies to govern this modern-day innovation, while keeping in mind the huge economic and societal benefits is crucial in order to prevent stifling future beneficial advancements.[99]

4. PROPOSING EFFECTIVE REGULATION

4.1. WHY REGULATION?

There are at least four reasons why 3D printing regulation[100] is important to us. Firstly, as the technology progresses, it will undoubtedly have an influence on a broader spectrum of production processes, allowing for increased productivity and economic growth. Many heralded that 3D printing is the nearest approximation we have to a new industrial revolution.[101] Secondly, 3D printing makes for easier material utilization, allowing for enormous invention of objects that are only limited by human creativity. Some of these goods may be dangerous and present hazard for human use. Thirdly, 3D printing shows potential in a range of industries where applications and services were in the early stages of development. This technology has the potential to open doors to a variety of commercial sectors, which might have a significant and cyclical influence on other areas of the economy. Finally, 3D printing has applications in security and military, which may well have inadvertent security and safety ramifications.

As more powerful personal 3D printers become available, and as industrial clients understand they can create parts, components, and other goods in-house, production will become more democratized and less supervised. Many regulations will be jeopardized when anybody can 3D print devices with nearly any capability outside of government supervision. Since manufacturing becomes more democratized, current laws are expected to become more obsolete. Whenever anybody can 3D print products with nearly unlimited functionality, uncontrolled illicit activities

[98] Walther, G. (2015) *op. cit.*, p. 1443.
[99] Cosans, J. (2014) *op. cit.*, pp. 943-944.
[100] n this article, regulation refers to one of the four types of legislative instruments: delegated legislation. The procedure begins with Parliament enacting a broad statute (known as a parent or enabling Act) that delegated law-making authority to a government department or minister. The delegated legislation is referred to as a statutory instrument since it implements (helps to implement) the statute's provisions. See Huxley-Binns, R. and Martin, J. (2014) *Unlocking the English Legal System*. 4th ed. New York: Routledge, p. 12.
[101] Jensen-Haxel, P. (2012) *op. cit.*, p. 448.

will flourish (illicit/illegal activity). Such uncontrollable behavior will become progressively harder to identify (identification). Enforcing the law against such conduct will become more difficult or even impossible (impracticality or impossibility). These regulations may then become more ineffective—they will prevail and be enforced for 3D printing in supervised environments, but they will be mostly meaningless for 3D printing in unsupervised setting.

It is true that the judiciary develops more specific laws.[102] However, legislators are better at organizing bodies of law.[103] Stakeholders may seek for legal and regulatory reform if court action proves difficult.[104] Nevertheless, the concern with 3D-printed firearms is among ambiguity (uncertain) aversion, namely: how many innovations are we ready to endure if there really is a chance that those will be used to commit criminal acts? As a result, considering courts are unsuited to making such decisions,[105] it is ideal for ambiguous technology to be governed and regulated by authorized bodies (the executive and legislative).[106] The absence of guidance from the judiciary also paved the way to regulative commands. Therefore, supervising 3D-printed firearms is left to the legislative and executive branches for the time being.[107] Nonetheless, it is uncertain what kind of a danger or advantage 3D printing presents in our everyday lives. It is also feasible that technical advancements, notably the creation of more sophisticated

[102] Current laws and legal norms may already exist in the case of 3D printers, which can be utilized to handle societal concerns about future technologies. The best approach to understand the laws relating to specialized pursuits is to understand general rules, as Judge Frank H. Easterbrook highlighted in his 1996 essay, Cyberspace and the Law of the Horse. He maintained that the Internet was not exceptionally distinctive or special, necessitating either a reassessment of established legal principles or the creation of an altogether new set of regulations for the Internet. The very same logic may be used to 3D printing. Aside from existing legislation that may apply to new technology, several common law approaches exist to address issues that arise when things go south with emerging technologies. See Thierer, A.D. and Marcus, A. (2016) Guns, Limbs, and Toys: What Future for 3D Printing? *Minnesota Journal of Law, Science & Technology*, 17 (2), p. 827.

[103] KoŁacz, M.K., Quintavalla, A. and Yalnazov, O. (2019) Who Should Regulate Disruptive Technology? *European Journal of Risk Regulation*, 10 (1), p. 13.

[104] Some scholars have even heralded to legal and regulatory reform as *sui generis* means of protection for disruptive technology to boost its acceptance. See Craig, S. (2017) Protection for Printing: An Analysis of Copyright Protection for 3D Printing. *University of Illinois Law Review*, 2017 (1), pp. 338-339.

[105] The courts are the best overseer of risky technology. This is because the best cost-effective technique of funnelling relevant data from litigants to legislators is through the court. In the case of ambiguous/uncertain technology, regulatory decisions must be made based on subjective preferences rather than factual (objective) facts. The legislature is preferable than the judiciary because it is created to aggregate societal values. Moreover, if sophisticated governance is placed in hands of the court, it typically becomes hierarchically unclear. See Kołacz, M.K., Quintavalla, A. and Yalnazov, O. (2019) *op. cit*., p. 21.

[106] Kołacz, M.K., Quintavalla, A. and Yalnazov, O. (2019) *op. cit*., p. 13.

[107] Leon, K.N. (2019) *op. cit*., p. 463.

and user-friendly 3D printers, will expand criminal opportunities.[108] The complicated combination of 3D printing, existing legislation, and current practice merits a one-of-a-kind regulatory response. Whatever happens in reality with 3D printing will be paramount in addressing the legal concerns around the technology. [109] Legislative action, on the other hand, is slow, and campaigning for reform in the legislature is complicated.[110] Furthermore, there is a risk that using stringent legislative tools may unintentionally stifle innovation.[111] As a result, regulating the fast-moving technological innovation by the executive branch is still preferable. Regulation is largely acknowledged as "a sort of governance instrument, affecting the manner in which stakeholders involved in the innovation process conceive, execute, and use technologies." Regulation serves as the foundation of governance for technological innovation movements in the emerging technologies sector, which has an element of uncertainty amongst different players. In innovation process, regulation thereby integrates the activity of the stakeholders and acts as "guidance" towards collective good.[112]

Looking at the market aspects of 3D printing regulation, it is indeed interesting to observe the response from various stakeholders in the arms markets to the broader utilization and regulation of 3D printing technology. Again, a parallel can be drawn by looking at the music industry in 1999 striking down advancing technologies and new trends of social creations to maintain their markets and supply chain, i.e., album sales (see, case of Napster).[113] However, considering that the market dynamics are fluid

[108] It is really easy to see how increasingly powerful machines becoming more widely available at a cheaper rate will result in more people 3D printing at home, and thus the potential danger to effective law enforcement.

[109] Daly, A. (2016b) *Socio-Legal Aspects of the 3D Printing Revolution*. London: Palgrave Macmillan, p. 97.

[110] Craig, S. (2017) *op. cit.*, p. 339.

[111] *Ibid*.

[112] Dagne, T.W. (2020) Governance of 3-D Printing Applications in Health: Between Regulated and Unregulated Innovation. *The Columbia Science and Technology Law Review*, 21 (2), p. 304-305.

[113] Napster originated as a peer-to-peer file-sharing platform which gave users the freedom to freely exchange audio recordings with one another. The Recording Industry Association of America (RIAA) won its case against Napster for violating intellectual property rights. This case was monumental given that it constitutes one of the earliest instances of the music industry tackling the problem of online copyright violations. The RIAA claimed that Napster was involved in or encouraging users to duplicate material that was protected by copyrights without compensation or the explicit permission of the intellectual property holders. Napster, according to the RIAA, would seriously hurt the music industry's sales. The Napster case set a legal precedent for file-sharing platforms and copyright law. The ruling was significant because it established that Napster could be held liable for contributory and vicarious infringement of copyright. A protracted legal dispute between Napster and the RIAA along with numerous musicians resulted in a brief shutdown of the service in 2001. Napster suspended operations in 2001 and filed for bankruptcy in June 2002 shortly after

in the sense that it is not always necessarily a binary notion towards polarization—like "whoever is not with us is against us,"[114] thus predicting the plausible reactions of the stakeholders may not be an easy task. Following on the Napster model, it is logical to think that the arms industry would attempt to intervene with the regulatory processes and imprint its agenda to maintain the existing supply chains (e.g., argue for the ban of 3D-printed firearms). Yet, arguing for the ban of 3D-printed firearms could outright spark momentum towards clawing back on the conventional firearms as well.

Furthermore, only time can tell how disruptive 3D printing is from a legal standpoint. Given the current political economics of 3D printing's emergence as a consumer-accessible technology, and also the participation of the nation-state, major companies, and people in its application,[115] it appears that it is never too early or too late to begin devising indirect regulatory action against 3D-printed firearms today. Admittedly, there would still be some lawlessness all around the fringes of regulation, with desperate users capable to secretly build their own 3D printers, and get 3D printing files and materials for other channels if they know where to seek. The lingering "ungovernable" (or hard to regulate) portions of the Internet at the fringes, as well as other "under the radar" activity in the darknet, reflect this. As a result, the regulations governing 3D printing *vis-à-vis* legal enforcement will not be able to be effectively applied.[116] As previously stated, this was the case before all these technical advancements. In a progressively decentralized society or market, it may be more difficult to enforce laws. But, with decentralization, also comes transparency. Therefore, regulation is still the most viable option to regulate disruptive technological innovations. What is left is just the matter of how and when to regulate.

4.2. THE CASE AGAINST REGULATING 3D-PRINTED FIREARMS

Prominent opponents of regulating 3D printing technology argued that market inefficiencies in the technology sector could not be pinpointed and that the sector itself lacked identifiable traits that would justify government intervention. Advising the government to concentrate on programs that will enhance economic growth rather than stifling innovation.[117] Passing the rules to regulate technological advancement poses a significant danger

losing a string of lawsuits. In the succeeding decades, the corporation saw a number of ownership changes.

[114] According to the Synoptic Gospels, Jesus said, "Whoever is not with Me is against Me, and whoever does not gather with Me scatters." (See Matthew 12:30; Luke 9:50; and Mark 9:40).

[115] Daly, A. (2016b) *op. cit.*, p. 99.

[116] Daly, A. (2016b) *op. cit.*, pp. 99-100.

[117] Traficonte, D. (2020) Collaboration in the Making: Innovation and the State in Advanced Manufacturing. *The Columbia Science and Technology Law Review*, 21 (2), p. 339.

in a system designed to stimulate innovation and protect the public.[118] Any limitation on technical innovation and development will hinder the technology's utilization and potential to inspire others.[119] Any regulation must weigh the advantages to innovation and people's safety against the threat of stifling a technology that has considerably more benefits than potential downsides.[120]

Some claim that the fear of 3D-printed firearms is overblown, unfounded, and serves as a diversion from the many advantages 3D printers provide to our society. Early in May of 2013, the warning sirens started to ring endlessly. That month, numerous articles appeared, warning people about the grim future we all faced as a result of the oncoming avalanche of 3D-printed firearms.[121] Other periodicals participated in the panic, building the hysteria. Most of these narratives have the same overarching theme: be terrified, be extremely fearful. Soon, the streets will be swarming with crooks equipped with many 3D-printed firearms that they can simply make at home. These 3D-printed gun-toting criminals would be capable of committing horrendous crimes that would be impossible to track.[122] For the following few years, the avalanche of articles died down. The news of 3D-printed firearms has started to trickle in since then. Yet, several years later, the actual reality is a far cry from what has been predicted. After nearly nine years, there has so far been little increase in 3D-printed gun-related incidents.

As a result, the concern of what transpired must be addressed—why did the worries of a slew of 3D-printed gun-wielding criminals materialize? The simplest answer to that complex question is that the alarms went off just a bit too soon. The fundamentals of making 3D-printed firearms have always been difficult to get right in terms of cost and functionality. The majority of the plastic 3D-printed firearms just were not sturdy enough, and they shattered when discharged.[123] Most 3D-printed firearm could only discharge one

[118] As a result, when it comes to the issue of regulation on emerging technology innovation, regulation is frequently seen as a determinant that escalates the time and expense of research and commercialization, hence reducing the motivation to innovate. See Stern, A.D. (2017) Innovation Under Regulatory Uncertainty: Evidence from Medical Technology. *Journal of Public Economics*, 145 (1), p. 181.

[119] Couch, J. (2016) *op. cit.*, p. 535.

[120] *Ibid*.

[121] Hassan, K. (2020) op. cit., p. 45.

[122] *Ibid*.

[123] Forensic scientist Olivier Delémont thinks that anybody who does have access to a traditional firearm would not be tempted by such a firearm, stating that "It would be more dangerous to be the shooter than to be the target." See Wilke, C. (2019) *3-D Printed "Ghost Guns" Pose New Challenges for Crime-Scene Investigators.* [online] Washington, D.C.: Science News. Available from: `https://www.sciencenews.org/article/3d-printed-guns-plastic-ballistics-crime` [Accessed 29 April 2022].

round before the barrel will need to be replaced. A blade, on the other hand, may be more deadly because it can be used multiple times. For instance, if a terrorist was forced to discharge the firearm during an airline hijacking, his leverage over the other passengers would be lost.[124] Optionally, 3D printing a metal firearm would produce a more potent weapon than a 3D-printed plastic firearm. Unfortunately, the costs would be exorbitant because an industrial-grade printer is required to do such task.

Furthermore, in Adam Thierer's book entitled: Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom, he defines permissionless innovation as "refer[ring] to the notion that experimentation with new technologies and business models should generally be permitted by default."[125] Will innovators be compelled to gain validation from government officials before developing and deploying new devices and services, or should they be liberated to innovate with new technology and business models? If the former, "the precautionary principle," prevails over the latter, "permissionless innovation," Adam Thierer claims, the outcome will be fewer services, lower-quality products, increased cost, sluggish economic growth, and a generally lower living standard.[126] The key idea is that governments should "allow" unfettered experimentation and risk-taking with new technology until and unless there is a strong reason to do otherwise. That is, policymakers must only act if there is a genuine harm or issue, or if it can be demonstrated that unfettered innovation will cause substantial damage to society.[127] Governments must be able to demonstrate that the advantages of intervention outweigh the downsides of continuing to experiment. Permissionless invention should be given the "benefit of the doubt" unless they can prove otherwise. The position's principal justification is based on economics. This notion suggests that defaulting to permissionless innovation will "advance long-term economic progress."[128]

The aforementioned argument however, was not meant to be the "overarching" and "one-size-fits-all" panacea, simply because it fails to

[124] Walther, G. (2015) *op. cit.*, p. 1441.

[125] Thierer, A.D. (2014) *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom.* 1st ed. Arlington, Virginia: Mercatus Center at George Mason University, p. 1.

[126] Whenever "precautionary principle" rationale is used to mould government policy, it poses a major threat to technological innovation, socioeconomic entrepreneurialism, and long-term development. "Permissionless innovation," on the other hand, has recently driven the boom of the Internet along with much of the current tech sector, and it is poised to drive the next industrial revolution—if we allow it. See Thierer, A.D. (2014) *op. cit.*, p. 2.

[127] Pantella IV, J.J. (2017) Ready, Print, Fire! Regulating the 3D-Printing Revolution. *Journal of Law, Technology & the Internet*, 8 (1), pp. 3-4.

[128] Thierer, A.D. (2014) *op. cit.*, p. 128-129.

take into account the Coasean approach.[129] Coase's paper criticized the conventional notion of externalities. In his paper, it was claimed that in an environment without transaction costs, bargaining over contracts would remove externalities and would force the market to an effective outcome without the need for interference from the government. Such involvement is only necessary when transaction costs are not zero.[130] In that case, regulation may accomplish a number of objectives—and from a Coasean standpoint, laws and regulations are put in place to lower transaction costs and improve market efficiency.[131] The online-based 3D printing platform paradigm offers a previously unthinkable prospect of moving closer to Coase's portrayed equilibrium. At the same time, issues surrounding platform regulation remain complicated and will primarily hinge on the socioeconomic policies and objectives at hand—like those of Thierer's. The 3D printing industry may be suitable for private ordering in certain contexts, for instance developing safety feature by means of firmware programmed to identify unprintable objects, as technical and trade-related mechanisms grow in breadth and depth—in this case, let the market innovate and private ordering structures the markets in unregulated industries. However, the outcomes of private ordering might not be optimal. Therefore, for other contexts, like guaranteeing basic public safety requirements by means of oversight, deviants may disrupt and circumvent the safety features of private ordering. Thus, regulators must intervene to offer an auxiliary framework that adds another layer of protective mechanisms.

4.3. PROPOSED REGULATORY RESPONSE: A THREE-PRONGED APPROACH

3D printing is a two-edged sword:[132] although it has numerous prospective benefits to the public, it also has certain potentially serious repercussions

[129] In law and economy, the Coase theory is a property rights economic and legal theory put out by economist Ronald H. Coase. According to the Coase Theorem, when parties have competing property rights, negotiations between them will result in an effective outcome regardless of who ends up receiving the rights to the property in the end, provided that the transaction costs resulting from the negotiations are negligible. See Coase, R.H. (2013) The Problem of Social Cost. *The Journal of Law & Economics*, 56 (4), p. 838.

[130] Elkin-Koren, N. and Salzberger, E.M. (1999) Law and Economics in Cyberspace. *International Review of Law and Economics*, 19 (4), p. 567.

[131] Dempsey, P.S. (1989) Market Failure and Regulatory Failure as Catalysts for Political Change: The Choice Between Imperfect Regulation and Imperfect Competition. *Washington and Lee Law Review*, 46 (1), p. 20.

[132] "When you have a general-purpose technology, it will be [utilized] for things you [do not] want people to use it for," Michael Weinberg as remarked by Anne Lewis in his commentary. See Lewis, A. (2014) *op. cit.*, p. 310.

which should not be overlooked.[133] It would be impossible to oversee once household and industrial 3D printers are capable of large-scale manufacturing. Instead of dismissing the reality that the 3D printing revolution ushers in new eras of growth, prosperity, and alternatives, we must contend not only with the ambiguity that comes with the 3D printing period, but also with the grave risks, hazards, perils, and dangers that follow it. Regulators must be cognizant of the whole range of risks and problems in order to prepare society before catastrophic events emerge.[134]

Beyond the realm of intellectual property, 3D printing has become a hot topic in the criminal justice system. Currently, 3D printers have demonstrated that they are capable of creating real, working firearms— hence compromising current gun restrictions.[135] This has prompted authorities throughout the world to assess the risks of 3D printing technology and, in some cases, introduce laws prohibiting such usage.[136] Although these actions are admirable, they are still in their early phases, and they only attempt to utilize retaliatory sanctions to prohibit particular applications of the technology—they do little to eliminate its unlawful usage in the first place.[137]

A movement for regulatory change in the context of 3D printers and their capabilities has been proposed by some scholars. Obviously, each scholarship contributes a unique viewpoint to the discussion.[138] Most scholars write in the hopes of informing or alerting 3D printer aficionados for the need to obtain license to manufacture, or to be aware of regulations

[133] Gilpin, L. (2014) *The Dark Side of 3D Printing: 10 Things to Watch.* [online] San Francisco, CA: TechRepublic. Available from: `https://www.techrepublic.com/article/the-dark-side-of-3d-printing-10-things-to-watch/` [Accessed 8 May 2022].

[134] Yanisky-Ravid, S. and Kwan, K. S. (2017) *op. cit.*, p. 927.

[135] *Ibid*.

[136] The City Council of Philadelphia declared in November 2013, no individual shall utilize a 3D printer to build any weapon, or any portion or part thereof, unless such individual possesses a permit to fabricate weapons under Federal law, 18 U.S.C. § 923(a). See Lewis, A. (2014) *op. cit.*, p. 308; New South Wales, an Australian state, has outlawed the ownership of files for 3D printing guns. See Butler, J. (2015) *NSW Tightens 3D Printed Gun Legislation As Expert Warns They're Getting Cheaper, More Effective.* [online] New York City: HuffPost. Available from: `https://www.huffpost.com/archive/au/entry/3d-printed-gun-laws-nsw_n_8595818` [Accessed 8 May 2022]; The United Kingdom's Firearms Licensing Law was modified to include a paragraph specifically prohibiting 3D-printed firearms. The prohibitions in section 57(1) of the Firearms Act 1968 cover the manufacturing, procurement, transfer, and ownership of 3D-printed firearms, ammunition, or spare parts in the United Kingdom. See Home Office (2021) *Guide on Firearms Licensing Law (Accessible Version).* [online] London: Gov.UK. Available from: `https://www.gov.uk/government/publications/firearms-law-guidance-to-the-police-2012/guide-on-firearms-licensing-law-accessible-version#chapter-23-proof-of-firearms` [Accessed 8 May 2022].

[137] Yanisky-Ravid, S. and Kwan, K.S. (2017) *op. cit.*, pp. 930-931.

[138] Kinsley, K., Brooks, G. and Owens, T. (2014) *op. cit.*, p. 13.

that require them to declare the firearms printed.[139] Another viewpoint is that 3D printer laws ought not be enacted too soon.[140] Nevertheless, the aforementioned regulatory measures fail to take into account the concerns of personal liberty, the technological development, and the interest of public safety as a whole. Prevailing scholarships also proposed ambitious regulation to require licensing for 3D printers and 3D-printed firearms. But this initiative lacks enforceability.[141] Simply requiring licensing and transfer registration of 3D-printed firearms does not address the issues of illicit 3D-printed firearms. 3D-printed gun-toting criminals will just refuse to comply.[142] Another initiative is to impose complete ban on 3D-printed firearms, which would be highly impractical—and even if it were to happen, such restrictions and rules would be hard to enforce.[143] In addition, efforts to regulate online file sharing may also be futile.[144] Another strategy is to make the processes of manufacturing a firearm and owning it more complex and expensive, thus delaying the technology's adoption.[145] However, it would be too desperate and counterproductive to the purpose of developing technological development and reaping the advantages it delivers to society. Efforts have also been made to enhance the capacity of 3D printer software to reject producing components that are analogous to firearms. However, improving the software's security may be meaningless since the software itself might be jailbroken.[146]

Ultimately, the suggested regulation appears to address several major concerns: gun manufacturing and possession by inappropriate individuals such as felons or minors, the fabrication of ghost guns, and ghost guns still passing through security screening. Bans, including on 3D-printed plastic firearms, does not entirely answer any of these problems since it does not prevent the manufacture of the firearms; rather, it penalizes those who manufacture illegal firearms. Likewise, the serial numbers with registration

[139] Lewis, A. (2014) *op. cit.*, p. 307.
[140] Finocchiaro thinks that given the small possibility for 3-D printing technology to inflict economic harm and the fact that neither politicians nor the courts can predict its future potential, it would be smart to minimize legislative incursions into the industry. See Finocchiaro, C. (2013) Personal Factory or Catalyst for Piracy? The Hype, Hysteria, and Hard Realities of Consumer 3-D Printing. *Cardozo Arts & Entertainment Law Journal*, 31 (2), pp. 507-508.
[141] Leon, K.N. (2019) *op. cit.*, p. 446.
[142] Jacobs, J.B. and Haberman, A. (2017) *op. cit.*, p. 146.
[143] Osborn, L.S. (2013) *op. cit.*, p. 579.
[144] Langvardt, K. (2016) *op. cit.*, p. 794.
[145] Leon, K.N. (2019) *op. cit.*, p. 464.
[146] Leon, K.N. (2019) *op. cit.*, p. 465.

technique tries to solve the broader issues,[147] but it mainly fails owing to its dependence on human compliance with merely the threat of modest penalty.[148] While some kinds of 3D-printed items are supervised, there is presently no overall government regulatory scheme in place for 3D printers. While establishing the foundation for such a mechanism would be tricky at first, diverting the regulatory attention away from 3D-printed weapons and toward the 3D-printers themselves might prove to be a more successful way of adopting and executing firearms-tracing rules.[149] In addition, a meaningful approach will resolve these problems at their source and therefore will necessitate a multifaceted approach.

Additionally, since there is currently no empirical evidence as to how effective (or not) these various measures criminalizing and seeking to constrain the production and distribution of 3D-printed firearms, and considering the paucity of reliable and systematic evidence on the incidence of 3D-printed firearms (or firearm components) being found by police,[150] there really is no guarantee that the existing approaches proposed by the prevailing scholarships may be effective in regulating and supervising 3D-printed firearms. The open-source era provides myriad of unique obstacles to law enforcement, but this issue does not have to be unsolvable.[151]

The previous sections have brought up to surface that in this open-source era, ghost guns do possess potential security implications that necessitate governmental intervention. In relation to laws over technological innovations, this complexity is oftentimes exacerbated by the dynamics of the markets and societal standards which tends to be complex and multifaceted. There are cases against regulating technological innovation, but there are some merits for regulatory actions as an effective tool for managing technological innovations. To come up with regulatory responses

[147] 3D printers are designed to be identical, but little differences in their hardware result in distinct, immutable features. This feature might be used in place of a serial number. The researchers used this information to design a test in which they manufactured "five door keys apiece" using 14 different widely accessible 3D printers. They were able to identify the key to its printer 99.8% of the time using the algorithm and cross-referencing data about the keys. The test was replicated ten months later to see if the ability to match things to their original 3D-printer was impaired by increased usage of the printers, but the findings remained the same. This study implies that identifying the origin of a 3D-printed weapon without using a serial number system is a viable possibility. A regulatory framework focusing on 3D printers may be easier to implement than one attempting to govern the guns they create. See Eichner, A.W. (2020) *op.cit.*, pp. 223-224.

[148] Beyer, K.E. (2014) *op. cit.*, pp. 446-447.

[149] Eichner, A.W. (2020) *op. cit.*, p. 222.

[150] Daly, A. et al. (2021) *op. cit.*, p. 45.

[151] Tremble, C. (2018) Don't Bring a CAD File to a Gun Fight: A Technological Solution to the Legal and Practical Challenges of Enforcing ITAR on the Internet. *Fordham Law Review*, 87 (1), p. 139.

that are balanced enough to ensure public safety without stifling the positive advancements of 3D printing technology, this paper approaches this issue using solution-oriented approach by taking a more problem-solving strategy by beginning with a real-world issue followed by examining which theories may be used to address it.[152]

The synthetization in this paper argues based on the solution-oriented approach argues that producers of at-home 3D printers will tolerate government regulation and are willing to collaborate with governmental intervention to a certain degree—known as the producers' "threshold" based on the threshold models of collective behavior by Granovetter.[153] This model is deemed straightforward but tenable to explain individual or collective willingness under the pressure of social influence.[154] In this case, the practical problems and dilemmas as mentioned above are the social influences or "shocks." Since threshold models and game-theoretic models depend on the premise that players act rationally in the face of ample information, and consequently, both contend that logic (occasionally deliberate) frequently influences behavior as a whole.[155] This model is predicated on the notion that human beings are more inclined to be shaped by the actions of others, and that whenever they are subjected to circumstances that include "shocks" caused by societal influence, they will behave in accordance with the standards and expectations of those around them. Additionally, it implies that despite being confronted with complex situations, individuals will frequently make reasonable decisions based on the information at hand.

Game-theoretic models such as the prisoner's dilemma is a wonderful example of how self-serving actions by both players (producers and government) will lead to a conclusion that is unfavorable for neither the producers nor the government. This game-theoretic approach enables each player to comprehend the potential risks and benefits of their choices and take action to maximize the outcomes they achieve. They can come up with a solution that maximizes the collective benefit whilst minimizes the individual cost. Unregulated market will also result in a tragedy of the commons, where the lack of regulation could lead to a race to the bottom in terms of quality, safety, and environmental standards.[156] The aforementioned findings shows that cooperation amongst participants is necessary to develop a more just

[152] Watts, D. (2017) Should social science be more solution-oriented? *Nature Human Behaviour*, 1, p. 1.
[153] Granovetter, M. (1978) Threshold Models of Collective Behavior. *American Journal of Sociology*, 83 (6), p. 1422.
[154] Watts, D. et al. (2017) *op. cit.*, p. 1.
[155] Granovetter, M. et al. (1978) *op. cit.*, p. 1433.
[156] This is not only detrimental to customers, but it is also detrimental to businesses, who will be forced to compete on pricing as opposed to the quality of their goods or services. This could

and equitable framework that benefits everyone in the long run. This article also believes that the applicable regulatory actions that can be implemented may be in the form of law and designing-out crime (infrastructure). The definition of law is rather self-explanatory: it is an authoritative instrument that establishes the legal foundation for the imposition of penalties for criminal behavior. On the contrary, designing-out crime entails altering the physical environment in order to lessen the chances of wrongdoing.[157]

Instead of attempting to prematurely pigeonhole new technological invention into prevailing regulatory categorization, governments might allow the sector to be "born free" rather than "regulated in captivity." As a result, the sector prospered from a policy of benign neglect in this regard.[158] Regulators should not seek an outright ban. They may instead, regulate the fringes of this innovative technology, in hope to control such developments so not to harm public interests, but careful enough not to stifle its growth. For both the Internet and digital technology, permissionless innovation would seem to be the standard practice, giving entrepreneurs an "unequivocal free pass" to just let their imaginations run freely and experimenting with a limitless array of intriguing new products and services. 3D printing can be governed by the same strategy and regulatory approach.[159] Governments may explain and advocate a vision of permissionless innovation for 3D printing, sending a clear message to people that commercial and non-commercial entrepreneurial activities will be permissible.

This suggests that, in the case of 3D printing, governments would make it absolutely clear in their statements that creators in this field will be granted wide leeway in their creative pursuits, and that governance will not be founded on hypothetical concerns or handled via ex ante regulatory limitations. People will be free to experiment with 3D printing technology in general, and any difficulties that arise will be dealt ex post.[160] This article also contends that the first step in regulating this field should not be to restrict the sharing of "technical information" generated by people. Therefore, this article proposes a three-pronged regulatory approach along the fringes of 3D printers as a preventive measure that incorporates protection for public security in the face of the dangers posed by 3D-printed firearms, but still taking into account technological development aspects of this innovation and

result in unsustainable rivalry that spirals out of control, driving down prices and lowering overall product and service quality.

[157] Nelken, D. (2018) The Legitimacy of Global Social Indicators: Reconfiguring Authority, Accountability and Accuracy. *Les Cahiers de Droit*, 59 (1), p. 44.

[158] Thierer, A.D. and Marcus, A. (2016) *op. cit.*, p. 823.

[159] Thierer, A.D. and Marcus, A. (2016) *op. cit.*, pp. 824-825.

[160] Thierer, A.D. and Marcus, A. (2016) *op. cit.*, p. 826.

the personal liberty of its users. The true objective of this approach would be to discourage people from making 3-D printed firearms at home and reduce the likelihood of increased gun violence.

4.3.1 Turn to Technology

Rather than controlling and penalizing the sharing or possession of CAD files, this article suggested that the government collaborate with producers of at-home 3D printers to develop firmware that can identify whether a file is capable towards becoming an undetected weaponry or a component of firearm. The approach would start with the development of firmware that stops 3D printers from creating gun-making components. The printer might be programmed to reject creation of undetectable firearms that are constructed by the user from printed components.[161] This can be seen as a form of private ordering structures that fill in the gaps in the market that is currently unregulated, known as technological protection for exclusion measures. It is also a way of designing-out crime[162] since by programming 3D printers to not be able to print firearm components, it prevents criminals from being able to easily create ghost guns. This is a way of deterring criminals from attempting to commit this type of crime in the first place.

This firmware mimics current printers' inability to duplicate currencies. Many copiers nowadays are unable to scan or copy banknotes as a result of this firmware. These setups can definitely be applied to 3D printers as well. In addition, 3D printers would need to be kept updated on which newer designs they are not permitted to manufacture.[163] However, such firmware can definitely be compromised, but it would be a lot more difficult task than obtaining a weapon CAD file freely online. The creation of exclusionary mechanisms frequently inspires users to create counter-mechanisms for code-cracking and hacking programs. Hence, the effectiveness of security measures in technology hinges on its resistance to attempted hacking and the absence of cheap ways to get around it. To function effectively, the exclusion measures must be resilient to hacking. Once broken into, authorities then have historically reacted to circumvention by passing anti-circumvention legislation that renders circumvention of safety precautions illegal.[164]

The anti-circumvention legislation by the authorities will act as an auxiliary. Elkin-Koren and Salzberger contends that there are two

[161] Tremble, C. (2018) *op. cit.*, pp. 139-140.
[162] See Nelken, D. (2018) *op. cit.*, p. 44.
[163] Walther, G. (2015) *op. cit.*, p. 1443.
[164] Elkin-Koren, N. and Salzberger, E.M. (2013) *The Law and Economics of Intellectual Property in the Digital Age: The Limits of Analysis*. New York: Routledge, pp. 192-193.

economic rationales to justify the anti-circumvention regime: the necessity to discourage circumvention and the dire need to prevent what others see as an unnecessary technological race.[165] The former simply means that the anti-circumvention regime is there to discourage circumvention tools by making it not cost-effective, while the latter bears a deeper understanding—the urgency to end the technological arms race between anti-exclusion tools and their counterparts.[166] The government may also work with 3D printer manufacturers to use the blockchain technology to keep records on every printed items.

Blockchain[167] was at the heart of some of the next-generation firearms startups' product ideas. [168] This initiative intends to integrate blockchain into a 3D printer so that it logs every time the device 3D prints an item, as well as its exact location, and the blockchain data are totally safe and reliable.

4.3.2 Cooperate with Industries

Measures might be targeted at 3D printer manufacturers to develop firmware that demands personal identity to be submitted first in order to operate the device. [169] This approach is fashioned after the regulatory framework that oversees the sale of controlled drugs to verify that they have not acquired above a certain amount of the medication. The 3D printer manufacturers would be in charge of keeping the records, which would be accessible to law enforcement through appropriate channels.[170]

Manufacturers may be obliged to ensure that 3D printers marketed to the general public may only produce specific materials. A license would

[165] Elkin-Koren, N. and Salzberger, E.M. (2013) *op. cit.*, pp. 197-198.

[166] A number of economists have argued that the creation of circumvention tools is an unnecessary use of economic resources. They contend that such a competition can waste resources which might be better spent to make more worthwhile investments. Furthermore, the constantly changing dynamics of this rivalry in technology is not recognized by the present-day economic system. The interactions between emerging technology versus counter-technology could feed into the technological arms race, which may eventually give rise to more advancements in exclusion tools as well as various other technologies. In this regard, the competition amongst technological instruments for technological exclusion and technological circumvention could contribute to advancements in technology in other areas, thereby benefitting overall innovation, advancement, and societal welfare. See *Ibid*.

[167] Blockchain is a more advanced sort of digital ledger technology ("DLT") that is best recognized for its correlation to cryptocurrencies like Bitcoin. Blockchain is a sort of computerized archiving that is decentralized and verifiable. Encrypted and numerous independent backups of data are frequently used in blockchain to actually make information more resistant to malicious tampering, loss of data, and unwanted access. Blockchain can be used to keep track of specific occasions or incidents in an unalterable, automatically documented ledger.

[168] Stevenson, D. (2020) Smart Guns, the Law, and the Second Amendment. *Penn State Law Review*, 124 (3), p. 734.

[169] Tremble, C. (2018) *op. cit.*, p. 140.

[170] *Ibid*.

be necessary for members of the public who wish to print things requiring regulated materials. The license may impose a cap on the amount of controlled material they can acquire, along with a requirement that the licensed user reports on the final product created with this material.[171] In addition to reporting on materials manufactured by 3D printers, the proposed regulation may also compel licensees to inform on any unused materials.[172] This would make licensees responsible for any unused materials, making it more difficult for them to resell or even use them unlawfully.

4.3.3 Strengthening the Regulation on Propellant and Projectile

Since it is constructed of plastic, a 3D-printed plastic firearm poses a number of drawbacks, such as the printing of actual projectiles and propellant out of 3D printers is still unachievable.[173] Simply restricting a gun's frame will no longer be appropriate since 3D-printed firearms may be created at home and thus avoid all of those restrictions. To prevent the abuse of 3D-printed firearms, policymakers must go far beyond the frame and focus on alternative gun-control alternatives. For the time being, and for the near future, 3D printers are unable to produce every single component required to simply print, aim, and fire.[174] Printing gunpowder is now not possible thanks to a required chemical reaction, and will most certainly be incredibly complicated to achieve.[175] Since modern ammunition contains gunpowder, those who print firearms have two alternatives for ammunition: buy cartridges from nearby sports equipment retailers or buy propellant to use in printed ammo. As a result, regulating propellant is the most realistic approach to govern 3D-printed guns.

Since many bullets[176] is pre-loaded with propellant, it is important to broaden the regulation to every transaction of munitions containing propellant or a gunpowder substitute in order to govern it successfully.[177] This strategy would achieve a common ground between discouraging

[171] Reddy, P. (2014) The Legal Dimension of 3D Printing: Analyzing Secondary Liability in Additive Layer Manufacturing. *The Columbia Science and Technology Law Review*, 16 (1), p. 246.
[172] *Ibid.*
[173] Walther, G. (2015) *op. cit.*, p. 1441.
[174] Berkowitz, J. (2018) *op. cit.*, p. 81.
[175] Little, R. (2014) *op. cit.*, p. 1508.
[176] In common parlance, "bullet" usually refers to a cartridge, which really is a three-part vehicle with the actual bullet installed on the very end. The primer, propellant, and projectile itself are the three basic components of a cartridge. The chemical reaction is started by the primer. The propellant contains the chemical explosive's energy. Its job is to propel the bullet out of the firearm and into the target down range. The front segment of the cartridge is the actual projectile, the part that actually travels to hit the target.
[177] Berkowitz, J. (2018) *op. cit.*, p. 81.

the manufacture of illegal 3D-printed firearms while not hamstringing individuals who use 3-D printing for non-firearm applications. As a result of some sort of government oversight in place to regulate the presence and distribution of 3D-printed firearms, the possibility of increasing gun violence against society would be reduced.[178]

In addition to the three-pronged regulatory approach as mentioned above, regulators must also think about how teaching the public and business on how to use new technology properly might help achieve policy goals in a less expensive and much more efficient way. The purpose of such literacy instruction and "digital citizenship" activities is to develop rational thinking standards to enable the assimilation of new technology into society while also encouraging ethical conduct, politeness and responsible utilization new technologies.[179] For 3D printing, this might include lectures on the risks of developing instruments that could have negative societal consequences, such as guns, unsafe medical gadgets, or counterfeit items.

The 3D printing community may also want to exercise caution and refrain from publishing CAD files for firearm or its component. This would not preclude a motivated individual from constructing a firearm using their own CAD program, but it would be more difficult than merely downloading a file and printing it off. However, in the absence of regulatory solutions, engaging the 3D printing community in a meaningful discussion about the potential repercussions of their action may be beneficial. Communities could also adopt a code of conduct. A similar collaboration could help to alleviate 3D printing security problems.[180]

Considering 3D technology is being more widely used across the world, moral and legal difficulties may vary from country to country,[181] but most will be comparable enough to exhibit the traits addressed in this article. Regretfully, the approach offered in this paper is neither conclusive nor exhaustive. Building on lessons learnt from previous scholarships, it is believed that this suggested regulatory framework—schematic as it is for now—represents a tiny step forward in the appreciation of the complexities of regulating technological disruptors *vis-à-vis* 3D printing.

Governments would also be wise to wait and watch how social norms and society attitudes change, even if no rules or regulations exist. New technologies can be regulated in ways that go beyond the law. Since norms generally discourage many actions that are accessible but undesirable,

[178] Johnson, J.J. (2013) Print, Lock, and Load: 3-D Printers, Creation of Guns, and the Potential Threat to Fourth Amendment Rights. *Journal of Law, Technology and Policy*, 2013 (2), p. 358.
[179] Thierer, A.D. and Marcus, A. (2016) *op. cit.*, p. 829.
[180] Walther, G. (2015) *op. cit.*, p. 1443.
[181] Kinsley, K., Brooks, G. and Owens, T. (2014) *op. cit.*, p. 17.

social pressure and personal norms often operate as a "regulator" of new technology applications (and misappropriations).[182] To put it another way, many of today's fears surrounding 3D printer abuse might not always materialize in a significant way, or the public may grow to regard those behaviors more positively in the future. When all else fails, lawmakers can enact tailored legislation to address the most pressing matters, such as those involving the possibility for obvious, cataclysmic, imminent, and irreversible harm. Lastly, a shifting market is really not a terrible thing. At the very least, the oncoming shift has already been nice enough to announce itself publicly; we need to recognize what it is and how to reap the benefits of it.

5. CONCLUSION

3D printers and their printed firearms are not apocalyptic machines, given the risks they pose to public safety. We are on the precipice of the next industrial revolution, and opposing this directly will only result in penalizing the unforeseen and uncertain, while enraging a huge society that innovates or benefited from the technological advancements brought about by 3D printing. Lessons learned from the 2013 3D-printed firearms hysteria has proven that in the long term, no exhaustive prohibition on 3D-printed firearms can preserve public safety; instead, it would leave the law enforcement scurrying to catch up. The genie is also not yet out of the bottle, and current regulatory framework, on the other hand, can and will safeguard public safety from egregious infringers, such as those who try to 3D print a firearm for criminal activities by extending current regulations to tangentially target 3D-printed firearms manufacturing processes.

The solution to this potential problem is to ignore the regulations requiring strict controls on 3D printers and instead embrace 3D printing technology to assist people that are in need creating a better life. The authorities should take into account the many advantages of 3D printing as a technology when creating new regulations. The authorities may try to design narrower regulations to circumvent a stringent public scrutiny while providing timely oversight of 3D-printed firearms. The three-pronged approach relies on 3D printer producers as a control point for untraceable firearm creation and illicit firearm manufacturing surveillance. This strategy avoids contentious questions of public liberty while allowing gun restriction to the degree that the legislature has already reached an agreement. Ultimately, cognizance should be made of other possible illegal uses of 3D printing beyond just firearms fabrication.

[182] Thierer, A.D. and Marcus, A. (2016) *op. cit.*, pp. 829-830.

LIST OF REFERENCES

[1] Berkowitz, J. (2018) Computer-Aided Destruction: Regulating 3D-Printed Firearms Without Infringing on Individual Liberties. *Berkeley Technology Law Journal*, 33(1).

[2] Beyer, K. E (2014) Busting the Ghost Guns: A Technical, Statutory, and Practical Approach to the 3-D Printed Weapon Problem. *Kentucky Law Journal*, 103(3).

[3] Blackman, J. (2014) The 1st Amendment, 2nd Amendment, and 3D Printed Guns. *Tennessee Law Review*, 81(3).

[4] Butler, J. (2015) *NSW Tightens 3D Printed Gun Legislation As Expert Warns They're Getting Cheaper, More Effective.* [online] New York City: HuffPost. Available from: `https://www.huffpost.com/archive/au/entry/3d-printed-gun-laws-nsw_n_8595818` [Accessed 8 May 2022].

[5] Calandrillo, S. and Anderson, N.K. (2022) Terrified by Technology: How Systemic Bias Distorts U.S. Legal and Regulatory Responses to Emerging Technology. *University of Illinois Law Review*, 2022(2).

[6] Berkowitz, J. (2018) Computer-Aided Destruction: Regulating 3D-Printed Firearms Without Infringing on Individual Liberties. *Berkeley Technology Law Journal*, 33(1).

[7] Beyer, K. E (2014) Busting the Ghost Guns: A Technical, Statutory, and Practical Approach to the 3-D Printed Weapon Problem. *Kentucky Law Journal*, 103(3).

[8] Blackman, J. (2014) The 1st Amendment, 2nd Amendment, and 3D Printed Guns. *Tennessee Law Review*, 81(3).

[9] Butler, J. (2015) *NSW Tightens 3D Printed Gun Legislation As Expert Warns They're Getting Cheaper, More Effective.* [online] New York City: HuffPost. Available from: `https://www.huffpost.com/archive/au/entry/3d-printed-gun-laws-nsw_n_8595818` [Accessed 8 May 2022].

[10] Calandrillo, S. and Anderson, N.K. (2022) Terrified by Technology: How Systemic Bias Distorts U.S. Legal and Regulatory Responses to Emerging Technology. *University of Illinois Law Review*, 2022(2).

[11] Captain, S. (2013) *Journalists Smuggle 3-D Printed Gun into Israeli Parliament*. [online] New York: NBC News. Available from: ff `https://www.nbcnews.com/technolog/journalists-smuggle-3-d-printed-gun-israeli-parliament-6c10570532` [Accessed 10 May 2022].

[12] Chan, H.K. et al. (2018) The Impact of 3D Printing Technology on the Supply Chain: Manufacturing and Legal Perspectives. *International Journal of Production Economics*, 205.

[13] Christopher, G. (2015) 3D Printing: A Challenge to Nuclear Export Controls. *Strategic Trade Review*, 1(1).

[14] Coase, R.H. (2013) The Problem of Social Cost. *The Journal of Law & Economics*, 56 (4).

[15] Cosans, J. (2014) Between Firearm Regulation and Information Censorship: Analyzing First Amendment Concerns Facing the World's First 3-D Printed Plastic Gun. *American University Journal of Gender Social Policy and Law*, 22(4).

[16] Couch, J. (2016) Additively Manufacturing a Better Life: How 3D Printing Can Change the World Without Changing the Law. *Gonzaga Law Review*, 51(3).

[17] Craig, S. (2017) Protection for Printing: An Analysis of Copyright Protection for 3D Printing. *University of Illinois Law Review*, 2017(1).

[18] Dagne, T.W. (2020) Governance of 3-D Printing Applications in Health: Between Regulated and Unregulated Innovation. *The Columbia Science and Technology Law Review*, 21(2).

[19] Daly, A. (2016) Don't Believe the Hype? Recent 3D Printing Developments for Law and Society. In: Dinusha Mendis, Mark Lemley and Matthew Rimmer (eds.) *3D Printing and Beyond*. Cheltenham: Edward Elgar Publishing.

[20] (2016) *Socio-Legal Aspects of the 3D Printing Revolution*. London: Palgrave Macmillan.

[21] Daly, A. et al. (2021) 3D Printing, Policing and Crime. *Policing and Society*, 31(1).

[22] de Jong, J.P.J. and de Bruijn, E. (2013) Innovation Lessons From 3-D Printing. *MIT Sloan Management Review*, 54(2).

[23] Dempsey, P.S. (1989) Market Failure and Regulatory Failure as Catalysts for Political Change: The Choice Between Imperfect Regulation and Imperfect Competition. *Washington and Lee Law Review*, 46 (1).

[24] Eichner, A.W. (2020) Crime in the Age of Printable Guns: Methodologies and Obstacles to Prosecuting Federal Offenses Involving 3D-Printed Firearms. *Vermont Law Review*, 45(2).

[25] Elkin-Koren, N. and Salzberger, E.M. (1999) Law and Economics in Cyberspace. *International Review of Law and Economic*s, 19 (4).

[26] (2013) *The Law and Economics of Intellectual Property in the Digital Age: The Limits of Analysis*. New York: Routledge.

[27] Ferguson, C. (2013) *3-D Printed Guns Are a Boon for Criminals*. [online] Atlanta: CNN. Available from: `https://edition.cnn.com/2013/05/07/opinion/ferguson-printable-gun/index.html` [Accessed 25 April 2022].

[28] Finocchiaro, C. (2013) Personal Factory or Catalyst for Piracy? The Hype, Hysteria, and Hard Realities of Consumer 3-D Printing. *Cardozo Arts & Entertainment Law Journal*, 31(2).

[29] Gilpin, L. (2014) *The Dark Side of 3D Printing: 10 Things to Watch.* [online] San Francisco, CA: TechRepublic. Available from: https://www.techrepublic.com/article/the-dark-side-of-3d-printing-10-things-to-watch/ [Accessed 8 May 2022].

[30] Granovetter, M. (1978) Threshold Models of Collective Behavior. *American Journal of Sociology*, 83 (6).

[31] Hanrahan, J. (2019) *3D-Printed Guns Are Back, and This Time They Are Unstoppable*. [online] San Francisco, CA: WIRED. Available from: https://www.wired.co.uk/article/3d-printed-guns-blueprints [Accessed 6 May 2022].

[32] Hassan, K. (2020) Three-Dimensional Printed Hysteria. *3D Printing and Additive Manufacturing*, 7(2).

[33] Holbrook, T.R. and Osborn, L.S. (2015) Digital Patent Infringement in an Era of 3D Printing. *The UC Davis Law Review*, 48 (4).

[34] Home Office (2021) Guide on Firearms Licensing Law (Accessible Version). [online] London: Gov.UK. Available from: https://www.gov.uk/government/publications/firearms-law-guidance-to-the-police-2012/guide-on-firearms-licensing-law-accessible-version#chapter-23-proof-of-firearms [Accessed 8 May 2022].

[35] Huxley-Binns, R. and Martin, J. (2014) *Unlocking the English Legal System*. 4th ed. New York: Routledge.

[36] Jacobs, J.B. and Haberman, A. (2017) 3D-Printed Firearms, Do-It-Yourself Guns, & the Second Amendment. *Law and Contemporary Problems*, 80(2).

[37] Jensen-Haxel, P. (2012) 3D Printers, Obsolete Firearm Supply Controls, and the Right To Build Self-Defense Weapons Under Heller. *Golden Gate University Law Review*, 42(3).

[38] ——, (2015) A New Framework for a Novel Lattice: 3D Printers, DNA Fabricators, and the Perils in Regulating the Raw Materials of the Next Era of Revolution, Renaissance, and Research. *Wake Forest Journal of Law & Policy*, 5(2).

[39] Jiang, R., Kleer, R. and Piller, F.T. (2017) Predicting the Future of Additive Manufacturing: A Delphi Study on Economic and Societal Implications of 3D Printing for 2030. *Technological Forecasting & Social Change*, 117.

[40] Johnson, J.J. (2013) Print, Lock, and Load: 3-D Printers, Creation of Guns, and the Potential Threat to Fourth Amendment Rights. *Journal of Law, Technology and Policy*, 2013(2).

[41] Khasawneh, O.Y. (2018) Technophobia: Examining Its Hidden Factors and Defining It. *Technology in Society*, 54(1).

[42] Kietzmann, J., Pitt, L. and Berthon, P. (2015) Disruptions, Decisions, and Destinations: Enter the Age of 3-D Printing and Additive Manufacturing. *New Media and Society*, 58(2).

[43] Kinsley, K., Brooks, G. and Owens, T. (2014) International Legal and Ethical Challenges Related to the Use and Development of 3D Technology in the U.S. and China. *Journal of Knowledge Management Economics and Information Technology*, 4(1).

[44] Kołacz, M.K., Quintavalla, A. and Yalnazov, O. (2019) Who Should Regulate Disruptive Technology? *European Journal of Risk Regulation*, 10(1).

[45] Langvardt, K. (2016) The Doctrinal Toll of Information as Speech. *Loyola University Chicago Law Journal*, 47(3).

[46] Lara, S.S. (2019) The iTunes of Downloadable Guns: Firearms as a First Amendment Right. *Catholic University Journal of Law and Technology*, 28(1).

[47] Leon, K.N. (2019) Beyond the Single-Use Plastic Gun: The Need to Make 3D-Printed Gun Laws Shatterproof. *Houston Law Review*, 57(2).

[48] Lewis, A. (2014) The Legality of 3D Printing: How Technology Is Moving Faster than the Law. *Tulane Journal of Technology and Intellectual Property*, 17.

[49] Lewis, D. (2016) *Thanks to Sneaky Scanners, Anyone Can 3D Print a Copy of Nefertiti's Bust.* [online] Washington, D.C.: Smithsonian Magazine. Available from: `https://www.smithsonianmag.com/smart-news/thanks-sneaky-scanners-anyone-can-3d-print-copy-nefertitis-bust-180958213/` [Accessed 6 May 2022].

[50] Little, R. (2014) Guns Don't Kill People, 3D Printing Does? Why the Technology Is a Distraction from Effective Gun Controls. *Hastings Law Journal*, 65(6).

[51] Loutocký, P. (2019) 3D Printing and Beyond: Intellectual Property and Regulation. Mendis, D.; Lemley, M.; Rimmer, M. (Eds.). *Masaryk University Journal of Law and Technology*, 13(1).

[52] Ma, V.C.K. (2017) 3D Printing and the Law. *Intersect: The Stanford Journal of Science, Technology, and Society*, 11(1).

[53] McCutcheon, C. (2014) Deeper than a Paper Cut: Is It Possible to Regulate Three Dimensionally Printed Weapons or Will Federal Gun Laws Be Obsolete Before the Ink Has Dried? *Journal of Law, Technology and Policy*, 2014(2).

[54] McMullen, K.F. (2014) Worlds Collide When 3D Printers Reach the Public: Modeling a Digital Gun Control Law after the Digital Millenium Copyright Act. *Michigan State Law Review*, 2014(1).

[55] Murphy, S. (2013) *How Mail On Sunday "Printed" First Plastic Gun in UK Using a 3D Printer-and Then Took It on Board Eurostar without Being Stopped in Security Scandal.* [online] London: Dailymail. Available

from: https://www.dailymail.co.uk/news/article-2323158/How-Mail-On-Sunday-printed-plastic-gun-UK--took-board-Eurostar-stopped-security-scandal.html [Accessed 10 May 2022].

[56] Nelken, D. (2018) The Legitimacy of Global Social Indicators: Reconfiguring Authority, Accountability and Accuracy. *Les Cahiers de Droit*, 59(1).

[57] Nielson, H. (2015) Manufacturing Consumer Protection for 3-D Printed Products. *Arizona Law Review*, 57(2).

[58] Osborn, L.S. (2013) Regulating Three-Dimensional Printing: The Converging Worlds of Bits and Atoms. *San Diego Law Review*, 51(2).

[59] Pantella IV, J.J. (2017) Ready, Print, Fire! Regulating the 3D-Printing Revolution. *Journal of Law, Technology & the Internet*, 8(1).

[60] Pucino, D. (2020) *Ghost Guns: How Untraceable Firearms Threaten Public Safety*. [online] San Francisco, CA: Giffords Law Center. Available from: https://giffords.org/lawcenter/report/ghost-guns-how-untraceable-firearms-threaten-public-safety/ [Accessed 12 June 2022].

[61] Reddy, P. (2014) The Legal Dimension of 3D Printing: Analyzing Secondary Liability in Additive Layer Manufacturing. *The Columbia Science and Technology Law Review*, 16(1).

[62] Richardson, M. (2016) Pre-Hacked: Open Design and the Democratisation of Product Development. *New Media and Society*, 18(4).

[63] Rustad, M.L. and Koenig, T.H. (2019) Towards a Global Data Privacy Standard. *Florida Law Review*, 71 (2).

[64] Sharpe, M. (2019) Products Liability in the Digital Age: Liability of Commercial Sellers of Cad Files for Injuries Committed With a 3D-Printed Gun. *American University Law Review*, 68(6).

[65] Staed, K.C. (2017) Open Source Download Mishaps and Product Liability: Who Is to Blame and What Are the Remedies? *Saint Louis University Public Law Review*, 36(1).

[66] Stern, A.D. (2017) Innovation Under Regulatory Uncertainty: Evidence from Medical Technology. *Journal of Public Economics*, 145(1).

[67] Stevenson, D. (2020) Smart Guns, the Law, and the Second Amendment. *Penn State Law Review,* 124(3).

[68] (2021) Going Gunless. *Brooklyn Law Review*, 86(1).

[69] Talbot, T. and Skaggs, A. (2020) Regulating 3D-Printed Guns Post-Heller: Why Two Steps are Better than One. *Journal of Law, Medicine and Ethics*, 48(4).

[70] Taylor, D.O. (2013) Patent Misjoinder. *New York University Law Review*, 88 (2).

[71] Thierer, A.D. (2014) *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom*. 1st ed. Arlington, Virginia: Mercatus Center at George Mason University.

[72] Thierer, A.D. and Marcus, A. (2016) Guns, Limbs, and Toys: What Future for 3D Printing? *Minnesota Journal of Law, Science & Technology*, 17(2).

[73] Traficonte, D. (2020) Collaboration in the Making: Innovation and the State in Advanced Manufacturing. *The Columbia Science and Technology Law Review*, 21(2).

[74] Tran, J.L. (2015) The Law and 3D Printing. *UIC John Marshall Journal of Information Technology Privacy Law*, 31(4).

[75] Tremble, C. (2018) Don't Bring a CAD File to a Gun Fight: A Technological Solution to the Legal and Practical Challenges of Enforcing ITAR on the Internet. *Fordham Law Review*, 87(1).

[76] Tu, K.V. and Meredith, M.W. (2015) Rethinking Virtual Currency Regulation in the Bitcoin Age. *Washington Law Review,* 90 (1).

[77] Tversky, A. and Kahneman, D. (1973) Availability: A Heuristic for Judging Frequency and Probability. *Cognitive Psychology*, 5(2).

[78] Walther, G. (2015) Printing Insecurity? The Security Implications of 3D-Printing of Weapons. *Science and Engineering Ethics*, 21(6).

[79] Watts, D. (2017) Should social science be more solution-oriented? *Nature Human Behaviour*, 1.

[80] Weinberger, V.P., Quiñinao, C. and Marquet, P.A. (2017) Innovation and the Growth of Human Population. *Philosophical Transactions of the Royal Society B: Biological Sciences*, 372(1735).

[81] Wilbanks, K. (2013) The Challenges of 3D Printing to the Repair-Reconstruction Doctrine in Patent Law. *George Mason Law Review*, 20(4).

[82] Wilke, C. (2019) *3-D Printed "Ghost Guns" Pose New Challenges for Crime-Scene Investigators.* [online] Washington, D.C.: Science News. Available from: `https://www.sciencenews.org/article/3d-printed-guns-plastic-ballistics-crime` [Accessed 29 April 2022].

[83] Willcocks, L., Venters, W. and Whitley, A. (2014) *Moving to the Cloud Corporation: How to Face the Challenges and Harness the Potential of Cloud Computing.* Hampshire: Palgrave Macmillan UK.

[84] Xu, D., Taylor, C.J. and Ren, Y. (2022) Wait-and-See or Whack-a-Mole: What Is the Best Way to Regulate Fintech in China? *Asian Journal of Law and Society*, First View.

[85] Yanisky-Ravid, S. and Kwan, K. S. (2017) 3D Printing the Road Ahead: The Digitization of Products When Public Safety Meets Intellectual Property

Rights—A New Model. *Cardozo Law Review*, 38(3). https://www.nbcnews.com/technolog/journalists-smuggle-3-d-printed-gun-israeli-parliament-6c10570532 [Accessed 10 May 2022].

[86] Chan, H.K. et al. (2018) The Impact of 3D Printing Technology on the Supply Chain: Manufacturing and Legal Perspectives. *International Journal of Production Economics*, 205.

[87] Christopher, G. (2015) 3D Printing: A Challenge to Nuclear Export Controls. *Strategic Trade Review*, 1(1).

[88] Coase, R.H. (2013) The Problem of Social Cost. *The Journal of Law & Economics*, 56 (4).

[89] Cosans, J. (2014) Between Firearm Regulation and Information Censorship: Analyzing First Amendment Concerns Facing the World's First 3-D Printed Plastic Gun. *American University Journal of Gender Social Policy and Law*, 22(4).

[90] Couch, J. (2016) Additively Manufacturing a Better Life: How 3D Printing Can Change the World Without Changing the Law. *Gonzaga Law Review*, 51(3).

[91] Craig, S. (2017) Protection for Printing: An Analysis of Copyright Protection for 3D Printing. *University of Illinois Law Review*, 2017(1).

[92] Dagne, T.W. (2020) Governance of 3-D Printing Applications in Health: Between Regulated and Unregulated Innovation. *The Columbia Science and Technology Law Review*, 21(2).

[93] Daly, A. (2016) Don't Believe the Hype? Recent 3D Printing Developments for Law and Society. In: Dinusha Mendis, Mark Lemley and Matthew Rimmer (eds.) *3D Printing and Beyond*. Cheltenham: Edward Elgar Publishing.

[94] (2016) *Socio-Legal Aspects of the 3D Printing Revolution*. London: Palgrave Macmillan.

[95] Daly, A. et al. (2021) 3D Printing, Policing and Crime. *Policing and Society*, 31(1).

[96] de Jong, J.P.J. and de Bruijn, E. (2013) Innovation Lessons From 3-D Printing. *MIT Sloan Management Review*, 54(2).

[97] Dempsey, P.S. (1989) Market Failure and Regulatory Failure as Catalysts for Political Change: The Choice Between Imperfect Regulation and Imperfect Competition. *Washington and Lee Law Review*, 46 (1).

[98] Eichner, A.W. (2020) Crime in the Age of Printable Guns: Methodologies and Obstacles to Prosecuting Federal Offenses Involving 3D-Printed Firearms. *Vermont Law Review*, 45(2).

[99] Elkin-Koren, N. and Salzberger, E.M. (1999) Law and Economics in Cyberspace. *International Review of Law and Economic*s, 19 (4).

[100] (2013) *The Law and Economics of Intellectual Property in the Digital Age: The Limits of Analysis*. New York: Routledge.

[101] Ferguson, C. (2013) *3-D Printed Guns Are a Boon for Criminals.* [online] Atlanta: CNN. Available from: https://edition.cnn.com/2013/05/07/opinion/ferguson-printable-gun/index.html [Accessed 25 April 2022].

[102] Finocchiaro, C. (2013) Personal Factory or Catalyst for Piracy? The Hype, Hysteria, and Hard Realities of Consumer 3-D Printing. *Cardozo Arts & Entertainment Law Journal*, 31(2).

[103] Gilpin, L. (2014) *The Dark Side of 3D Printing: 10 Things to Watch.* [online] San Francisco, CA: TechRepublic. Available from: https://www.techrepublic.com/article/the-dark-side-of-3d-printing-10-things-to-watch/ [Accessed 8 May 2022].

[104] Granovetter, M. (1978) Threshold Models of Collective Behavior. *American Journal of Sociology*, 83 (6).

[105] Hanrahan, J. (2019) *3D-Printed Guns Are Back, and This Time They Are Unstoppable*. [online] San Francisco, CA: WIRED. Available from: https://www.wired.co.uk/article/3d-printed-guns-blueprints [Accessed 6 May 2022].

[106] Hassan, K. (2020) Three-Dimensional Printed Hysteria. *3D Printing and Additive Manufacturing*, 7(2).

[107] Holbrook, T.R. and Osborn, L.S. (2015) Digital Patent Infringement in an Era of 3D Printing. *The UC Davis Law Review*, 48 (4).

[108] Home Office (2021) Guide on Firearms Licensing Law (Accessible Version). [online] London: Gov.UK. Available from: https://www.gov.uk/government/publications/firearms-law-guidance-to-the-police-2012/guide-on-firearms-licensing-law-accessible-version#chapter-23-proof-of-firearms [Accessed 8 May 2022].

[109] Huxley-Binns, R. and Martin, J. (2014) *Unlocking the English Legal System*. 4th ed. New York: Routledge.

[110] Jacobs, J.B. and Haberman, A. (2017) 3D-Printed Firearms, Do-It-Yourself Guns, & the Second Amendment. *Law and Contemporary Problems*, 80(2).

[111] Jensen-Haxel, P. (2012) 3D Printers, Obsolete Firearm Supply Controls, and the Right To Build Self-Defense Weapons Under Heller. *Golden Gate University Law Review*, 42(3).

[112] (2015) A New Framework for a Novel Lattice: 3D Printers, DNA Fabricators, and the Perils in Regulating the Raw Materials of the Next Era of Revolution, Renaissance, and Research. *Wake Forest Journal of Law & Policy*, 5(2).

[113] Jiang, R., Kleer, R. and Piller, F.T. (2017) Predicting the Future of Additive Manufacturing: A Delphi Study on Economic and Societal Implications of 3D Printing for 2030. *Technological Forecasting & Social Change*, 117.

[114] Johnson, J.J. (2013) Print, Lock, and Load: 3-D Printers, Creation of Guns, and the Potential Threat to Fourth Amendment Rights. *Journal of Law, Technology and Policy*, 2013(2).

[115] Khasawneh, O.Y. (2018) Technophobia: Examining Its Hidden Factors and Defining It. *Technology in Society*, 54(1).

[116] Kietzmann, J., Pitt, L. and Berthon, P. (2015) Disruptions, Decisions, and Destinations: Enter the Age of 3-D Printing and Additive Manufacturing. *New Media and Society*, 58(2).

[117] Kinsley, K., Brooks, G. and Owens, T. (2014) International Legal and Ethical Challenges Related to the Use and Development of 3D Technology in the U.S. and China. *Journal of Knowledge Management Economics and Information Technology*, 4(1).

[118] Kołacz, M.K., Quintavalla, A. and Yalnazov, O. (2019) Who Should Regulate Disruptive Technology? *European Journal of Risk Regulation*, 10(1).

[119] Langvardt, K. (2016) The Doctrinal Toll of Information as Speech. *Loyola University Chicago Law Journal*, 47(3).

[120] Lara, S.S. (2019) The iTunes of Downloadable Guns: Firearms as a First Amendment Right. *Catholic University Journal of Law and Technology*, 28(1).

[121] Leon, K.N. (2019) Beyond the Single-Use Plastic Gun: The Need to Make 3D-Printed Gun Laws Shatterproof. *Houston Law Review*, 57(2).

[122] Lewis, A. (2014) The Legality of 3D Printing: How Technology Is Moving Faster than the Law. *Tulane Journal of Technology and Intellectual Property*, 17.

[123] Lewis, D. (2016) *Thanks to Sneaky Scanners, Anyone Can 3D Print a Copy of Nefertiti's Bust.* [online] Washington, D.C.: Smithsonian Magazine. Available from: `https://www.smithsonianmag.com/smart-news/thanks-sneaky-scanners-anyone-can-3d-print-copy-nefertitis-bust-180958213/` [Accessed 6 May 2022].

[124] Little, R. (2014) Guns Don't Kill People, 3D Printing Does? Why the Technology Is a Distraction from Effective Gun Controls. *Hastings Law Journal*, 65(6).

[125] Loutocký, P. (2019) 3D Printing and Beyond: Intellectual Property and Regulation. Mendis, D.; Lemley, M.; Rimmer, M. (Eds.). *Masaryk University Journal of Law and Technology*, 13(1).

[126] Ma, V.C.K. (2017) 3D Printing and the Law. *Intersect: The Stanford Journal of Science, Technology, and Society*, 11(1).

[127] McCutcheon, C. (2014) Deeper than a Paper Cut: Is It Possible to Regulate Three Dimensionally Printed Weapons or Will Federal Gun Laws Be Obsolete Before the Ink Has Dried? *Journal of Law, Technology and Policy*, 2014(2).

[128] McMullen, K.F. (2014) Worlds Collide When 3D Printers Reach the Public: Modeling a Digital Gun Control Law after the Digital Millenium Copyright Act. *Michigan State Law Review*, 2014(1).

[129] Murphy, S. (2013) *How Mail On Sunday "Printed" First Plastic Gun in UK Using a 3D Printer-and Then Took It on Board Eurostar without Being Stopped in Security Scandal.* [online] London: Dailymail. Available from: `https://www.dailymail.co.uk/news/article-2323158/How-Mail-On-Sunday-printed-plastic-gun-UK--took-board-Eurostar-stopped-security-scandal.html` [Accessed 10 May 2022].

[130] Nelken, D. (2018) The Legitimacy of Global Social Indicators: Reconfiguring Authority, Accountability and Accuracy. *Les Cahiers de Droit*, 59(1).

[131] Nielson, H. (2015) Manufacturing Consumer Protection for 3-D Printed Products. *Arizona Law Review*, 57(2).

[132] Osborn, L.S. (2013) Regulating Three-Dimensional Printing: The Converging Worlds of Bits and Atoms. *San Diego Law Review*, 51(2).

[133] Pantella IV, J.J. (2017) Ready, Print, Fire! Regulating the 3D-Printing Revolution. *Journal of Law, Technology & the Internet*, 8(1).

[134] Pucino, D. (2020) *Ghost Guns: How Untraceable Firearms Threaten Public Safety*. [online] San Francisco, CA: Giffords Law Center. Available from: `https://giffords.org/lawcenter/report/ghost-guns-how-untraceable-firearms-threaten-public-safety/` [Accessed 12 June 2022].

[135] Reddy, P. (2014) The Legal Dimension of 3D Printing: Analyzing Secondary Liability in Additive Layer Manufacturing. *The Columbia Science and Technology Law Review*, 16(1).

[136] Richardson, M. (2016) Pre-Hacked: Open Design and the Democratisation of Product Development. *New Media and Society*, 18(4).

[137] Rustad, M.L. and Koenig, T.H. (2019) Towards a Global Data Privacy Standard. *Florida Law Review*, 71 (2).

[138] Sharpe, M. (2019) Products Liability in the Digital Age: Liability of Commercial Sellers of Cad Files for Injuries Committed With a 3D-Printed Gun. *American University Law Review*, 68(6).

[139] Staed, K.C. (2017) Open Source Download Mishaps and Product Liability: Who Is to Blame and What Are the Remedies? *Saint Louis University Public Law Review*, 36(1).

[140] Stern, A.D. (2017) Innovation Under Regulatory Uncertainty: Evidence from Medical Technology. *Journal of Public Economics*, 145(1).

[141] Stevenson, D. (2020) Smart Guns, the Law, and the Second Amendment. *Penn State Law Review,* 124(3).

[142] (2021) Going Gunless. *Brooklyn Law Review*, 86(1).

[143] Talbot, T. and Skaggs, A. (2020) Regulating 3D-Printed Guns Post-Heller: Why Two Steps are Better than One. *Journal of Law, Medicine and Ethics*, 48(4).

[144] Taylor, D.O. (2013) Patent Misjoinder. *New York University Law Review*, 88 (2).

[145] Thierer, A.D. (2014) *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom*. 1st ed. Arlington, Virginia: Mercatus Center at George Mason University.

[146] Thierer, A.D. and Marcus, A. (2016) Guns, Limbs, and Toys: What Future for 3D Printing? *Minnesota Journal of Law, Science & Technology*, 17(2).

[147] Traficonte, D. (2020) Collaboration in the Making: Innovation and the State in Advanced Manufacturing. *The Columbia Science and Technology Law Review*, 21(2).

[148] Tran, J.L. (2015) The Law and 3D Printing. *UIC John Marshall Journal of Information Technology Privacy Law*, 31(4).

[149] Tremble, C. (2018) Don't Bring a CAD File to a Gun Fight: A Technological Solution to the Legal and Practical Challenges of Enforcing ITAR on the Internet. *Fordham Law Review*, 87(1).

[150] Tu, K.V. and Meredith, M.W. (2015) Rethinking Virtual Currency Regulation in the Bitcoin Age. *Washington Law Review,* 90 (1).

[151] Tversky, A. and Kahneman, D. (1973) Availability: A Heuristic for Judging Frequency and Probability. *Cognitive Psychology*, 5(2).

[152] Walther, G. (2015) Printing Insecurity? The Security Implications of 3D-Printing of Weapons. *Science and Engineering Ethics*, 21(6).

[153] Watts, D. (2017) Should social science be more solution-oriented? *Nature Human Behaviour*, 1.

[154] Weinberger, V.P., Quiñinao, C. and Marquet, P.A. (2017) Innovation and the Growth of Human Population. *Philosophical Transactions of the Royal Society B: Biological Sciences*, 372(1735).

[155] Wilbanks, K. (2013) The Challenges of 3D Printing to the Repair-Reconstruction Doctrine in Patent Law. *George Mason Law Review*, 20(4).

[156] Wilke, C. (2019) *3-D Printed "Ghost Guns" Pose New Challenges for Crime-Scene Investigators.* [online] Washington, D.C.: Science News. Available from: `https://www.sciencenews.org/article/3d-printed-guns-plastic-ballistics-crime` [Accessed 29 April 2022].

[157] Willcocks, L., Venters, W. and Whitley, A. (2014) *Moving to the Cloud Corporation: How to Face the Challenges and Harness the Potential of Cloud Computing*. Hampshire: Palgrave Macmillan UK.

[158] Xu, D., Taylor, C.J. and Ren, Y. (2022) Wait-and-See or Whack-a-Mole: What Is the Best Way to Regulate Fintech in China? *Asian Journal of Law and Society*, First View.

[159] Yanisky-Ravid, S. and Kwan, K. S. (2017) 3D Printing the Road Ahead: The Digitization of Products When Public Safety Meets Intellectual Property Rights—A New Model. *Cardozo Law Review*, 38(3).

DOI 10.5817/MUJLT2023-2-2

HOW THE TWO CHILD ABUSE CASES HELPED TO SHAPE THE TEST OF ORIGINALITY OF PHOTOGRAPHIC WORKS*

by

MARIAN JANKOVIC †

The author intends to assess the approach to finding originality in photographic works in the courts of the United States of America and the approach developed by the Court of Justice of the European Union. The means through which such assessment is to be made are two cases, each decided in a respective jurisdiction; nonetheless they are connected via both factual and legal circumstances - both involving child abuse and a dispute regarding a copyright infringement in a photographic work. The article will thoroughly assess the legal circumstances of each case and describe the methods of identification of originality applied therein. Following the said assessment, an analysis of the possible merger of both methods will be conducted, with emphasis on the possible added value for the test of originality applied to photographic works within the copyright framework of the European Union. The author's intention is to conduct a comparison between both approaches to highlight their individual advantages and disadvantages, with a final assessment of their possible joint application in cases involving copyright infringement of photographic works within the copyright framework of the European Union.

KEY WORDS

Originality, Photographic Works, Photography, Originality Standard, Court of Justice of the European Union

* This paper was written within the project, and with the financial support of the Grant Agency of the Czech Republic, No. GA22-22517S ("Copyrighted Works and the Requirement of Sufficient Precision and Objectivity").

† marian.jankovic@law.muni.cz, doctoral student and expert, Institute of Law and Technology of Masaryk University Brno, Czech Republic.

1. INTRODUCTION

Initially, at the time of its invention in the early 19th century, photographers made no claims to be artists and declared photographs were obtained rather than made and emphasized the mechanical nature of the production process.[1] Nonetheless, shortly after its invention, copyright protection was extended to this new medium, despite copyright law not being completely comfortable with it - a state of affairs that persists to this day.[2] The issue at hand was the difficulty of understanding the distinction between the "original" and the "copy" of a photograph, a situation unlikely to occur within the realm of traditional works of art.[3] Nevertheless, with the gradual expansion of the technology, photography came to be considered an artistic activity, and its output – a photographic work - as potentially artistic and original.[4] Still, being a special subject matter, photographic works have continued to create problems for copyright law.[5] Even nowadays, widespread new photographic technologies contribute to numerous and significant challenges and implications within the said domain of law.[6]

As described above, the photography as a medium still raises ambiguities. Due to this, it also enjoys different treatment when it comes to its appropriation by copyright or related-right protection in various national legal frameworks. The link created by the factual circumstances of the two selected cases, as well as the shared medium at the centre of their interest – the photographic work - inspired the conducted assessments of the understanding of originality of photographic works in the two contrasting copyright frameworks: the one of the United States of America and the European Union.

Just two years apart, two cases concerning the analysis of photographic works were decided by courts in different jurisdictions. The first one could be considered ground-breaking, but nonetheless within the context of the court's continuous stance on the matter. The second one, for the purpose of this article, is in many ways a possible addendum to the first one. The former being the Painer case[7] decided by the Court of Justice of the European Union

1 Farley, C. H. (2004) The lingering Effects of Copyright's Response to the Invention of Photography, *University of Pittsburgh Law Review*, 65(3).

2 Bently, L. and Sherman B. (2014) *Intellectual Property Law*. 4th ed. Oxford University Press, p. 75.

3 Bowrey K. (1995) Copyright, Photography and Computer Works: The Fiction of an Original Expression. *UNSW Law Journal*, 18(2).

4 Bently L. and Sherman B. (2004) *Intellectual Property Law*. Oxford University Press, p. 91.

5 Laddie, H. (2011) *The Modern Law of Copyright and Designs*. LexisNexis, p. 253.

6 Katzenberger P. (1989) Neue Urheberrechtsprobleme der Photographie – Reproduktionsphotographie, Luftbild – und Satellitenaufnahmen. *GRUR*, 116.

7 Judgment of 1 December 2011, Painer, C-145/10, EU:C:2011:798.

("CJEU"). The latter being the Harney v. Sony Pictures Television, decided by the United States Court of Appeals For the First Circuit.[8] The analysed national test of originality applied in each selected case within its respective jurisdiction might, however, result in a different outcome if applied outside of it. The implications of this possibility will be elaborated on in the following text.

2. DEFINING ORIGINALITY - THE WAY TOWARDS EU ORIGINALITY STANDARD OF PHOTOGRAPHIC WORKS

As part of the first phase of the harmonisation process undertaken in the European Union ("EU") in the field of copyright, an originality standard deriving from the traditions of the continental EU was formed. However different the copyrightable subject matters might be, the basis of the originality standard is always the "author's own intellectual creation". This established originality standard for works was to be applied to every area of copyright harmonised through its corresponding Directive. All relevant Directives touching upon the issue of originality are consistent in their terminology: protection by copyright can be provided only to works that are the author's own intellectual creation.[9] Other criteria, such as aesthetics[10],

[8] *Harney v. Sony Pictures Television Inc.* (2013) 704 F.3d 173.

[9] For example, amongst such relevant Directives explicitly referring to the notion of "a*uthor's own intellectual creation*" are the Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the Legal Protection of Computer Programs. *Official Journal of the European Union* (L111/16), 23 April. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0024 [Accessed 20 August 2023], the Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases. *Official Journal of the European Union* (L 77/20) 11 March. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31996L0009 [Accessed 20 August 2023], the Directive 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and Amending Directive 96/9/EC and 2001/29/EC. *Official Journal of the European Union* (L130/92) 17 April. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0790&qid=1692731521579 [Accessed 20 August 2023] and the Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the Term of Protection of Copyright and Certain Related Rights. *Official Journal of the European Union* (L 372/12) 12 December. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0116 [Accessed 20 August 2023]

[10] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases. *Official Journal of the European Union* (L 77/20) 11 March. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31996L0009 [Accessed 20 August 2023] Recital 16

quality[11], merit[12] or purpose[13] are explicitly prohibited from being applied to determine work's eligibility for copyright protection. Given its direct relation to the subject of photographic works, only the provisions of the Term Directive[14] will be elaborated on in detail. Also, the development of the Directive itself, as well as the originality standard contained therein, will be given substantial attention.

The earliest codified version of the Term Directive, the Council Directive 93/98/EEC[15], included the first uniform standard of originality to be applied solely to photographic works in all Member States. The wording of its Recital 17 was later transposed in full into the Recital 16 of the currently effective Term Directive. Both the Recital 17 of the Council Directive 93/98/EEC and Recital 16, of the Term Directive read as follows:

> *"...a photographic work within the meaning of a Berne Convention is to be considered original if it is the author's own intellectual creation reflecting his personality, no other criteria such as merit or purpose being taken into account..."*[16]

To fully comprehend its meaning and implications in terms of applicability to photographic works, we shall proceed to deconstruct the quoted originality standard by providing individual definitions of its notions.

The first notion, "photographic work", represents an umbrella term used in both the Council Directive 93/98/EEC and the Term Directive for photographs and other photographs. The former is considered to be an original work worthy of copyright protection, while the latter is not. From a traditional (analogue) technical standpoint, a photographic work can be characterised as product of the art or a process of producing images by means of the chemical action of light upon a sensitive film on a basis of paper, metal,

---

[11] *Ibid*.

[12] Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the Term of Protection of Copyright and Certain Related Rights. *Official Journal of the European Union* (L 372/12) 12 December. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0116 [Accessed 20 August 2023] Recital 16

[13] *Ibid.*

[14] Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the Term of Protection of Copyright and Certain Related Rights. *Official Journal of the European Union* (L 372/12) 12 December. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0116 [Accessed 20 August 2023]

[15] Council Directive 93/98/EEC of 29 October 1993 Harmonizing the Term of Protection of Copyright and Certain Related Rights. *Official Journal of the European Communities* (L 290/9) 29 October. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31993L0098 [Accessed 20 August 2023]

[16] *Op. cit.*, Recital 17.

glass, etc.[17] However, this definition must be revised to reflect the current state of the art of photographic apparatus and equipment. In simplified wording, a photograph is an image created by light on any photosensitive surface, whether it be a photographic film or a digital electronic image sensor. However, the notion of a photographic work should always be understood within the meaning of the "Berne Convention", according to both versions of the Directive. Direct references to the Berne Convention only emphasize the importance of this international treaty. Photographic works have been in the scope of protection provided by the Berne Convention since its inception, although they were officially added to the wording of its Article 2 (1) only after the "Brussels Revision" in 1948.[18] All Member States of the European Union ("Member States") are also its contracting parties. The photographic work must also be "original", i.e. not secondary, derivative or imitative.[19] In this sense, the notion "originality" therefore requires a photographic work to be the first instance or initial source.

In general terms, the fourth selected notion of the "author" signifies the originator or a creator of something.[20] When photographic works are created, their author is called a photographer. In overly simplified terms, a photographer is thus a person who produces a photographic work using a photographic apparatus. Closely connected to the person of an author is the fifth notion of "own intellectual creation". The adjective "intellectual" is meant to stem from one's intellect. The notion itself can be defined as the faculty of reasoning and understanding objectively, especially with regard to abstract matters.[21] The condition highlights the photographer's intellectual input into the creation of a photographic work, emphasising the level of the originality standard for input in the form of abstract concepts into photographer's mind and their transformation into an objectively perceived medium: the photographic work. This input has to be the photographer's own and personal, as indicated in the formulation of the originality requirement. The resulting creation represents an act of creating or bringing something into existence - something that is created.[22]

[17] Gendreau Y. and Nordemann A. and Oesch R. (1999) *Copyright and Photographs, An International Survey (Informational Law Sries Set). Kluwer International*, p. 26.

[18] Ricketson, S. and Ginsburg J. C. (2006) *International Copyright and Neighbouring Rights*. Oxford University Press, p. 442.

[19] (2023) *Original* [online] The Merriam-Webster.com Dictionary. Available from: https://www.merriam-webster.com/dictionary/original [Accessed on 20 August 2023]

[20] (2023) *Author* [online] The Merriam-Webster.com Dictionary. Available from: https://www.merriam-webster.com/dictionary/author [Accessed on 20 August 2023]

[21] (2023) *Intellect* [online] Lexico Dictionaries. Available from https://en.oxforddictionaries.com/definition/intellect [Accessed on 20 August 2023]

[22] (2023) *Creation* [online] Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/creation [Accessed on 20 August 2023]

In addition to the above, a photographic work must reflect its creator's personality. The sixth notion of "personality" can be defined as a combination of characteristics or qualities that form an individual's distinctive character.[23] Apart from the requirement of own intellectual creation, the photographic work must be unique in the way it displays the photographer's personal distinctive touch. This part of the originality requirement ensures that the photographic work is distinguishable from the works of other photographers based on the uniqueness of each photographer's personality as an individual.

The seventh notion is "merit" and the final eight notion is "purpose". Merit can be characterised as a quality of being particularly good or worthy, especially so as to deserve praise or reward.[24] Purpose, which shall not be taken into account when assessing the originality of a photographic work, represents the reason for which something is done or created or for which something exists.[25] Evaluating the merit and purpose of a photographic work can lead to assessments based on the reputation or popularity standing of the photographic work, the genre it belongs to, or its author's profile in society or amongst other photographers. This can lead to biased court decisions. Merit and purpose are excluded to prevent subjective assessments of the originality of photographic works. Photographic works would, therefore, be assessed without prejudice related to the reason behind their creation or their creator as a person.

However, Recital 17 of the Council Directive 93/98/EEC, the predecessor of the Term Directive, also included the following wording:

> *"...whereas in order to achieve a sufficient harmonization of the term of protection of photographic works, in particular of those which, due to their artistic or professional character, are of importance within the internal market..."*[26]

To some degree, this is contradictory to further statements prohibiting the assessment of the merit and purpose of a photographic work, as described above. It is hard to understand the descriptors "artistic" or "professional" other than to indicate the context or aesthetic worth of the photographic

[23] (2023) *Personality* [online] Lexico Dictionaries, https://en.oxforddictionaries.com/definition/personality [Accessed on 20 August 2023]

[24] (2023) *Merit* [online] Lexico Dictionaries, https://en.oxforddictionaries.com/definition/merit [Accessed on 20 August 2023]

[25] (2023) *Purpose* [online] Lexico Dictionaries, https://en.oxforddictionaries.com/definition/purpose[Accessedon20August2023]

[26] Council Directive 93/98/EEC of 29 October 1993 Harmonizing the Term of Protection of Copyright and Certain Related Rights. *Official Journal of the European Communities* (L 290/9) 29 October. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31993L0098 [Accessed 20 August 2023] Recital 17.

work.[27] It has been suggested, that the decision whether or not there is a sufficient amount of creative input may, therefore, depend illogically on the type of context in which the photographic work was taken. [28] This contradiction was later amended by the Term Directive, in which the reworded diction of its now Recital 16 completely left out references to artistic or professional character as well as to importance within the internal market, thus declaring the requirement of total objectivity when assessing the originality, in accordance with the originality standard stated therein.

Having covered the development of the Recital 16 of the Term Directive, the focus will now be put on its Article 6, which has the following wording:

> *"Photographs which are original in the sense that they are the author's own intellectual creation shall be protected ... No other criteria shall be applied to determine their eligibility for protection... „*[29]

The cited wording of the Article 6 of the Term Directive sums up the general originality premise already outlined in its Recital 16. Additionally, the Article 6 is not only in line with Recital 16 but also with the originality provisions of other relevant aforementioned Directives. Therefore, the wording of Article 6 can be considered a completion and manifestation of efforts to establish a standard of originality for photographic works.

To conclude this section, the concept of the "author's own intellectual creation" was adopted as a compromise formula during the first phase of the harmonisation process between the relatively low originality threshold required as a precondition for copyright protection in the UK and the higher standards being used throughout the Member States.[30] Nonetheless, the true meaning of this definition and its applicability remained still rather unclear. Further clarification of the drafted originality standard was left to the CJEU through its case law during the second harmonisation phase.

---

[27] Tritton G. (2008) *Intellectual Property in Europe.* Sweet & Maxwell, p. 519.

[28] *Ibid.*

[29] Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the Term of Protection of Copyright and Certain Related Rights. *Official Journal of the European Union* (L 372/12) 12 December. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0116` [Accessed 20 August 2023] Article 6.

[30] Stamatoudi, I. and Torremans P. (2014) *EU Copyright Law: A Commentary.* Edward Elgar, p. 1103.

3. THE PAINER CASE[31]

The official guide to the Berne Convention leaves the question of originality to be answered by courts.[32] In light of this, copyright law of the EU must rely on further interpretation of the Article 6 of the Term Directive by the CJEU through its case law. Such additional interpretation of legislation by the CJEU represents the second phase of the harmonisation process.[33]

Further interpretation of legislation by the CJEU provides an additional significant source of information on the applicability of legal provisions and their approximation to factual situations. In the past, the CJEU was asked to decide a number of cases related to originality and copyright. The case law chosen to demonstrate the development of originality standard was selected with respect to its relevance in terms of the degree of assessment of originality of works and suitability of its analogous applicability to photographic works. Due to the limited space provided by this paper, only the most relevant decisions of the CJEU to the paper's topic are to be described in detail below. Amongst the cases intentionally left out for the aforementioned reasons are the following: The Infopaq case[34], The Bezpečnostní softwarová asociace case[35], The Murphy case[36], The Football Dataco case[37], The SAS case[38], The Levola case[39], The Cofemel[40] and The Brompton Bicycle case[41]. Fundamentally, the underlying principle of fulfilment of the originality requirement set by the CJEU is achieved when, through the choice, sequence and combination of elements, an author expresses their creativity in an original matter.[42]

In essence, the referring Austrian court in the Painer case sought clarification, as to whether the originality standard for photographic works, as defined in Article 6 of the Term Directive and according to which copyright protection vests in photographs that are their "author's own intellectual

[31] JUDGMENT OF 1 DECEMBER 2011, PAINER, C-145/10, EU:C:2011:798.

[32] (1978) *Guide to the Berne Convention for the Protection of Literary and Artistic Works* (Paris Act, 1971). Geneva: World Intellectual Property Organization, p. 18.

[33] Margoni, T. (2016) *The Harmonization of EU Copyright Law: The Originality Standard.* [online] SSRN. Available from: `https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2802327` [Accessed on 20 August 2023].

[34] Judgment of 16 July 2009, Infopaq International, C-5/08, EU:C2009:465.

[35] Judgment of 22 December 2010, Bezpečnostní softwarová asociace, C-393/09, EU:C:2010:816.

[36] Judgment of 4 October 2011, Football Association Premier League and Others, C-403/08, EU:C:2011:631.

[37] Judgment of 1 March 2012, Football Dataco and Others, C-604/10, EU:C:2012:115.

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

[39] Judgment of 13 November 2018, Levola Hengelo, C-310/17, EU:C:2018:899.

[40] Judgment of 12 September 2019, Cofemel, C-683/17, EU:2019:721.

[41] Judgment of 11 June 2020, Brompton Bicycle, C-833/18, EU:C:2020:461.

[42] Rosati, E. (2021) *Copyright in the Digital Single Market: Article-by-Article Commentary to the Provisions of Directive 2019/790*. Oxford University Press, p. 246.

creation", includes photographic works of portrait genre.[43] If the answer to this question were affirmative, the follow-up question of the referring Austrian court was whether the threshold for protection should be higher than for other categories of photographic works, because of the allegedly minor degree of creative freedom that such photographic works display.[44] In other words, the referring court wanted to clarify if the photographic works of portrait genre are afforded "weaker" copyright protection or no copyright protection at all due to their realistic nature and the minor formative freedom of a photographer connected with it.[45]

Apart from the main question brought before the CJEU concerning the issue of copyrightability of the photographic work or, essentially, the features of a work, two additional questions were also referred to the CJEU. The first concerned the jurisdiction to sue a defendant abroad (whether joint legal proceedings are to be precluded if the actions are brought against several defendants for copyright infringement, which are identical in substance, but based on differing national legal grounds).[46] The second concerned the public security exception (the need of official appeal for publication of a photographic work made by criminal justice bodies in the context of public security).[47] The CJEU answered both additional referred questions in the negative.[48] Therefore, a claimant can sue defendants coming from various Member States of the EU if the substance of the action brought against them, in this case, the copyright infringement, is identical. Also, criminal justice bodies are exempt from obtaining a prior consent of the rightsholder in cases where a publication of a photographic work is required for the matters of public security.

Before moving to the analysis of the merits of the case itself, a breakdown of the Advocate General Trstenjak's opinion[49] will be presented first to provide the broadest insight possible. Amongst other considerations, Trstenjak noted that the creator of a portrait photographic work enjoys a small degree of individual formative freedom, thus the copyright protection

[43] Rosati, E. (2013) *Originality in EU Copyright: Full Harmonization through Case Law*. Edward Elgar, p. 151.

[44] *Ibid*.

[45] Judgment of 1 December 2011, Painer, C-145/10, EU:C:2011:798, paragraph 43.

[46] Brophy, D. (2011) *All photos are created equal – the Painer case in the CJEU*, [online] The IPKat, Available from: `https://ipkitten.blogspot.com/2011/12/all-photos-are-creatd-equal-painer.html` [Accessed 20 August 2023]

[47] *Ibid*.

[48] Judgment of 1 December 2011, Painer, C-145/10, EU:C:2011:798, paragraph 84 and paragraph 116.

[49] Opinion of advocate general Trstenjak of 12 April 2011, Painer, C-145/10 Painer, EU:C:2011:239.

of such photographic work is accordingly narrow.[50] In order for such a photographic work to be original in similar cases, a photographer must utilise the available formative freedom available to them.[51] Trstenjak also noted the absence of several aspects, such as a certain degree of artistic quality or novelty, purpose of creation, expenditure and costs.[52] In respect to the aforementioned, the conclusion reached by Trstenjak stated that due to the not excessively high criteria governing copyright protection of photographic works in the Term Directive, photographic works of the portrait genre are afforded copyright protection if they are an original intellectual creation of a photographer, which requires them to have left their mark by using the available formative freedom.[53]

In her opinion, Advocate General Trstenjak also engaged in considerations regarding a question: whether a photo-fit created from the original portrait photographic work infringes the copyright bestowed on it.[54] Although not directly addressed by the CJEU, in her opinion, the Advocate General Trstenjak expressed that the publication of such a photo-fit constitutes reproduction within the meaning of the Article 2 (a) of the Digital Single Market Directive, only if in such a photo-fit the personal intellectual creation justifying the copyright protection is still embodied.[55]

In line with its previous case law on the subject, the CJEU held that in order for a photographic work to be eligible for copyright protection, it must be the author's own intellectual creation[56] provided that the author was able to express their creative abilities in its production by making free and creative choices.[57] The most recent referral to the stated requirement of author's own intellectual creation prior to the decision in the Painer case was made in the The Bezpečnostní softwarová asociace case.[58] Following the decision in the Painer case, the importance of free and creative choices was confirmed in the The Brompton Bicycle case[59]. Repeated application of both requirements by the CJEU highlights their significance for the EU copyright doctrine and also retrospectively confirms its correct application in the Painer case.

[50] *Op. cit.*, paragraph 108.
[51] *Op. cit.*, paragraph 122.
[52] *Op. cit.*, paragraph 123.
[53] *Op. cit.*, paragraph 215.
[54] Eechoud, M. (2014) *The Work of Authorship*. Amsterdam University Press, p. 166.
[55] Opinion of advocate general Trstenjak of 12 April 2011, Painer, C-145/10 Painer, EU:C:2011:239, paragraph 129.
[56] C Judgment of 1 December 2011, Painer, C-145/10, EU:C:2011:798, paragraph 87.
[57] *Op. cit.*, paragraph 89.
[58] Judgment of 22 December 2010, Bezpečnostní softwarová asociace, C-393/09, EU:C:2010:816, paragraph 46
[59] Judgment of 11 June 2020, Brompton Bicycle, C-833/18, EU:C:2020:461, paragraph 26.

These creative choices can be characterised as those which can be isolated by a method of asking whether two authors would have been likely to produce essentially the same work in comparable circumstances.[60] It is these creative choices that produce the protectable expression – an original work.[61] According to the CJEU, copyright-protected expression in the form of an original photographic work may manifest in several ways and at various points throughout its production:

> *"In the preparation phase, the photographer can choose the background, the subject's pose and the lighting. When taking a portrait photograph, he can choose the framing, the angle of view and the atmosphere created. Finally, when selecting the snapshot, the photographer may choose from a variety of developing techniques the one he wishes to adopt or, where appropriate, use computer software."*[62]

The remaining room for creative choices, however limited, is nonetheless still sufficient to produce an original photographic work.[63] Therefore, the creative choices, as described by the CJEU, can be conveniently executed by photographers in the context of production of a photographic work. However, the CJEU did not provide guidance on how much significance should be attributed to the creative part of the choices taken.[64] Accordingly, whether or not the input in the form of creative choices is sufficient for a finding of originality depends on the context of a photographic work.[65] Nonetheless, the final decision on the presence of the "personal touch" of a photographer in the photographic work is to be determined by national courts on case-to-case basis.[66]

The CJEU's emphasis on the presence of a "personal touch", the manifested outcome of the author's creative choices in a work, serves the purpose of clarifying the applicable sole criterion for originality – a combination of author's personality and their own intellectual creation.[67] Additionally, the concept of a personal touch itself serves as a convenient

---

[60] Gervais D. and Derclaye E. (2015) The Scope of computer program protection after SAS: are we closer to answers?, *European Intellectual Property Review*, 34(8), pp. 565-572.

[61] *Ibid.*

[62] Judgment of 1 December 2011, Painer, C-145/10, EU:C:2011:798, paragraph 91.

[63] Handig C. (2013) The "sweat of the brow" is not enough! – more than a blueprint of the European copyright term "work", *European Intellectual Property Review*, 35(6), pp. 334-340.

[64] *Ibid.*

[65] Stamatoudi, I. and Torremans P. (2014) *EU Copyright Law: A Commentary*. Edward Elgar, p. 278.

[66] Judgment of 1 December 2011, Painer, C-145/10, EU:C:2011:798, paragraph 94.

[67] Rosati, E. (2013) *Originality in EU Copyright: Full Harmonization through Case Law*. Edward Elgar, p. 153.

tool to differentiate between carefully composed photographic works and mere "point and shoot" snapshots.[68] The CJEU's decision in the Painer case has had an immense impact on the subject matter categorisation. The CJEU stressed the need to focus on the actual presence of originality in the photographic work, rather than on the photographic genre the assessed photographic work belongs to.[69]

Through its decision in the Painer case, the CJEU forces national courts to explore the potential of photography as a medium. National courts have to assess photographic works in detail and investigate their production process to discover aspects in which the originality of such works might reside. The CJEU has also affected photographers. They now have a manual of steps that, if taken and manifested in photographic works via the notion of a "personal touch", shall ensure originality – thus strengthening their position in terms of copyright protection. Last but not least, the CJEU has also influenced the social perception of certain traditionally non-original photographic genres as original; in other words no distinctions ought to be made between different types of photographs.[70] Lastly, the opinion of the CJEU is also consistent with the general legal principle of equal treatment that is to be applied in the European Union.[71]

To conclude this section, by application of CJEU's guidance, whether it be direct instructions or tests derived from its case law, the national courts must make a finding of originality in works that, at that time, appeared to be the sole requirement qualifying a work for copyright protection.[72] However, the notion of a copyright-protectable work now also presupposes the fulfilment of requirement of "sufficient precision and objectivity" of the expression, apart from originality.[73] Therefore, following the decisions in The Levola, The Cofemel and The Brompton Bicycle cases, any creative product, regardless of its nature, may be considered an object of copyright protection if

[68] Lee Y. H. (2012) Photographs and the standard of originality in Europe: Eva-Maria Painer v Standard VerlagsGmbH, Axel Springer AG, Süddeutsche Zeitung GmbH, SPIEGEL-Verlag Rudolf AUGSTEIN GmbH & Co KG and Verlag M. DuMont Schauberg Expdition der Kölnischen Zeitung GmbH & Co KG (C-145/10), *European Intellectual Property Review*, 34, pp. 290-293.

[69] *Op. cit.*, p. 154.

[70] Rosati, E. (2013) *Originality in EU Copyright: Full Harmonization through Case Law*. Edward Elgar, p. 155.

[71] Pila, J. and Torremans P. (2019) *European Intellectual Propety Law*. 2nd ed., Oxford University Press, p. 254.

[72] Rosati, E. (2013) *Originality in EU Copyright: Full Harmonization through Case Law*. Edward Elgar, p. 188.

[73] Rosati, E. (2019) *The Cofemel decision well beyond the "simple" issue of designs and copyright*. [online] The IPKat. Available from: `https://ipkitten.blogspot.com/2019/09/the-cofemel-decision-well-beyond-simple.html` [Accessed on 20 August 2023].

the cumulative requirements of originality and identification with sufficient precision and objectivity are fulfilled. [74] However, objectivity and precision are considered to be criteria known for their hard conceptualisation and application to artistic expressions. [75] Nevertheless, their fulfilment should not pose a problem for photographic works.

4. HARNEY V. SONY PICTURES TELEVISION

In 2013, the United States District Court for the district of Massachusetts ("the District Court") and later the United States Court of Appeals ("the Court of Appeals") both decided and reached the same conclusion in a case involving alleged copyright infringement in a photographic work. The case involved claimant Donald A. Harney, the photographer, and defendants Sony Pictures Television Inc. and A & E Television Networks, LLC, the alleged infringers of Mr. Harney's copyright (the "Harney v. Sony").[76] The main issue before the District court and later the Court of Appeals was whether the defendants infringed Mr. Harney's copyright in his photographic work by recreating certain parts of the image depicted in the said photographic work.[77] Although the merits of Harney v. Sony substantially differ from those of Painer case, the former case can be used to complete the missing pieces of originality establishment test applicable to photographic works hinted by the CJEU in the Painer case.

The question that stood before both courts was whether the claimant's photographic work, depicting a girl sitting on man's shoulders, a man who would later abduct his daughter and be exposed as a famous impostor, was infringed by recreation of its certain parts by defendants for their documentary about the case.[78] Even though the originality of a photographic work in the Harney v. Sony was not contested, a matter which was settled by the Court of Appeal's acknowledgement of the fact on several occasions, the Court of Appeals has provided a step-by-step test on how to identify and distinguish originality-forming elements in a photographic work, which might prove useful for additional enhancement of the originality test applied to photographic works in the copyright framework of the European Union.

---

[74] Sganga, C. (2018) *The Notion of "Work" in EU Copyright Law After Levola Hengelo: One Answer Given, Three Question Marks Ahead.* [online] SSRN. Available from: `https://ssrn.com/abstract=3323011` [Accessed on 20 August 2023].

[75] *Ibid.*

[76] *Harney v. Sony Pictures Television Inc.* (2013) 704 F.3d 173.

[77] Wallace, R. (2014) Framing the issue: avoiding substantial similarity finding in reproduced visual art. *Washington Journal of Law, Technology & Arts*, 10(2), p. 93.

[78] Kogan, T. S. (2017) *How photographs Infringe.* [online] SSRN, Available from: `https://doi.org./10.2139/ssrn.2963353` [Accessed on 20 August 2023].

Traditionally, the courts in the United States of America have been applying two types of tests (methods) when deciding substantial similarity cases, such as the one in question[79] since separating copyrightable and non-copyrightable elements might often prove difficult in reality.[80] First, the "ordinary observer test", which involves a two-step method requiring dissection of the elements of a photographic work in its first step followed by a response of the "ordinary observer" or the "laypeople" in its second.[81] The second employed test also involves two parts: "extrinsic", in which objective elements of a photographic work are analysed and "intrinsic", in which it is up to jury to decide whether, based on the first part, infringement occurred.[82] As a consequence, both approaches result in a thorough examination of individual elements of a photographic work.[83]

In Harney v. Sony, both courts chose to perform a "judicial surgery" to excise the central originality-forming elements.[84] In other words, the idea behind the applied excision is to make room for a clear distinction between originality-forming elements and those which occur naturally, or without the photographer's contribution in a particular photographic work. In respect to this, a process labelled by both courts in the respective case as an "ordinary dissection analysis"[85] was performed in order to separate all expressive elements present in the photographic work and assess the extent to which these were willingly affected by the photographer's choices.

The said "ordinary dissection analysis" was applied due to circumstances of the alleged infringement involving recreation of certain parts of the photographic work in question. Parts of both the original and the recreated photographic works were dissected, compared, and their origin assessed in order to establish their originality forming potential. In other words, to identify the expressive choices of a photographer in the photographic work that qualify as original, and therefore, copyright constituting, one must dissect the photographic work in question and inspect whatever elements are present and distinguish between their origin – the author of the said photographic work or someone else.

Similar to the Painer case, the Court of Appeals noted that elements of originality in a photographic work may include, amongst other, posing of the

[79] Meaning the *Harney v. Sony Pictures Television Inc.* (2013) 704 F.3d 173.

[80] Mazurek, C. (2017) Through the looking glass: photography and the Idea/Expression dichotomy. *New York Journal of Intellectual Property & Entertainment Law*, 6(2), p. 281.

[81] *Op. cit.*, p. 282

[82] *Ibid.*

[83] *Ibid.*

[84] Kogan, T. S. (2017) *How photographs Infringe.* [online] SSRN, Available from: `https://doi.org./10.2139/ssrn.2963353` [Accessed on 20 August 2023].

[85] Henceforth, the term will be used to refer to the excision of elements of a photographic work.

subjects, lighting, angle, selection of film and camera, achieving the desired expression of the subject, and any variants of combination of the listed. [86] Such elements, bearing the mark of the author's willingly performed choices in the course of the production process of a photographic work in the form of arrangement or creation of the depicted content, are, in fact, those of originality-forming type.

However, when the author is not involved in creating the subject or object depicted in the photographic work, such element is to be considered equivalent to an idea and, therefore, not protectable by copyright.[87] Such elements can be therefore viewed as mere facts not entitled to copyright protection.[88] The way an element constituting originality is formed via choices made by the author, thus transforming their idea into a protectable expressive work.[89] Nonetheless, the camera related choices - the protectable elements - made by the photographer of the allegedly infringed photographic work were not found to be substantially similar to the photographic work of the defendant by the court.[90] To draw from this conclusion, if the photographer does not create relationships between the elements in a photographic work, or the elements themselves, such photographic works might not be viewed as original.[91]

To conclude this section, even though as the originality of the photographic work in question was not contested, the applied excision provides a far deeper insight into the very production process of a photographic work. When originality of any photographic work would, in fact, be contested, the said analysis can be employed to "dissect" the photographic work, identify, separate and assess its elements in order to reach a conclusion regarding its originality and, with it, connected copyrightability. The final take from the case is that it is permissible, in other words, not copyright-infringing, to imitate those elements of a photographic work that were found to be non-copyrightable by the aforementioned excision method.[92]

---

[86] *Harney v. Sony Pictures Television Inc.* (2013) 704 F.3d 173, p. 13.
[87] *Ibid.*
[88] *Ibid.*
[89] *Op. cit.*, p. 14.
[90] Kogan, T. S. (2017) *How photographs Infringe*. [online] SSRN, Available from: `https://doi.org./10.2139/ssrn.2963353` [Accessed on 20 August 2023].
[91] Woo Jiang Ming, S. (2020) The basis for originality in photographs, *Singapore Academy of Law Journal*, 32(2), pp. 1101-1152.
[92] Wallace, R. (2014) Framing the issue: avoiding substantial similarity finding in reproduced visual art. *Washington Journal of Law, Technology & Arts*, 10(2), p. 94.

5. THE ENHANCED TEST OF ORIGINALITY OF PHOTOGRAPHIC WORKS?

Following the decision of the CJEU in the Painer case, the originality of a photographic work was also touched upon, amongst other considerations, only once - in the Renckhoff case.[93] The photographic work at the heart of this case, taken in the Spanish city of Cordoba, by a professional German photographer, depicts a cityscape. In his opinion, Advocate General Campos Sánchez-Bordona expressed doubts whether the photographic work in question, a simple shot, satisfies the requirements for originality laid down in the Painer case.[94] In accordance with this decision, it may be assumed that the free and creative choices may also be expressed in a landscape or cityscape photograph.[95] However, the doubt cast on the originality of this photographic work was unfortunately not further elaborated on by the CJEU, apart from a general preliminary point reference to originality of photographic works and the Painer case.[96] Nonetheless, the string of case law of the CJEU on the subject of originality is united by one common notion – the "author's own intellectual creation". The notion itself, first adopted as a standard for originality of photographic works in the Painer case, is to be understood as consisting of "creative freedom",[97] "personal touch"[98] and "free and creative choices".[99]

The CJEU in the Painer case does not explicitly mention elements but rather focuses on the three phases of a production of a photographic work and the actions a photographer can make within the defined phases. This is in opposition to the approach in the United States of America, where the choice of various elements and the effects these produce, prevails over the choices the photographer has made during the course of the production process, thereby making the photographic work original.[100] The approach of the CJEU might seem rather superficial in situations where a more thorough inspection

[93] Judgment of 7 August 2018, Renckhoff, C-161/17, EU:C:2018:634.

[94] Opinion of advocate general Campos Sánchez-Bordona of 25 April 2018, C-161/17, EU:C:2018:279, paragraph 54.

[95] Synodinou, T. (2019) *The Renckhoff Judgement: The CJEU Swivels the Faces of the Copyright Rubik's Cube (Part I)*, [online] Kluwer Copyright Blog, Available from: `http://copyrightblog.kluweriplaw.com/2018/09/27/renckhoff-judgement-cjeu-swivels-faces-copyright-rubiks-cuber-part` [Accessed on 20 August 2023]

[96] Judgment of 7 August 2018, Renckhoff, C-161/17, EU:C:2018:634, paragraph 14.

[97] Judgment of 4 October 2011, Football Association Premier League and Others, C-403/08, EU:C:2011:631.

[98] Judgment of 1 December 2011, Painer, C-145/10, EU:C:2011:798.

[99] Judgment of 1 March 2012, Football Dataco and Others, C-604/10, EU:C:2012:115.

[100] Woo Jiang Ming, S. (2020) The basis for originality in photographs, *Singapore Academy of Law Journal*, 32(2), pp. 1101-1152.

of an allegedly infringed photographic work is required. Although it belongs to a different jurisdiction, the reasoning of the Court of Appeals in the Harney v. Sony regarding the dissection of a photographic work and extraction of its elements hypothetically adds an additional universal and deeper layer of actions to the test of originality applicable to photographic works, which a court can apply in its decision-making within the copyright framework of the EU.

However, the application of the "ordinary dissection analysis" might raise questions in connection with the Painer case decision, if it were applied by the CJEU. The said question involves the omitted analysis by the CJEU of the original photographic work depicting the missing girl. The sued magazines have only used a cut-out of the original photographic work, depicting the child's face and a small part of the background. Applying the ordinary dissection analysis or considering the remark of the Advocate General Trstenjak related to the photo-fit's originality in her opinion, would maybe assess the depicted elements as non-original. In light of this, the said parts would, in fact, be treated differently than the original "whole" photographic work, since the parts would not be able to share the originality of the original copyright-protected photographic work.[101] Therefore, depending on the photofit's size and elements it would display, the final decision on originality might be different if the said excision were employed.

6. CONCLUSION

To conclude, the decision in the Harney v. Sony provides theoretical guidance in terms of argumentation regarding the copyrightability of any photographic work. According to it, if one can argue only non-copyrightable elements of a photographic work were copied or reproduced, a copyright infringement may not be even considered.[102] Combining parts of both tests, the one applied by the courts in the United States of America and the one of the CJEU, it seems to introduce a more complex tool for identifying production phases of a photographic work and also the manifested elements - the results of the said phases in better detail. Moreover, such joint approach, incorporating both originality assessment methods, might prove to be more thorough. If the factual circumstances of the case would require it, a deeper insight into the production process of a photographic work and, through it, the identification of individual originality-forming elements and creative steps of the photographer would be enabled with greater precision. This could

[101] Judgment of 16 July 2009, Infopaq International, C-5/08, EU:C2009:465, paragraph 38.

[102] Wallace, R. (2014) Framing the issue: avoiding substantial similarity finding in reproduced visual art. *Washington Journal of Law, Technology & Arts*, 10(2), p. 95.

prove to be beneficial to photographers in a role of claimants, strengthening their position in terms of evidence and arguments.

However, despite the apparent benefits mentioned above, the thorough excision of elements of a photographic work, even a deconstructionist analysis[103], applied by the courts in the United States of America does not seem to be compatible with the approach applied by the CJEU. It appears that the CJEU has recognised the potential issues that such an approach might bring in copyright infringement cases. Despite Advocate General Trstenjak's aforementioned considerations on the matter in her opinion, the CJEU has decided to reject such an approach and instead, continue to apply its previous jurisprudence on the matter. The CJEU maintains the doctrine of "parts sharing the originality of the whole work",[104] which was firstly introduced in the Infopaq case.

Consequently, however beneficial the approach in the United States of America might be in terms of theoretical analysis of the components of a photographic work, it would prove to be quite the contrary in the application practice within the copyright framework of the EU. Therefore, the omitted deeper dive into the identification process of elements in a photographic work by the CJEU might seem to have the purpose of enabling the provision of copyright protection to a larger number of photographic works. In other words, by the CJEU's decision of not applying the approach from the United States of America, the copyright protection is extended to more photographic works and the risks of its refusal on the basis of their dissection into separate parts is to a large extent mitigated. Simply put, the authors in the role of photographers would not benefit in practice from the merger of both approaches in the current copyright doctrine of the EU. As a result, photographic works or their parts are still looked upon as a whole in the eyes of the copyright framework of the EU and not dissected into individual elements when their originality is challenged.

LIST OF REFERENCES

[1] *Author* [online] The Merriam-Webster.com Dictionary. Available from: https://www.merriam-webster.com/dictionary/author [Accessed on 20 August 2023]

[2] Bently L. and Sherman B. (2004) *Intellectual Property Law*. Oxford University Press.

[103] Mazurek, C. (2017) Through the looking glass: photography and the Idea/Expression dichotomy, *New York Journal of Intellectual Property & Entertainment Law*, 6(2), p. 282.

[104] Judgment of 16 July 2009, Infopaq International, C-5/08, EU:C2009:465, paragraph 38.

[3] Bently, L. and Sherman B. (2014) *Intellectual Property Law*. 4th ed. Oxford University Press.

[4] Bowrey K. (1995) Copyright, Photography and Computer Works: The Fiction of an Original Expression. *UNSW Law Journal*, 18.

[5] Brophy, D. (2011) *All photos are created equal – the Painer case in the CJEU*, [online] The IPKat, Available from: https://ipkitten.blogspot.com/2011/12/all-photos-are-creatd-equal-painer.html [Accessed 20 August 2023]

[6] Council Directive 93/98/EEC of 29 October 1993 Harmonizing the Term of Protection of Copyright and Certain Related Rights. *Official Journal of the European Communities* (L 290/9) 29 October. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31993L0098 [Accessed 20 August 2023]

[7] Council Directive 93/98/EEC of 29 October 1993 Harmonizing the Term of Protection of Copyright and Certain Related Rights. *Official Journal of the European Communities* (L 290/9) 29 October. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31993L0098 [Accessed 20 August 2023]

[8] *Creation* [online] Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/creation [Accessed on 20 August 2023]

[9] Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the Term of Protection of Copyright and Certain Related Rights. *Official Journal of the European Union* (L 372/12) 12 December. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0116 [Accessed 20 August 2023]

[10] Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the Term of Protection of Copyright and Certain Related Rights. *Official Journal of the European Union* (L 372/12) 12 December. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0116 [Accessed 20 August 2023]

[11] Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the Term of Protection of Copyright and Certain Related Rights. *Official Journal of the European Union* (L 372/12) 12 December. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0116 [Accessed 20 August 2023]

[12] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases. *Official Journal of the European Union* (L 77/20) 11 March. Available from: https://eur-lex.europa.

eu/legal-content/EN/TXT/PDF/?uri=CELEX:31996L0009 [Accessed 20 August 2023]

[13] Eechoud, M. (2014) *The Work of Authorship*. Amsterdam University Press.

[14] Farley, C. H. (2004) The lingering Effects of Copyright's Response to the Invention of Photography, *University of Pittsburgh Law Review*, 65.

[15] Gendreau Y. and Nordemann A. and Oesch R. (1999) *Copyright and Photographs, An International Survey (Informational Law Sries Set)*. Kluwer International.

[16] Gervais D. and Derclaye E. (2015) The Scope of computer program protection after SAS: are we closer to answers?, *European Intellectual Property Review*, 34.

[17] *Guide to the Berne Convention for the Protection of Literary and Artistic Works (Paris Act, 1971).* Geneva: World Intellectual Property Organization.

[18] Handig C. (2013) The "sweat of the brow" is not enough! – more than a blueprint of the European copyright term "work", *European Intellectual Property Review*, 35.

[19] *Harney v. Sony Pictures Television Inc.* (2013) 704 F.3d 173.

[20] *Intellect* [online] Lexico Dictionaries. Available from https://en.oxforddictionaries.com/definition/intellect [Accessed on 20 August 2023]

[21] Judgment of 1 December 2011, Painer, C-145/10, EU:C:2011:798.

[22] Judgment of 1 March 2012, Football Dataco and Others, C-604/10, EU:C:2012:115.

[23] Judgment of 11 June 2020, Brompton Bicycle, C-833/18, EU:C:2020:461.

[24] Judgment of 12 September 2019, Cofemel, C-683/17, EU:2019:721.

[25] Judgment of 13 November 2018, Levola Hengelo, C-310/17, EU:C:2018:899.

[26] Judgment of 16 July 2009, Infopaq International, C-5/08, EU:C2009:465.

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

[28] Judgment of 22 December 2010, Bezpečnostní softwarová asociace, C-393/09, EU:C:2010:816.

[29] Judgment of 4 October 2011, Football Association Premier League and Others, C-403/08, EU:C:2011:631.

[30] Judgment of 7 August 2018, Renckhoff, C-161/17, EU:C:2018:634.

[31] Katzenberger P. (1989) Neue Urheberrechtsprobleme der Photographie – Reproduktionsphotographie, Luftbild – und Satellitenaufnahmen. GRUR, 116.

[32] Kogan, T. S. (2017) *How photographs Infringe*. [online] SSRN, Available from: https://doi.org./10.2139/ssrn.2963353 [Accessed on 20 August 2023].

[33] Laddie, H. (2011) *The Modern Law of Copyright and Designs*. LexisNexis, p. 253.

[34] Lee Y. H. (2012) Photographs and the standard of originality in Europe: Eva-Maria Painer v Standard VerlagsGmbH, Axel Springer AG, Süddeutsche Zeitung GmbH, SPIEGEL-Verlag Rudolf AUGSTEIN GmbH Co KG and Verlag M. DuMont Schauberg Expdition der Kölnischen Zeitung GmbH Co KG (C-145/10), *European Intellectual Property Review*, 34.

[35] Margoni, T. (2016) *The Harmonization of EU Copyright Law: The Originality Standard.* [online] SSRN. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2802327[Accessed on 20 August 2023].

[36] Mazurek, C. (2017) Through the looking glass: photography and the Idea/Expression dichotomy. *New York Journal of Intellectual Property Entertainment Law*, 6.

[37] Mazurek, C. (2017) Through the looking glass: photography and the Idea/Expression dichotomy, *New York Journal of Intellectual Property Entertainment Law*, 6.

[38] *Merit* [online] Lexico Dictionaries, https://en.oxforddictionaries.com/definition/merit [Accessed on 20 August 2023]

[39] Opinion of advocate general Campos Sánchez-Bordona of 25 April 2018, C-161/17, EU:C:2018:279, paragraph 54.

[40] Opinion of advocate general Trstenjak of 12 April 2011, Painer, C-145/10, EU:C:2011:239.

[41] *Original* [online] The Merriam-Webster.com Dictionary. Available from: https://www.merriam-webster.com/dictionary/original [Accessed on 20 August 2023]

[42] *Personality* [online] Lexico Dictionaries, https://en.oxforddictionaries.com/definition/personality [Accessed on 20 August 2023]

[43] Pila, J. and Torremans P. (2019) *European Intellectual Propety Law*. 2nd ed., Oxford University Press.

[44] *Purpose* [online] Lexico Dictionaries, https://en.oxforddictionaries.com/definition/purpose [Accessed on 20 August 2023]

[45] Ricketson, S. and Ginsburg J. C. (2006) *International Copyright and Neighbouring Rights*. Oxford University Press.

[46] Rosati, E. (2013) *Originality in EU Copyright: Full Harmonization through Case Law*. Edward Elgar.

[47] Rosati, E. (2019) *The Cofemel decision well beyond the "simple" issue of designs and copyright*. [online] The IPKat. Available from: https://ipkitten.blogspot.com/2019/09/the-cofemel-decision-well-beyond-simple.html [Accessed on 20 August 2023].

[48] Rosati, E. (2021) *Copyright in the Digital Single Market: Article-by-Article Commentary to the Provisions of Directive 2019/790.* Oxford University Press.

[49] Sganga, C. (2018) *The Notion of "Work" in EU Copyright Law After Levola Hengelo: One Answer Given, Three Question Marks Ahead.* [online] SSRN. Available from: https://ssrn.com/abstract=3323011 [Accessed on 20 August 2023].

[50] Stamatoudi, I. and Torremans P. (2014) *EU Copyright Law: A Commentary.* Edward Elgar.

[51] Synodinou, T. (2019) *The Renckhoff Judgement: The CJEU Swivels the Faces of the Copyright Rubik's Cube* (Part I), [online] Kluwer Copyright Blog, Available from: http://copyrightblog.kluweriplaw.com/2018/09/27/renckhoff-judgement-cjeu-swivels-faces-copyright-rubiks-cuber-part [Accessed on 20 August 2023]

[52] Tritton G. (2008) *Intellectual Property in Europe*. Sweet & Maxwell.

[53] Wallace, R. (2014) Framing the issue: avoiding substantial similarity finding in reproduced visual art. *Washington Journal of Law, Technology & Arts*, 10.

[54] Woo Jiang Ming, S. (2020) The basis for originality in photographs, *Singapore Academy of Law Journal*, 32.

DOI 10.5817/MUJLT2023-2-3

ADDRESSING EVOLVING DIGITAL PIRACY THROUGH CONTRIBUTORY LIABILITY FOR COPYRIGHT INFRINGEMENT: THE MOBDRO CASE STUDY

by

MINDAUGAS KIŠKIS *

Digital piracy, i.e., large-scale commercial copyright infringement online, is a constantly evolving phenomenon. Following the enactment and expansion of online intermediary liability rules, professional pirates have shifted away from easily blockable websites and services. Streaming piracy on dedicated platforms, monetised through embedded services, has become the prevalent model in Europe, as is well illustrated by the Mobdro case study analysed in this article. These dedicated platforms are supported by embedded service providers who, as they are not online intermediaries, can avoid the online intermediary liability regime. One potential solution to this issue could be the application of contributory copyright infringement rules, which are well-established in US copyright law but absent in EU law, to all parties that contribute to digital piracy. The CJEU has opened expressly this path in the recent C-682/18 YouTube and C-683/18 Cyando cases. Based on the CJEU's initiative and the existing precedent of harmonising intellectual property tort rules within EU law, further contributory liability rules could be modelled after US rules by updating the Enforcement Directive 2004/48/EC. Addressing this gap in EU copyright law is crucial for enhancing the effectiveness of digital copyright enforcement against evolving digital piracy.

KEY WORDS

Copyright, Contributory liability, Piracy, Streaming, Embedded SDK

* mkiskis@mruni.eu, Professor, Faculty of Public Governance and Business & MRU Law School, Mykolas Romeris University, Lithuania

1. INTRODUCTION

General legal liability principles of criminal and tort law in modern legal systems suggest that liability for unlawful action causing damage shall apply not only to direct infringers, but also to parties who contribute to the infringement. There are no material reasons why substantive copyright law should apply different liability principles, but for various historical reasons the liability rules for copyright infringements vary significantly in different jurisdictions. The US substantive copyright law has developed a thorough concept of secondary civil liability for copyright infringements, the two main branches of which are contributory liability and vicarious liability; however, substantive copyright laws in Europe are rather shy in regulating indirect copyright infringement and legal liability for it. European scholars have also not adopted a uniform concept or nomenclature for secondary liability for copyright infringement, with some resorting to overly narrow interpretations[1] which may exclude contributors from secondary liability for copyright infringement. This is representative of the overwhelming focus of European jurisprudence on the liability of online intermediaries, which may prove increasingly insufficient in view of recent directions in the evolution of digital piracy, i.e., large-scale commercial copyright infringement online.

In one of the most famous copyright enforcement cases in the EU – the Pirate Bay criminal cases in Sweden – the operators of the Pirate Bay website were all convicted not for direct or primary copyright infringement, but rather for aiding and abetting copyright infringement performed by others.[2] The crime of the Pirate Bay operators was contributing to the copyright infringement committed by the users of the Pirate Bay. The Pirate Bay perpetrators were found liable for the civil damages caused to

[1] See, e.g., the definition of "secondary liability" in Husovec, M. (2013) Injunctions against Innocent Third Parties: The case of Website Blocking. *JIPITEC*, 4, p. 118, para. 11, note 4 – the statement that "Secondary liability could be further divided into fault-based secondary liability that requires the breach of a certain duty of care, and no-fault-based secondary liability that triggers liability regard-less of such a breach" excludes contributory liability as it is understood in US common law, i.e., fault-based secondary liability that requires inducing or material contribution to the activity of the direct infringer. "Fault-based secondary liability that requires the breach of a certain duty of care" according to US common law would imply vicarious liability only. For comparison, on the US common law doctrine of "secondary liability for copyright infringement" see Folsom, T. C. (2009) Toward Non-Neutral Principles of Private Law: Designing Secondary Liability Rules for New Technological Uses. *Akron Intellectual Property Journal*, 3, pp. 45, 52, and Mehra, S. K. (2011) Keep America Exceptional! Against Adopting Japanese and European-Style Criminalization of Contributory Copyright Infringement. *Vanderbilt Journal of Entertainment and Technology Law*, 13 (4), which clearly differentiate "contributory liability" and "vicarious liability", which are separate from faultless secondary liability.

[2] Kravets, D. (2009) *English Transcript of Pirate Bay Guilty Verdicts Released*. Wired. Available from: `https://www.wired.com/2009/04/english-transcript-of-pirate-bay-guilty-verdicts-released/`

the rightsholders; however, these tort claims were resolved as part of the criminal cases, which lasted for almost a decade, and not through separate civil action procedures, which may have been simpler and faster. More than a decade later, civil action against a perpetrator who did not violate copyright themselves and who is not an online intermediary remains a murky topic in European copyright law.

On the one hand, the Electronic Commerce Directive 2000/31/EC, the InfoSoc Directive 2001/29/EC, and the Enforcement Directive 2004/48/EC introduced special rules on the secondary liability of and injunctions against internet intermediaries,[3] which were inspired by the substantively similar earlier rules in US copyright law (the 1998 Digital Millennium Copyright Act) and the TRIPS agreement. On the other hand, secondary liability rules remain generally absent with respect to parties who are not explicit online intermediaries. This gap in the liability and infringement rules of European copyright law is most apparent in comparison to US copyright law. To a certain extent, this gap already manifested in European copyright liability case law, where the attempt was made to address secondary liability for copyright infringement through the stretched interpretation of the right to communicate to the public, or by imaginative applications of obscure national tort law doctrines, which have only indirect relationships to, and no statutory basis in, copyright (e.g., Störerhaftung in Germany).

European jurisprudence on the issue of secondary liability for copyright infringement predominantly focusses on issues of online intermediary liability and injunctions against intermediaries.[4] A substantial body of work addresses trademark-specific issues: mainly injunctions against platforms for offering counterfeit goods, which has been the subject matter of multiple cases at the Court of Justice of the European Union (CJEU).[5] The research acknowledges that secondary liability actions are most prevalent in cases involving digital content, which also includes copyrighted material.[6] It is also notable that existing comparative analyses of intermediary liability issues in the EU,[7] including rare work that focusses on European intermediary

[3] Husovec, M. (2018) *Injunctions against intermediaries in the European Union: Accountable but not liable?* Cambridge: Cambridge University Press, pp. 42–46.

[4] Frosio, G. (ed.) (2020) *Oxford Handbook of Online Intermediary Liability*. Oxford: OUP.

[5] Dinwoodie, G., Dreyfuss, R., and Kur, A. (2009) The Law Applicable to Secondary Liability in Intellectual Property Cases. *New York University Journal of International Law and Politics*, 2, pp. 201–235. Available from: `https://nyujilp.org/wp-content/uploads/2013/02/42.1-Dinwoodie-Dreyfuss-Kur.pdf`

[6] *Op. cit.*, p. 204.

[7] Leistner, M. (2014) Structural aspects of secondary (provider) liability in Europe. *Journal of Intellectual Property Law & Practice*, 9 (1), pp. 75–90, Available from: `https://doi.org/`

liability in copyright,[8] are limited only to German and French law, which are not representative of the whole of the EU. All aforementioned research recognises that secondary liability is important for the effective enforcement of intellectual property online, and urges the further harmonisation of rules at the EU level.[9] This is crucial in the context of digital piracy, which is an inherently cross-border phenomenon and requires supranational legal rules to address it. Digital piracy is also a very dynamic and rapidly evolving phenomenon, which is shall studied by looking at very recent examples, such as the Mobdro case study presented in this article. This case study illustrates how piracy platforms are avoiding online intermediary liability and monetising their activities through the embedded services model, thus making it difficult for rightsholders to pursue damages. Embedded service providers themselves are not online intermediaries – at least not in the traditional sense – and therefore their activities cannot be addressed through online intermediary liability rules, allowing them to slip through the legal gaps of copyright infringement liability rules, at least in Europe.

There are no existing EU legal research articles specifically addressing the secondary liability of non-intermediary parties that are instrumental and material contributors to copyright infringement. To address the particularities of this aspect, in the authors' opinion it is preferable to use the term *contributory liability* for copyright infringement, rather than the general term *secondary liability*.[10] Although secondary liability in the context of digital piracy is little-explored in European legal research, in the US it has been one of the main topics of secondary liability for copyright infringement,[11] particularly focusing on contributory liability. Some US scholars specifically highlight the advantages of the civil law enforcement

10.1093/jiplp/jpt213, and Husovec, M. (2018) *Injunctions against intermediaries in the European Union: Accountable but not liable?* Cambridge: Cambridge University Press.

8 Angelopoulos, C. (2016) *European Intermediary Liability in Copyright: A Tort-Based Analysis*. Wolters Kluwer.

9 Husovec, M. (2018) *Injunctions against intermediaries in the European Union: Accountable but not liable?* Cambridge: Cambridge University Press, pp. 42–46., Dinwoodie, G., Dreyfuss, R., and Kur, A. (2009) The Law Applicable to Secondary Liability in Intellectual Property Cases. *New York University Journal of International Law and Politics*, 2, pp. 201–235. Available from: https://nyujilp.org/wp-content/uploads/2013/02/42.1-Dinwoodie-Dreyfuss-Kur.pdf, Leistner, M. (2014) Structural aspects of secondary (provider) liability in Europe. *Journal of Intellectual Property Law & Practice*, 9 (1), pp. 75–90, Available from: https://doi.org/10.1093/jiplp/jpt213, Angelopoulos, C. (2016) *European Intermediary Liability in Copyright: A Tort-Based Analysis*. Wolters Kluwer.

10 Differences between the two are discussed in note 1. Also, note that the term of contribution to infringement ("*contributes [...] in breach of copyright*") was recently introduced by the CJEU in judgement in joined cases C-682/18 and C-683/18, par. 102, which is analysed below in the article.

11 Lemley, M. A., and Reese, R. A. (2004) Reducing Digital Copyright Infringement Without Restricting Innovation. *Stanford Law Review*, 56 (6), pp. 1345–1434.

of contributory liability for copyright infringement vis-à-vis contributory liability under criminal law, and argue that criminal prosecution could have a chilling effect on innovation in technologies with "lawful promise".[12] Nevertheless, even in the US secondary liability for copyright infringement has not been investigated in the context of novel digital piracy models.

The purpose of this article is to fill the identified research gap: the lack of proper secondary liability for copyright infringement rules with respect to parties who are not online intermediaries. Through a specific case study, it will be demonstrated how this may be driving online digital piracy in Europe.

The first section of the article briefly comparatively analyses the law relevant to contributory liability for copyright infringement in the EU and the US. Note that the analysis in this article is limited only to copyright law. The second section discusses the changes in digital piracy "business models" over the last two decades and highlights the embedded services model as the current default. The third section examines the Mobdro case study as a recent example of modern dedicated piracy platforms, and analyses it in the context of copyright infringement rules. In the conclusions, the authors argue in favour of proper statutory rules on contributory infringement in the EU, which are crucial for enhancing the effectiveness of digital copyright enforcement against evolving digital pirates.

2. THE LEGAL CONTEXT OF CONTRIBUTORY COPYRIGHT INFRINGEMENT

From a legal perspective, digital piracy is the act of illegal public performance, distribution and reproduction of copyrighted works on the internet, which gives rise to the legal liability of the parties involved. Liability shall generally apply not only to the direct infringer, but also to parties who contribute to the infringement and indirectly infringe copyright, yet European statutory copyright law contains few rules dealing with contributory copyright infringement and collaborators' liability for copyright infringement.

In US copyright law, rightsholders enjoy a century-old doctrine of contributory copyright infringement, a form of secondary liability that makes one party liable for the harm caused by another. According to this case law doctrine, US copyright law thus allows rightsholders to seek relief from all parties who have materially contributed to the copyright infringement. Notably, secondary liability for copyright infringement is a general and

[12] Mehra, S. K. (2011) Keep America Exceptional! Against Adopting Japanese and European-Style Criminalization of Contributory Copyright Infringement. *Vanderbilt Journal of Entertainment and Technology Law*, 13 (4).

autonomous doctrine of US federal copyright law, which is independent from state tort law doctrines, such as the doctrine of tortious interference, which is an autonomous doctrine of tort law in many US states. For context, it is important to bear in mind that copyright law is an exclusive matter of federal jurisdiction in the US, while tort law, with the exception of specific torts (e.g., environmental damage), is a matter of state law. Therefore, copyright law and tort law doctrines generally do not intersect.

EU substantive copyright law is quasi-federal in that it has been very significantly harmonised through the EU Acquis and overrides pertinent national law. Nevertheless, there is no general concept or doctrine of secondary liability for copyright infringement in EU copyright law. One of the main sources of EU substantive copyright law – InfoSoc Directive 2001/29/EC – expressly discusses inducing, enabling, facilitating or concealing an infringement only in the very specific context of rights management (DRM) information (Art. 7(1)), and separately provides for the possibility of intermediary liability (Art. 8(2)) and injunctions against intermediaries (Art. 8(3)). Liability rules for online intermediaries were first introduced in E-Commerce Directive 2000/31/EC (Art. 12-15), and originally meant internet service providers, but gradually expanded in their interpretation to include all online intermediaries, such as online service providers and online platforms that host or convey third party data. Injunction rules are further elaborated with respect to all forms of intellectual property in the Enforcement Directive 2004/48/EC (Art. 9(1) and Art. 11). Note that none of these rules apply to parties who cannot be considered online intermediaries.

Directive 2001/29/EC does not provide for a general definition of copyright infringement, and does not expressly mention secondary or contributory liability. Theoretically, one could argue that this does not preclude secondary liability for copyright infringement as it allows for national rules with higher protection standards (i.e., stricter), but this is then entirely left out for the national law of the Member States. The statutory copyright laws of many EU Member States (which at least include Lithuania, Latvia, Estonia, Poland, Finland, and Germany) follow the same pattern – there are no express statutory provisions on contributory copyright liability, save for specific and limited rules pertaining to the DRM, intermediary liability, and injunctions against online intermediaries based on the national implementation of the aforementioned EU Directives. Theoretically, contributory liability for copyright infringement may be invoked in national law on the basis of various doctrines of national tort law, but this puts a heavy burden on the shoulders of the judiciary and

requires judicial bravery, creativity and activism, which is unlikely in courts of lower instance and is not a very attractive proposition for both judges and rightsholders seeking quick and efficient copyright infringement relief. Unsurprisingly, at least in some countries (for example, Lithuania), there is not a single copyright liability case where secondary liability of a non-online intermediary would be attempted. In other countries (Germany), the lack of statutory contributory infringement rules in national copyright law is somewhat compensated for in the higher instance courts by applying earlier precedents from trademark and patent law cases based on the historical tort law doctrine of Störerhaftung,[13] which is roughly equivalent to the abovementioned US state common law doctrine of tortious interference, but is historically applied in cases of trademark and patent law in Germany.

As was noted, existing comparative analyses of online intermediary liability issues in EU jurisdictions is limited to German and French law[14]; however, the paths taken in these two jurisdictions are complex, specific to the legal traditions of these particular countries, and reliant on decades of case law. The original sources on the pertinent doctrines are not even available in English, the *lingua franca* of Europe. Therefore, transferring this approach to other parties is problematic. In the absence of EU-level rules, differences in national law would inevitably result in substantively different liability outcomes, which is not desirable and may also lock contributory liability enforcement attempts within a jurisdictional maze. None of this would be an issue if indirect copyright infringement or contribution to infringement were explicated in substantive copyright law at the EU level.

The liability of contributors to digital piracy must be addressed at the supranational level, because digital piracy or large-scale commercial copyright infringement online is an inherently cross-border phenomenon that cannot be addressed through national laws alone. This is already recognised at the EU level through efforts to harmonise some intellectual property tort

[13] Leistner, M. (2014) Structural aspects of secondary (provider) liability in Europe. *Journal of Intellectual Property Law & Practice*, 9 (1), pp. 75–90, Available from: https://doi.org/10.1093/jiplp/jpt213, and Husovec, M. (2018) *Injunctions against intermediaries in the European Union: Accountable but not liable?* Cambridge: Cambridge University Press.

[14] Dinwoodie, G., Dreyfuss, R., and Kur, A. (2009) The Law Applicable to Secondary Liability in Intellectual Property Cases. *New York University Journal of International Law and Politics*, 2, pp. 201–235. Available from: https://nyujilp.org/wp-content/uploads/2013/02/42.1-Dinwoodie-Dreyfuss-Kur.pdf, Leistner, M. (2014) Structural aspects of secondary (provider) liability in Europe. *Journal of Intellectual Property Law & Practice*, 9 (1), pp. 75–90, Available from: https://doi.org/10.1093/jiplp/jpt213, and Husovec, M. (2018) *Injunctions against intermediaries in the European Union: Accountable but not liable?* Cambridge: Cambridge University Press., Angelopoulos, C. (2016) *European Intermediary Liability in Copyright: A Tort-Based Analysis*. Wolters Kluwer.

rules, most notably the Enforcement Directive 2004/48/EC, yet the lack of comprehensive contributory liability rules is apparent.

Because limited substantive rules on contributory liability are already included in EU law and further harmonisation has already been advocated for and substantiated in existing research,[15] this paper will not discuss whether contributory liability is compatible with the Treaty on the Functioning of the European Union and the Treaty on European Union. The purpose of this article is to highlight the lack of secondary liability for non-online intermediaries in substantive European copyright law, which in the authors' opinion is a critical gap in view of evolving digital piracy models.

It is also noteworthy that the statutory intermediary liability rules and obligations have recently been expanded through the introduction of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act (DSA)). Therefore, it is time to revisit and comprehensively address other copyright liability questions that have been side-lined for the last decade.

Despite some statutory uncertainties, copyright case law in the US has addressed the matter of contributing to copyright infringement with a long-standing doctrine of contributory copyright infringement. This doctrine was introduced by the US courts in 1911 (*Kalem Co. v. Harper Bros.*, 222 U.S. 55, 63 (1911)),[16] and its modern version allows intellectual property rightsholders to seek relief not only from direct infringers, but also from those who somehow knew of and materially contributed to infringing behaviour (*Gershwin Publishing Corp. v. Columbia Artists Mgmt., Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971)). To establish contributory infringement, it must first be shown that the party had knowledge of the infringement of the right by another. Second, the party must materially contribute to the infringement. If it was reasonable for the defendant to think that infringement was taking place, the

[15] Husovec, M. (2018) *Injunctions against intermediaries in the European Union: Accountable but not liable?* Cambridge: Cambridge University Press, pp. 42–46, Dinwoodie, G., Dreyfuss, R., and Kur, A. (2009) The Law Applicable to Secondary Liability in Intellectual Property Cases. *New York University Journal of International Law and Politics*, 2, pp. 201–235. Available from: `https://nyujilp.org/wp-content/uploads/2013/02/42.1-Dinwoodie-Dreyfuss-Kur.pdf`, Leistner, M. (2014) Structural aspects of secondary (provider) liability in Europe. *Journal of Intellectual Property Law & Practice*, 9 (1), pp. 75–90, Available from: `https://doi.org/10.1093/jiplp/jpt213`, Angelopoulos, C. (2016) *European Intermediary Liability in Copyright: A Tort-Based Analysis*. Wolters Kluwer.

[16] Davis Powell, C. (2009) The Saga Continues: Secondary Liability for Copyright Infringement Theory, Practice and Predictions. *Akron Intellectual Property Journal*, 3 (1), Article 7. Available from: `https://ideaexchange.uakron.edu/akronintellectualproperty/vol3/iss1/7`

knowledge standard is satisfied. Moreover, a party that suspects wrongdoing and fails to investigate will also be deemed to satisfy the knowledge standard.

Although this doctrine was not expressly codified into the 1976 US Copyright Law, the U.S. Supreme Court has argued in follow-up cases that the "*absence of such express language in the copyright statute does not preclude the imposition of liability for copyright infringements on certain parties who have not themselves engaged in the infringing activity*" (*Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417, 104 S. Ct. 774 (1984)). The *Sony* precedent remains pivotal in establishing the requirement and limitations of secondary liability for copyright infringement. In *Sony*, the Court explained that "*[t]he sale of copying equipment, like the sale of other articles of commerce does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial noninfringing uses*" – thus essentially establishing safe-harbour exceptions from liability. Nevertheless, a party who knowingly induces, causes or materially contributes to copyright infringement by another person, but who has not committed or participated in the infringing acts themselves, may be held liable as a contributory infringer if they had knowledge, or reason to know, of the infringement. It is very important to note that Sony was not historically an online intermediary, but rather a hardware provider, and the US doctrine of secondary liability for copyright infringement has evolved without even considering the operational technicalities of the internet and the role that online intermediaries play in it.

Contributory liability for copyright infringement doctrine was essential and central in order for US copyright law to effectively address the challenge of peer-to-peer (P2P) copyright piracy starting with Napster (*A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th. Cir., 2001)). This later extended to P2P network operators such as Aimster, Morpheus, Kazaa and Grokster, who attempted to technologically evade liability by increasingly distancing themselves from direct infringement and claiming safe-harbour exceptions according to *Sony*. The 2005 case of *MGM Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005), where the doctrine of contributory infringement was addressed by the US Supreme Court, currently serves as the penultimate digital piracy precedent case of US copyright law. *Grokster* established that a maker or distributor of software with the object of promoting its use to infringe copyright is liable for the resulting acts of copyright infringement, even though the Grokster program was capable of substantial non-infringing uses. Grokster met the requirements for contributory liability because it induced copyright infringement, and this constituted material contribution to the copyright infringement committed by the users of Grokster. The

inducement rule foresees liability for purposeful, culpable expression and conduct aimed at copyright infringement. US scholars argue that the court based this interpretation of contributory liability on the patent infringement rules,[17] even though the Supreme Court did not mention this themselves. The notion of contributory inducement was further supported by Grokster aiming its technology towards known infringers, and receiving financial benefit from the infringing activities, all of which demonstrated unlawful intent.[18] Such intent towards infringement disqualified Grokster from defence involving the application's substantial noninfringing uses.[19]

A summary of the current US rules is provided in the instructions given to federal civil law jury members on matters of contributory infringement of copyright law.[20] In order for a contributor to be liable for copyright infringement, both of the following elements need to be established by a preponderance of evidence:

> *1) the contributor knew or had reason to know of the infringing activity of a direct infringer; and*
>
> *2) the contributor intentionally induced or materially contributed to the infringer's direct infringing activity. The contributor's intent to induce the infringing activity must be shown by clear expression of that intent or other affirmative steps taken by contributor.*

The requirement for knowledge of the infringement is met if the party is notified of the infringement. The reason to know standard is met if the infringement is reported in the public media or the contributor failed to perform due diligence where it would have been reasonable.

It is not clarified what would be considered material contribution, and in the US courts this is addressed on a case-by-case basis according to the available evidence. According to commentators,[21] material contribution shall be quantified in the context of the relationship between the contributor and the direct infringer, and independently between the contributor and the actual act of infringement. Contributions which modify and aggravate the

---

17 *Ibid.*

18 *Ibid.*

19 Bartholomew, M., and McArdle, P. F. (2011) Causing infringement. *Vanderbilt Law Review*, 64 (3), pp. 675–746.

20 Ninth Circuit Jury Instructions Committee. (2017) 17.21. Derivative Liability—Contributory Infringement—Elements and Burden of Proof. In: *Manual of Model Civil Jury Instructions* [online]. Available from: `https://www.ce9.uscourts.gov/jury-instructions/node/279`[Accessed 28 November 2022].

21 Tilly, J. M. (2008) Perfect 10 v. Visa: the future of contributory copyright infringement. *Oklahoma Law Review*, 61 (4), pp. 865–890; Bartholomew, M., and McArdle, P. F. (2011) Causing infringement. *Vanderbilt Law Review*, 64 (3), pp. 675–746.

infringement, whether actions, devices or software, are all material. This would certainly include contributions that (a) increase the damage caused by the infringement, (b) increase the illicit income from the infringement, (c) increase the scale of the infringement (e.g., the number of parties to whom the infringing content becomes available), or (d) provide financial or other benefit (e.g., business development benefit) from the infringement.

In EU copyright case law, there are only very limited attempts to establish contributory copyright infringement. The CJEU has attempted to stretch the rights of "communication to the public" and of "making available" to accommodate contributory copyright infringements, which would not have been needed if proper statutory regulation existed. The CJEU's attempts were based on the creative interpretation of EU Directives 2000/31/EC and 2001/29/EC, and are generally very complicated efforts to put new meaning into the economic rights of copyright under EU law, which was never conceived by the legislator. Most notable is C-527/15 *Filmspeler*, where the court held that "a communication to the public" includes when someone sells hardware with add-ons containing hyperlinks to pirate websites already installed. *Filmspeler* attempts to establish several complementary criteria for liability for infringing the right of "*a communication to the public*": "*[par 31.] The user makes an act of communication when he intervenes, in full knowledge of the consequences of his action, to give access to a protected work to his customers and does so, in particular, where, in the absence of that intervention, his customers would not, in principle, be able to enjoy the broadcast work*"

Note the "*full knowledge*" standard, which is not clarified and is much stricter than the knowledge standard in US copyright law ("*reasonable for the defendant to think that infringement was taking place*"). *Filmspeler* also required that "*protected work must be communicated using specific technical means, different from those previously used or, failing that, to a 'new public'*", and the communication to the public must be for profit ("*the profit-making nature of a communication*"). The latter conditions are endemic to digital piracy cases and for that reason not problematic, but they further complicate enforcement and would simply be unnecessary if there were proper contributory infringement rules. The latest CJEU attempt, presented in the CJEU's judgement in Cases C-682/18 *YouTube* and C-683/18 *Cyando*, is even more creative, as the court explicitly adopted the contributory infringement notion of US law, which is found nowhere else in EU statutory copyright law. The CJEU (Grand Chamber) ruled

> "1. Article 3(1) of 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 must be interpreted as meaning that the operator of a video-sharing platform [Youtube] or a file-hosting and -sharing platform [Uploaded.to], on which users can illegally make protected content available to the public, does not make a 'communication to the public' of that content, within the meaning of that provision, unless it contributes, beyond merely making that platform available, to giving access to such content to the public in breach of copyright. That is the case, inter alia, where that operator has specific knowledge that protected content is available illegally on its platform and refrains from expeditiously deleting it or blocking access to it, or where that operator, despite the fact that it knows or ought to know, in a general sense, that users of its platform are making protected content available to the public illegally via its platform, refrains from putting in place the appropriate technological measures that can be expected from a reasonably diligent operator in its situation in order to counter credibly and effectively copyright infringements on that platform, or where that operator participates in selecting protected content illegally communicated to the public, provides tools on its platform specifically intended for the illegal sharing of such content or knowingly promotes such sharing, which may be attested by the fact that that operator has adopted a financial model that encourages users of its platform illegally to communicate protected content to the public via that platform"

Overall, these interpretations are an example of explicit judicial activism, are clearly forced, and have little to do with the right of "communication to the public" *per se*. The latter example (the joined *YouTube* and *Cyando* cases) shows undertones of influences from across the Atlantic, but, regrettably, is exceedingly specific to the "*operator of a video-sharing platform*" and "*a file-hosting and -sharing platform*", which are traditional online intermediaries. Such judicial activism and forced creativity would be unnecessary if the EU legislator would do their job of introducing proper statutory rules on contributory copyright infringement. The CJEU here did the commendable job of acknowledging the gaps in EU copyright law and laying the groundwork for contributory liability within it, but this issue has to be picked up by the EU legislator. For the rules to become effective in lower level national courts, without the need for expensive, multi-year litigation going all the way to the CJEU and back, they need to become general rules unencumbered by the specific facts and extreme conditionality of said cases.

Tort law is not part of the EU Acquis, and it would be impossible to unify the two anytime soon. Nevertheless, some aspects of torts related to intellectual property infringements (e.g. damages rules, injunctions) are already harmonised in EU Law through Directives 2000/31/EC, 2001/29/EC and 2004/48/EC, thus setting the precedent for the further *lex specialis* of intellectual property infringement torts.

There is an obvious need to harmonise contributory infringement criteria and rules. As the reasoning for this is thoroughly presented in an existing body of legal research,[22] there is no need to repeat it here. For the purposes of this article, it is most important to emphasise that harmonisation is also important because: new emerging models of digital piracy do not rely on traditional internet intermediaries and cannot be addressed through existing intermediary rules, even after the DSA updates; and digital piracy is inherently multinational (as will be illustrated by the Mobdro case study, below), spanning multiple EU jurisdictions and therefore being incapable of reasonably being addressed through national law. The reviewed US rules are not incompatible with the basic civil liability principles in European countries; therefore, the US rules may serve as the starting point for the harmonisation effort in EU copyright law, especially after the CJEU led with the surprise introduction of evidently US-influenced contributory copyright infringement terminology into substantive EU copyright law in C-682/18 *YouTube* and C-683/18 *Cyando*. The need for urgent harmonisation is further illustrated by the analysis below.

3. THE EVOLUTION OF DIGITAL PIRACY

Despite notable decreases, digital piracy remains significant and costs billions of euros per year for the EU economy.[23] Digital piracy is a dynamic phenomenon which is evolving and adapting in response to new internet technologies and internet use trends, as well as in response to legal developments. Copyright piracy is now being described as almost exclusively digital. The last two decades have seen the rapid growth of data transmission speeds, especially over wireless networks, which have

[22] Husovec, M. (2018) *Injunctions against intermediaries in the European Union: Accountable but not liable?* Cambridge: Cambridge University Press, pp. 42–46, Dinwoodie, G., Dreyfuss, R., and Kur, A. (2009) The Law Applicable to Secondary Liability in Intellectual Property Cases. *New York University Journal of International Law and Politics*, 2, pp. 201–235. Available from: `https://nyujilp.org/wp-content/uploads/2013/02/42.1-Dinwoodie-Dreyfuss-Kur.pdf`, Leistner, M. (2014) Structural aspects of secondary (provider) liability in Europe. *Journal of Intellectual Property Law & Practice*, 9 (1), pp. 75–90, Available from: `https://doi.org/10.1093/jiplp/jpt213`, Angelopoulos, C. (2016) *European Intermediary Liability in Copyright: A Tort-Based Analysis*. Wolters Kluwer.

[23] EUIPO. (2021) *Online Copyright Infringement in the European Union: Music, Films and TV (2017–2020), Trends and Drivers* [online].

resulted in digital piracy shifting from P2P downloads (download now, consume later) to the streaming of digital content (download and consume simultaneously). Over the last decade, streaming piracy has far outpaced the more traditional P2P download, and, according to the latest estimates, the piracy of live TV/sports programming is more than double that of film and music piracy combined.[24] The deployment of 4G and 5G networks and global entertainment and sports phenomena also led to the surge in demand for the streaming of live entertainment and sports programming.

In 2019, it was reported that digital video piracy costs to the US economy were $29.2 billion[25] a year, while "*collective revenues, according to most estimates, have reached nine or 10 figures*".[26] Streaming piracy via unlicensed IPTV services and apps is the largest-growing section of these figures. These services represent a good market fit for consumers, who are already accustomed to online streaming as a primary form of daily entertainment. For live sports and original shows, this is also the preferred form, as nobody wants to wait until content has become stale and outdated.

The online presence during the COVID-19 pandemic led to an increased array of high-quality streaming devices and a variety of illicit content offers.[27] Live sports were especially affected by streaming piracy during the COVID-19 pandemic: a 2021 estimate of sports streaming piracy alone put damages at an estimated $28.3 billion per year.[28] While these estimates are based on the US, estimates for the EU are likely even higher due to generally higher levels of piracy (45.72% in Europe compared to 13.48% in North America in 2020[29]) and larger population numbers (almost 500 million people in the EU compared to 330 million in the US).

---

[24] *Ibid*, pp. 15–55.

[25] Blackburn, D., Eisenach, J. A., and Harrison Jr., D. (2019) *Impacts of Digital Piracy on the U.S. Economy* [online]. NERA Economic Consulting, The Global Innovation Policy Center, U.S. Chamber of Commerce. Available from: `https://www.theglobalipcenter.com/wp-content/uploads/2019/06/Digital-Video-Piracy.pdf`

[26] Bushnell, H. (2019) *Inside the complex world of illegal sports streaming*. [online] Yahoo Sports. Available from: `https://sports.yahoo.com/inside-the-complex-world-of-illegal-sports-streaming-040816430.html` [Accessed 28 November 2022].

[27] EUIPO and Europol. (2022) *Intellectual Property Crime Threat Assessment 2022*. Luxembourg: Publications Office of the European Union. Available from: `https://www.europol.europa.eu/cms/sites/default/files/documents/Report.\%20Intellectual\%20property\%20crime\%20threat\%20assessment\%202022\_2.pdf` [Accessed 28 November 2022].

[28] Balderston, M. (2021) *Sports Piracy Costs $28.3B Per Year, Report Shows*. [online] TV Tech. Available from: `https://www.tvtechnology.com/news/sports-piracy-costs-dollar283b-per-year-report-shows` [Accessed 28 November 2022].

[29] Go-Globe. *Online Piracy in Numbers – Facts And Statistics* [Infographic]. [online]. Available from: `https://www.go-globe.com/online-piracy-in-numbers-facts-and-statistics-infographic/` [Accessed 3 July 2023]

The legislative effort with respect to stronger online intermediary liability rules and obligations has also caused another notable trend. Although its scope is not fully estimated, streaming piracy has increasingly taken place not on mainstream audio-visual content streaming platforms such as YouTube or Twitch, but on dedicated pirate-run digital piracy platforms. Dedicated piracy platforms are a little-researched part of the dark web, whose content is not readily accessible, not indexed by web search engines, and requires specific software, configurations, and/or authorisation to access. The main purpose of dedicated piracy platforms is to distribute pirated digital content; however, they may have multiple other purposes – e.g., to collect revenue, provide embedded services, corrupt user devices for cybercrime purposes, etc.

This trend is well illustrated by the Mobdro platform, which is analysed further in this article. At its peak in 2021, Mobdro reached an unparalleled scale of more than 100 million users. The emergence of dedicated piracy platforms implies that pirates have become adept at overcoming online intermediary-level measures aimed to contain piracy, such as filtering and blocking. For example, domain or IP address blocking is effective against websites, but not against dedicated pirate software and mobile apps, which bypass the DNS servers of online intermediaries and may use CDNs and dynamic IP addresses for the online part of their services. Moreover, digital content piracy platforms have become gateways for other criminal activities. Europol has linked piracy apps to cybercrime activities such as crypto-jacking or the distribution of malware. Pirates exploit new technologies to conceal digital traces and use proxy services to create resilient hosting networks.[30]

In a complex environment like the modern internet network, all kinds of internet infrastructure have been taken advantage of by digital pirates. From a purely instrumental perspective, it may appear that digital piracy is enabled not only by the actions of primary perpetrators, but also by the various internet platforms and services which host or distribute pirated content and run, make accessible or enable pirate services. This has been the rationale for establishing safe-harbour exceptions from secondary liability for online intermediaries, as long as they act as *bona fide* infrastructure service providers and are not aware of infringement. Internet services and internet infrastructure platforms have predominantly legitimate uses, which are not related to piracy. As a general rule, based on the so-called

[30] Turcotte, J. (2021) *Disrupting Attacker Value Propositions in Residential Networks*. [online] Doctoral dissertation, Worcester Polytechnic Institute. Available from: `https://digital.wpi.edu/downloads/1r66j4181` [Accessed 28 November 2022], EUIPO and Europol (2022).

mere conduit principle such services and platforms are considered internet intermediaries, providers of transparent services and not content controllers. Therefore, online intermediaries have been allowed safe harbour rules – a set of conditions under which intermediary service providers are exempted from liability for third party content. Safe harbour rules have been upheld multiple times in the case law; however, courts in the US and the EU have been slowly moving in the direction of limiting them in case of ignorance or sometimes even collaboration in unlawful activity by intermediaries. In US copyright law, this is underscored by the evolution from *Sony* to the *Aimster, Morpheus, Kazaa* and eventually *Grokster* cases; in EU copyright law, it is evident in the *Filmspeler*, *YouTube* and *Cyando* cases analysed in the preceding section of this article. While basic safe harbour liability exceptions are retained, the current rules include an extensive set of legal obligations with respect to protections against unlawful content (including pirated intellectual property content) extending to automatic filtering of explicitly infringing content, as well as promptly reacting to reports on infringing content. It is too early to assess the full effects of the latest rules introduced by the DSA, but it is very clear that they will have a very limited effect on the newest and currently dominant form of digital piracy: streaming piracy on dedicated platforms, such as Mobdro, which will be analysed in detail below.

As was noted, streaming piracy has been evolving towards major independent platforms dedicated to piracy which do not rely on safe harbour liability exceptions and which pretend to be legitimate only at end-user level (mainly by copying the high-quality UI and UX of legitimate platforms such as Netflix). After the OG online piracy websites such as the Pirate Bay became much more difficult to access due to blocking efforts, the opportunity emerged for blocking circumvention and piracy-concealing services, such as VPNs employed by more technically adept users, as well as for stand-alone software applications that work straight out of the box without any technical knowledge needed on part of the user.[31] This click-and-play format proved popular, with software such as Popcorn Time, Showbox and Terrarium TV attracting millions of viewers. One of the most popular click-and-play tools to emerge was Mobdro, an Android-based software application focusing on TV content from around the world. Live TV, sports channels and 24/7 content were all available on Mobdro, providing an easy-to-use solution for anyone capable of installing and running it.[32] Stand-alone software applications that

[31] Maxwell, A. (2021) *Pirate TV Streaming App Mobdro Disappears, Users in Mourning*. [online] Torrent Freak. Available from: `https://torrentfreak.com/pirate-tv-streaming-app-mobdro-disappears-users-in-mourning-210215/` [Accessed 28 November 2022].

[32] *Ibid.*

reproduce pirated content without any technical knowledge needed on part of the user are referred to as dedicated piracy platforms in this article. As was noted, by 2021 Mobdro was one of the most popular dedicated piracy platforms on the internet.

Another evolving facet of digital piracy is its monetisation. The costs involved in running and maintaining dedicated piracy platforms are significant, and require even not-for-profit pirates to seek ways to monetise their pirate operations. Traditionally, pirates would either collect direct payments in the form of subscription fees or donations or accept ads on the platform from various ad networks. Payment providers, VPN service providers and ad networks in these situations are caught up, at least indirectly, in enabling digital piracy, yet unless they knowingly and specifically profit from it, they are considered intermediaries just like almost any web service used by the pirate operation, including basic services like Google. The key aspect here is that the ad network, VPN network or payment network, like many online intermediaries, provide a basic and universal infrastructure service (a mere conduit) which can be used by anyone, including pirates.

The role of VPN networks in facilitating digital piracy is worth a separate research inquiry that is beyond the scope of this article. There are separate efforts to limit the use of payment and ad networks by pirates through stricter AML/KYC rules, as well as advertising ethics rules. These efforts have been moderately successful in at least complicating the monetisation potential of pirate platforms, while also helping to uncover perpetrators.[33] As a result, more recently the traditional direct commercialisation of illegal content (i.e., charging for access to pirated content or collecting ad revenue) has been complemented by or has competed with a new commercialisation model based on collecting fees for embedding additional services into pirate platforms.

Embedding third-party software code into another application is not a new phenomenon. Pirated content, software and services have long served as vehicles for spreading malicious code; however, until recently there have been no known cases in which the owners of the embedded code were directly paying for the operation of the pirate platform. The third-party embedded SDK model is thus an evolution in the pirate platform "business" model. From a technical perspective, this is achieved by including

[33] Batikas, M., Claussen, J., and Peukert, C. (2017) *Follow the money: Piracy and online advertising*. 28th European Regional Conference of the International Telecommunications Society (ITS): Competition and Regulation in the Information Age, Passau, Germany, 30th July–2nd August, 2017. Available from: `https://www.econstor.eu/handle/10419/169448` [Accessed 28 November 2022].

a third-party code (SDK) into the mobile, desktop or web application of the pirates. This turns the user's device into a slave node on the embedded service owner's network, which performs tasks on command from the embedded service owner (the master node). In most cases, the node operation is latent and not clearly noticeable to the user, who has installed or run a pirate app containing the embedded service node, and the ethics and lawfulness of this practice are questionable.[34] The pirates (pirate app owners) may be paid based on the number of active online instances of such embedded SDKs which are run on end-user devices; however, other models, e.g., based on uptime, volume of data transferred, etc., are certainly possible. Network security research on the residential proxy embedded SDK model has found that such SDK providers offer app developers mobile proxy SDKs as a competitive app monetisation channel, with $50,000 per month per 1 million MAU (monthly active users).[35]

There is limited research describing the functionality of such latent nodes on user devices. One common functionality involves residential proxy network nodes or user surveillance (data gathering) nodes. Note that all of this clearly raises very serious concerns on compliance with the privacy, data protection and cybersecurity regulations, and corresponding risks to consumers (the owners of end user devices, which are enslaved as proxy nodes). However, this is not investigated in this article, which is limited to copyright law and contributory liability for copyright infringements.

A key aspect of the embedded service model is that the pirate platform effectively becomes infrastructure for the embedded service network. This is the other way around compared to traditional intermediaries, where pirates are the users of an intermediary rather than providers of the infrastructure themselves. The pirate app user network thus becomes an embedded service network, and vice versa. The value of the embedded service grows alongside the size of the network where such a service is embedded, benefiting from the well-known economic network effects described by Metcalfe's law. The embedded service owner becomes directly interested in growing the pirate platform, as it also grows the embedded service network and allows the embedded service owner to collect even higher revenue from the users of embedded service. Thus, embedded services are indispensable for pirates to be able to collect revenue on their operation, which makes both sides directly

[34] Tosun, A., De Donno, M., Dragoni, N., and Fafoutis, X. (2021) RESIP Host Detection: Identification of Malicious Residential IP Proxy Flows. In *2021 IEEE International Conference on Consumer Electronics (ICCE)*. Las Vegas: IEEE, pp. 1–6.

[35] Mi, X., Tang, S., Li, Z., Liao, X., Qian, F., and Wang, X. (2021) Your Phone is My Proxy: Detecting and Understanding Mobile Proxy Networks. In *Proceeding of ISOC Network and Distributed System Security Symposium (NDSS), 2021*.

incentivised to grow the network. The latent nature of the embedded services is two-fold: it is not obvious to the consumers whose devices are enslaved as proxy nodes, and it is not clear to the users (most often businesses) of the proxy service. Without discussing the legality and ethics of the use of embedded services, it is noteworthy that the users of embedded services (e.g., business users of a residential proxy service) are very likely unaware that the service nodes are running on top of a piracy network. Research on this topic has discovered that user devices are exposed to major security and privacy risks, are often used for malicious purposes, and are likely compromised. The behaviour of residential proxies, which supposedly voluntarily serve on the network, differs starkly from expected usage in the home.[36]

This evolution of piracy "business" models highlights the limitations of the online intermediary-focused *lex specialis* – liability rules which are designed to address the use of legitimate intermediary infrastructure by bad actors (pirates), but were never designed to deal with the use of digital piracy infrastructure for non-piracy purposes, even if the latter are legitimate. While the former clearly requires carveouts from the legal liability rules for intermediaries, which is accepted in the current regulatory regime, the latter is more akin to a legal case of collaboration between two independent parties (pirates and the embedded services party) in copyright infringement – at least in maintaining and growing infrastructure whose primary purpose is mass copyright infringement on a commercial scale.

4. THE MOBDRO CASE STUDY

The Mobdro case study is representative of the evolution of digital piracy, underscored by shifts to live streaming and commercialisation through embedded services. The Mobdro app operated at least from 2018 to March 2021, and was the leading pirate streaming platform with more than 100 million users. Mobdro allowed users to stream copyrighted content (TV shows, live sports, movies, premium music videos, etc.) on Android OS devices, and was highly praised by reviewers for the availability and quality of content, including Live TV Channels (Worldwide), Live Sport Channels, the Latest Movies & TV Shows, as well as its intuitive and friendly UI and UX.[37] For all of these reasons Mobdro was the leading dedicated streaming piracy platform, which is representative of the direction that digital piracy is evolving in and provides a real-world context to the issues of contributory

[36] Turcotte, J. (2021) *Disrupting Attacker Value Propositions in Residential Networks.* [online] Doctoral dissertation, Worcester Polytechnic Institute. Available from: `https://digital.wpi.edu/downloads/1r66j4181` [Accessed 28 November 2022].

[37] Best Streaming App Reviews. *MOBDRO review.* [online]. Available from: `https://best-streaming-app.reviews/mobdro-review/` [Accessed 28 November 2022].

liability. The analysis of the Mobdro case was selected based on its relative recency and the reasonable abundance public information about it, including information from official sources (Europol) and direct evidence suggesting that Mobdro was monetised through the embedded services model. Such a case allows for the analysis of both the current digital piracy business model and the features of embedded services as intertwined phenomena. In order to achieve a maximally broad and deep analysis of the issue, the real-world case study method is the most appropriate, and case studies that allow for the analysis of multiple phenomena are preferred methodologically.[38]

The Mobdro app was not available through the official Google Play store; however, it was distributed as an APK download in alternative app stores (e.g., APK Free or F-Droid). It was also widely distributed as preloaded software on Android IPTV sticks (such as the Amazon Fire TV stick), which were sold online through various e-commerce marketplaces.

Although the makers of the Mobdro software were anonymous, the Mobdro application had more than 100 million users, and by that measure alone could be compared in popularity to such major legitimate audio-visual digital content platforms as Disney+ or HBOMax. Moreover, the Mobdro user count well exceeded that of multiple global streaming platforms such as Twitch, Tidal, Deezer, Pandora, and Apple TV.[39] The number of users of the Mobdro app is a direct determinant of the size and scale of the pirate network, and hence directly implies the unparalleled scale of this case: Mobdro was clearly a major global player – a whale – in the content streaming marketplace by any standard.

The scale and activities of Mobdro came to light in the context of a Europol investigation, which culminated in the March 2021 takedown of the main Mobdro infrastructure. Europol received complaints from rights holders, among them main European football leagues, about a mobile application illegally distributing video streams. According to Europol, "*The application, downloaded by more than 100 million users via different websites, illegally offered the streaming of videos and TV channels. The Europol investigation identified a number of connected websites and platforms located in Spain and Portugal with connections to servers in Czech Republic*". In addition, according to Europol, the "*Spanish company behind the illegal activity earned its profits through advertisements. Through the computer infrastructure and power, they were able to sell user information to a company related to botnet and DDoS attacks. Investigators*

[38] Gerring, J. (2017) *Case Study Research: Principles and Practices*. 2nd Ed. Cambridge: Cambridge University Press, p. 37.

[39] Snigdha, B. (2022) *Top Streaming Statistics for 2022*. [online] SaaS Worthy. Available from: `https://www.saasworthy.com/blog/top-streaming-statistics/`[Accessed 28 November 2022].

estimate the overall illegal profits at more than €5 million." Note that this is only the direct profit of Mobdro, while the damage done was likely far in excess of this amount. While the Mobdro takedown terminated its infringements, it took multiple years, and it did not address the damages to rightsholders caused by Mobdro and contributors to its operations.

It is noteworthy than in its default mode the Mobdro app operated with embedded services enabled, and only if the user opted out of the embedded services (third party SDK) were they shown ads. It is unclear whether embedded SDK was dormant or operational in ad mode, and how many users actually chose to run it in ad mode. It is also possible that the Mobdro app had multiple embedded SDKs. A Europol report on Mobdro references the fact that "*Through the computer infrastructure and power, they were able to sell user information to a company related to botnet and DDoS attacks*", which suggests monetisation through embedded SDK services.

One Mobdro-embedded SDK service-provider may have been the provider of the embedded SDK focusing on residential proxy network infrastructure, which they admitted themselves when suspending the SDK available to Mobdro after Europol action.[40] This operator of a residential proxy network stated that they "*have zero tolerance to illegal activities. When it came to our attention that Mobdro (a publisher which was using our commercial SDK) had been subject to a law enforcement investigation for alleged copyright infringement, we suspended their right to use our SDK*". However, this provider did not clarify what their relationship and commercial arrangement with the Mobdro publishers was.[41] The costs of residential proxy service providers for clients are based on the number of proxies used and data transfer volume[42]; therefore, it is reasonable to assume that the relationship between Mobdro and this SDK provider was continuous – i.e., Mobdro was continuously and periodically paid to host SDK based on the MAU of the Mobdro app.

In case of residential proxy SDKs, according to cybersecurity research, such SDKs turn the Android device running the app into a peer on a residential proxy network. The device becomes a network node, where the internet address and bandwidth of the Android device are used for unknown purposes. Such networks have previously been named malicious, dark services, and have been compared to botnets by network security

[40] Maxwell, A. (2021) *Mobdro: Luminati Proxy Service "Suspended Service" To Pirate App*. [online] Torrent Freak. Available from: `https://torrentfreak.com/mobdro-luminati-proxy-service-suspended-service-to-pirate-app-210315/` [Accessed 28 November 2022].

[41] *Ibid*.

[42] Proxy Way. (2023) *10 Best Residential Proxies of 2023*. [online]. Available from: `https://proxyway.com/best/residential-proxies`

researchers.[43] However, the full details of the Mobdro embedded service network are yet to be established.

The Mobdro case highlights the major risks not only of copyright infringement, but also regarding privacy and personal data, as well as from cybersecurity perspectives, since, according to Europol, it involved the sale of user information and may have exposed user devices to unsolicited data transfers. Mobdro was also not a one-off host for the embedded SDK, as such embedded services appear to be the predominant model to monetise various apps, of which many are related to piracy.

5. PARTIES BEHIND EMBEDDED SERVICES: INTERMEDIARIES OR COLLABORATORS?

It may be a useful exercise to try to map the known circumstances of the Mobdro case onto the conditions of contributory copyright infringement previously summarised in this article in order to evaluate the legal status of the party behind embedded services.

There is no doubt that the Mobdro developers and publishers were the direct infringers in this case. Mobdro was also a major player in content streaming, boasting more than 100 million installs, yet the developers stayed anonymous and the app was not distributed through the official Google Play app store, which normally requires clear disclosure of the app developers and subjects the app to the Google vetting process. Despite the app running the live broadcasting of major sport leagues, no legitimate content partnerships were publicly reported or confirmed. In 2018, reputable media sources already publicly reported doubts on the lawfulness of Mobdro.[44] In addition, by 2021 Mobdro had accumulated a handful of DMCA notice and takedown complaints.[45] These circumstances certainly suggest that Mobdro was engaging in copyright infringement "business", and it was public knowledge. Mobdro partners either knew of the illegitimacy of Mobdro operations or

[43] See Mi, X. et al. (2019) Resident Evil: Understanding Residential IP Proxy as a Dark Service. In *2019 IEEE Symposium on Security and Privacy (SP)*. San Francisco: IEEE, pp. 1185–1201; Hacid, H. et al. (Eds.). (2021) *Service-Oriented Computing – ICSOC 2020 Workshops*. Spinger, Cham; Tosun, A., De Donno, M., Dragoni, N., and Fafoutis, X. (2021) RESIP Host Detection: Identification of Malicious Residential IP Proxy Flows. In *2021 IEEE International Conference on Consumer Electronics (ICCE)*. Las Vegas: IEEE, pp. 1–6.

[44] Williams, A. (2018) *Mobdro: the app that wants to take on Kodi for a shot at the streaming crown*. [online] Tech Radar. Available from: `https://www.techradar.com/news/mobdro-the-app-that-wants-to-take-on-kodi-for-a-shot-at-the-streaming-crown` [Accessed 28 November 2022].

[45] Maxwell, A. (2021) *Pirate TV Streaming App Mobdro Disappears, Users in Mourning*. [online] Torrent Freak. Available from: `https://torrentfreak.com/pirate-tv-streaming-app-mobdro-disappears-users-in-mourning-210215/` [Accessed 28 November 2022].

had multiple direct and serious reasons to know and doubt the legitimacy thereof. It is implausible that the SDK developer did not have knowledge of the activities performed by the app where their SDK was embedded, especially since the relationship between Mobdro and the SDK providers was continuous, and the network of nodes supplied by Mobdro was very sizable (if not the largest). Separately, it is noteworthy that the residential proxy business which is known to rely on embedded service SDKs is highly lucrative and generates hundreds of millions dollars in revenue[46]; therefore, entities engaged in this business have ample resources with which to do due diligence on the platforms which run their residential proxy SDKs. Failure to know the customer (or business partner, as in the case between Mobdro and its SDK provider) at the very least raises serious questions about the fulfilment of duties of care, and may allow applications of vicarious liability, but this analysis would go beyond the scope of this article.

Collaboration between Mobdro and the providers of the embedded services SDK had to be significant, since at minimum such collaboration would include software code exchange, payment, as well as some form of accounting of MAU, on which the payment would be based. All of these cooperation activities are continuous and periodical (likely monthly). A significant and continuous relationship is necessitated by multiple distinct reasons. First, the MAU accounting and payments by the SDK provider for the services of the Mobdro platform. Second, the technical integration of the SDK and the Mobdro app. Both the SDK and the app underwent multiple versions (software updates) over the years,[47] and continuous technical functioning of the two would be impossible if there were not continuous technical collaboration and exchange of updates between the two parties. Since the SDK is part of the software code of the pirated app, the maker of such an SDK would normally provide support and maintenance with respect to integrating the SDK, and would maintain it up to date in subsequent releases of the new versions of the pirate app. Based on the basic analysis of versions of the Mobdro app available in the Internet Archive,[48] the software code of the embedded SDKs was obfuscated, at the very least to hide it from competition and deter reverse engineering, which further underscores the notion of continuous collaboration. Code obfuscation during compilation is

[46] Maayan, M. (2021) *Bright Data CEO: "We have crossed $100 million in annual revenue"*. [online] CTech, 12 December. Available from: `https://www.calcalistech.com/ctech/articles/0,7340,L-3924814,00.html` [Accessed 28 November 2022].

[47] Archive images of the Mobdro website suggest more than a dozen releases and multiple versions of the Mobdro app. See: `https://web.archive.org/web/20200810194730/https://mobdro.org/` [Accessed 3 July 2022]

[48] *Ibid*.

normally achieved by close cooperation between the provider of the code and the party compiling the final application, so that the functionality of the SDK is not impaired. All of this evidence of a continuous relationship between Mobdro and the SDK provider is a very important aspect from which to establish the collaborative and contributory nature of the relationship between the two. In turn, this can establish the causal and contributory relationship of the SDK in the copyright infringing activities of the piracy platform.

As was already noted, for the embedded service providers the Mobdro network is an important part of service infrastructure. The provider of the embedded services SDK has a vested interest in the growth of the Mobdro user base, since it also grows the embedded services infrastructure. This in turn would grow the income from the Mobdro operation for both parties and increase the scale of the infringement (the number of Mobdro end users). Thus, it is reasonable to assume, and it would not be surprising if it were the case, that the growth of the Mobdro user base (e.g., Mobdro marketing) was incentivised through payments by the SDK. However, even if it was not actively incentivised by the SDK provider, it is clear that Mobdro growth financially benefitted both Mobdro and the SDK provider, and thus the SDK provider directly (through the growth of the Mobdro network) benefitted from copyright infringement committed by Mobdro, as it would grow the business of the SDK provider.

In addition to the SDK provider's contribution to the relationship between themselves and Mobdro, it is independently useful to note that each actual act of piracy on the Mobdro platform (i.e., a Mobdro user running the Mobdro app and watching pirated content streamed by Mobdro) was an active node for the SDK provider. Thus, the SDK provider was actually directly benefiting from each act of copyright infringement committed by Mobdro.

All of this suggests material, indirect contribution to the Mobdro operation by the embedded service provider; their intentional participation in and benefit from the actual operation of the Mobdro app; and the implausibility of the idea that the SDK provider had no knowledge of the Mobdro "business" of copyright infringement, or had no intent with respect to Mobdro continuing and expanding their operations. In the studied case, all activities of the Mobdro app in the EU were *prima facie* illegitimate from a copyright law perspective, and there was not even a single attempt to portray them as legitimate. As was noted, serious legitimacy concerns were raised very early into Mobdro's operations, even by non-legal reviewers. In such a situation, the SDK provider could not have expected any legitimate use of the Mobdro platform, and no explanation to that end was provided

by the SDK provider in the post-takedown acknowledgment.[49] Instead, the SDK provider only denied their awareness of Mobdro's illegitimacy, which was already rebutted by the arguments above. The SDK provider had every reason to be aware of Mobdro's activities, and at the very least failed to perform due diligence where it would have been mandatory.

The assumptions in this mapping exercise are based on public information, which is not necessarily vetted and supported by evidence admissible in a court of law, yet this activity demonstrates that the contributory liability criteria appear to have been met in multiple ways. If the operations of the Mobdro platform and the SDK provider would have taken place in the US, the SDK provider would be in serious risk of facing contributory liability for copyright infringement. In the EU, where statutory contributory infringement rules are not available, the SDK provider continues without charge. If contributory liability for copyright infringement rules were available, it is likely that Mobdro would have been shut down much faster through civil action, and there would be opportunities for rightsholders to seek recovery of damages from the contributor – the SDK provider.

The takedown of Mobdro has immediately led to the appearance of multiple copycat streaming piracy platforms attempting to imitate Mobdro. So far, no party has been reported to be facing legal liability for the copyright infringements of the Mobdro pirate platform. The lack of cross-border statutory rules for contributory infringement in the EU is certainly not helpful in this case.

6. CONCLUSION

The lack of contributory liability rules represents a significant gap in substantive EU copyright law, which puts EU rights holders at a disadvantage compared to US rights holders. In the US, copyright case law has adopted a contributory liability doctrine and developed reasonable conditions to enforce such liability against parties contributing to copyright infringement independently from tort law remedies.

This gap is recognised in the jurisprudence, which has advocated for the harmonisation of the EU rules on this matter for more than a decade. In few EU countries, this gap is conditionally filled though national case law by the creative application of national tort law doctrines. The CJEU attempted – in C-527/15 *Filmspeler*, and more recently in joined cases C-682/18 *YouTube* and

[49] Maxwell, A. (2021) *Mobdro: Luminati Proxy Service "Suspended Service" To Pirate App*. [online] Torrent Freak. Available from: `https://torrentfreak.com/mobdro-luminati-proxy-service-suspended-service-to-pirate-app-210315/` [Accessed 28 November 2022]

C-683/18 *Cyando* – to fill this gap with commendable judicial activism based on the stretched interpretation of the "right to communicate to the public", and even the explicit introduction of contributory copyright infringement terminology into substantive EU substantive copyright law. Nevertheless, neither the tort law approach nor the latest CJEU approach are practical against the modern actors of digital piracy, as is evidenced by the very limited enforcement of copyright against parties that contribute to digital piracy in the EU and the continuous, multi-year operations of modern digital piracy platforms such as Mobdro within its borders. This is an acute problem which was nevertheless left out of the EU Digital Services Act (DSA), which only updated the online intermediary liability rules in EU law.

Neither the expansion of the right to communication to the public, nor national tort law, nor the rules governing online intermediary liability are equipped to address rapidly evolving and multinational digital piracy. Digital pirates have demonstrated adaptability to enforcement at the intermediary level by migrating to dedicated digital piracy platforms, which generate significant revenue through embedded services. The providers of these embedded services, not being online intermediaries, exploit this legal quagmire, utilising piracy infrastructure as an integral part of their services and thereby contributing to digital piracy. The case study of Mobdro presented in this article highlights the multinational reach and vast scope of these new digital piracy platforms, which surpass even their legitimate digital content counterparts. While Mobdro has been dismantled, this was the result of a lengthy effort for which final legal resolution remains pending. In the interim, dozens of new digital piracy platforms, monetised through embedded services, persist. Due to the absence of contributory liability rules, it is also problematic for rightsholders to seek civil damages relief from the parties that contributed to Mobdro's operations and profited from them. Separately, the Mobdro case study further illustrates how digital piracy is entwined with data protection and cybersecurity risks. These aspects, although not covered in this article, undoubtedly warrant separate legal research inquiries.

Judicial activism and forced judicial creativity would be unnecessary if the EU legislator would do their job of introducing proper statutory rules on contributory copyright infringement. In said judgements, the CJEU underscored this need and laid the groundwork for contributory liability in EU copyright law, but the job needs to be finished by the EU legislator. The simplest way that embedded services-fuelled piracy can be addressed is via the introduction of general statutory rules on contributory infringement. The limited statutory precedent of harmonising intellectual property tort

rules already exists in EU law. These rules should be modelled on US law, as was largely accomplished with online intermediary liability rules. By codifying them into statutory copyright law, the EU would reign in threats of digital piracy, enhance regulatory certainty and minimise national distortions. The conditions are ripe for such an effort at the EU level, and the proposed revision of the 2004/48/EC Enforcement Directive[50] may present an opportunity to address this matter.

LIST OF REFERENCES

[1] Angelopoulos, C. (2016) *European Intermediary Liability in Copyright: A Tort-Based Analysis*. Wolters Kluwer.

[2] Balderston, M. (2021) *Sports Piracy Costs $28.3B Per Year, Report Shows*. [online] TV Tech. Available from: https://www.tvtechnology.com/news/sports-piracy-costs-dollar283b-per-year-report-shows [Accessed 28 November 2022].

[3] Bartholomew, M., and McArdle, P. F. (2011) Causing infringement. Vanderbilt Law Review, 64 (3), pp. 675–746.

[4] Batikas, M., Claussen, J., & Peukert, C. (2017) *Follow the money: Piracy and online advertising*. 28th European Regional Conference of the International Telecommunications Society (ITS): Competition and Regulation in the Information Age, Passau, Germany, 30th July–2nd August, 2017. Available from: https://www.econstor.eu/handle/10419/169448 [Accessed 28 November 2022].

[5] Best Streaming App Reviews. *MOBDRO review*. [online]. Available from: https://best-streaming-app.reviews/mobdro-review/ [Accessed 28 November 2022].

[6] Blackburn, D., Eisenach, J. A., and Harrison Jr., D. (2019) *Impacts of Digital Piracy on the U.S. Economy* [online]. NERA Economic Consulting, The Global Innovation Policy Center, U.S. Chamber of Commerce. Available from: https://www.theglobalipcenter.com/wp-content/uploads/2019/06/Digital-Video-Piracy.pdf

[7] Bushnell, H. (2019) *Inside the complex world of illegal sports streaming*. [online] Yahoo Sports. Available from: https://sports.yahoo.com/inside-the-complex-world-of-illegal-sports-streaming-040816430.html [Accessed 28 November 2022].

[50] European Commission, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, Peter, V., Radauer, A., Markianidou, P., et al. (2017) *Support study for the ex-post evaluation and ex-ante impact analysis of the IPR enforcement Directive (IPRED): final report*. Luxembourg: Publications Office of the European Union, doi:10.2873/903149.

[8] Davis Powell, C. (2009) The Saga Continues: Secondary Liability for Copyright Infringement Theory, Practice and Predictions. *Akron Intellectual Property Journal*, 3 (1), Article 7. Available from: https://ideaexchange.uakron.edu/akronintellectualproperty/vol3/iss1/7

[9] Dinwoodie, G., Dreyfuss, R., and Kur, A. (2009) The Law Applicable to Secondary Liability in Intellectual Property Cases. *New York University Journal of International Law and Politics*, 2, pp. 201–235. Available from: https://nyujilp.org/wp-content/uploads/2013/02/42.1-Dinwoodie-Dreyfuss-Kur.pdf

[10] EUIPO. (2021) *Online Copyright Infringement in the European Union: Music, Films and TV (2017–2020), Trends and Drivers* [online]. DOI:102814/505158.

[11] EUIPO and Europol. (2022) *Intellectual Property Crime Threat Assessment 2022*. Luxembourg: Publications Office of the European Union. Available from: https://www.europol.europa.eu/cms/sites/default/files/documents/Report.\%20Intellectual\%20property\%20crime\%20threat\%20assessment\%202022_2.pdf [Accessed 28 November 2022].

[12] European Commission, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, Peter, V., Radauer, A., Markianidou, P., et al. (2017) *Support study for the ex-post evaluation and ex-ante impact analysis of the IPR enforcement Directive (IPRED): final report*. Luxembourg: Publications Office of the European Union.

[13] Folsom, T.C. (2009) Toward Non-Neutral Principles of Private Law: Designing Secondary Liability Rules for New Technological Uses. *Akron Intellectual Property Journal*, 3, pp. 43-104.

[14] Frosio, G. (ed.) (2020) *Oxford Handbook of Online Intermediary Liability*. OUP.

[15] Gerring, J. (2017) *Case Study Research: Principles and Practices*. 2nd Ed. Cambridge: Cambridge University Press.

[16] Go-Globe. *Online Piracy in Numbers – Facts And Statistics* [Infographic]. [online]. Available from: https://www.go-globe.com/online-piracy-in-numbers-facts-and-statistics-infographic/ [Accessed 3 July 2023]

[17] Hacid, H. et al. (Eds.). (2021) *Service-Oriented Computing – ICSOC 2020 Workshops*. Spinger, Cham, doi:10.1007/978-3-030-76352-7.

[18] Husovec, M. (2013) Injunctions against Innocent Third Parties: The case of Website Blocking. *JIPITEC*, 4, pp. 116–129.

[19] Husovec, M. (2018) *Injunctions against intermediaries in the European Union: Accountable but not liable?* Cambridge: Cambridge University Press.

[20] Kravets, D. (2009) *English Transcript of Pirate Bay Guilty Verdicts Released*. [online] Wired. Available from: https://www.wired.com/2009/04/english-transcript-of-pirate-bay-guilty-verdicts-released/

[21] Leistner, M. (2014) Structural aspects of secondary (provider) liability in Europe. *Journal of Intellectual Property Law & Practice*, 9 (1), pp. 75–90, https://doi.org/10.1093/jiplp/jpt213

[22] Lemley, M. A., and Reese, R. A. (2004) Reducing Digital Copyright Infringement Without Restricting Innovation. Stanford Law Review, 56 (6), pp. 1345–1434.

[23] Maayan, M. (2021) *Bright Data CEO: "We have crossed $100 million in annual revenue"*. [online] CTech, 12 December. Available from: https://www.calcalistech.com/ctech/articles/0,7340,L-3924814,00.html [Accessed 28 November 2022].

[24] Maxwell, A. (2021) *Mobdro: Luminati Proxy Service "Suspended Service" To Pirate App*. [online] Torrent Freak. Available from: https://torrentfreak.com/mobdro-luminati-proxy-service-suspended-service-to-pirate-app-210315/ [Accessed 28 November 2022].

[25] Maxwell, A. (2021) *Pirate TV Streaming App Mobdro Disappears, Users in Mourning*. [online] Torrent Freak. Available from: https://torrentfreak.com/pirate-tv-streaming-app-mobdro-disappears-users-in-mourning-210215/ [Accessed 28 November 2022].

[26] Mehra, S.K. (2011) Keep America Exceptional! Against Adopting Japanese and European-Style Criminalization of Contributory Copyright Infringement. *Vanderbilt Journal of Entertainment and Technology Law*, 13 (4).

[27] Mi, X. et al. (2019) Resident Evil: Understanding Residential IP Proxy as a Dark Service. In *2019 IEEE Symposium on Security and Privacy (SP)*. San Francisco: IEEE, pp. 1185–1201.

[28] Mi, X., Tang, S., Li, Z., Liao, X., Qian, F., and Wang, X. (2021) Your Phone is My Proxy: Detecting and Understanding Mobile Proxy Networks. In *Proceeding of ISOC Network and Distributed System Security Symposium (NDSS), 2021*. DOI: 10.14722/ndss.2021.24008.

[29] Ninth Circuit Jury Instructions Committee (2017) 17.21. Derivative Liability—Contributory Infringement—Elements and Burden of Proof. In: Manual of Model Civil Jury Instructions [online]. Available from: https://www.ce9.uscourts.gov/jury-instructions/node/279 [Accessed 28 November 2022].

[30] Proxy Way. (2023) *10 Best Residential Proxies of 2023*. [online]. Available from: https://proxyway.com/best/residential-proxies

[31] Snigdha, B. (2022) Top Streaming Statistics for 2022. [online] SaaS Worthy. Available from: https://www.saasworthy.com/blog/top-streaming-statistics/[Accessed 28 November 2022].

[32] Tilly, J. M. (2008) Perfect 10 v. Visa: the future of contributory copyright infringement. *Oklahoma Law Review*, 61 (4), pp. 865–890.

[33] Tosun, A., De Donno, M., Dragoni, N., and Fafoutis, X. (2021) RESIP Host Detection: Identification of Malicious Residential IP Proxy Flows. In *2021 IEEE International Conference on Consumer Electronics (ICCE)*. Las Vegas: IEEE, pp. 1–6.

[34] Turcotte, J. (2021) *Disrupting Attacker Value Propositions in Residential Networks*. [online] Doctoral dissertation, Worcester Polytechnic Institute. Available from: https://digital.wpi.edu/downloads/1r66j4181 [Accessed 28 November 2022].

[35] Williams, A. (2018) *Mobdro: the app that wants to take on Kodi for a shot at the streaming crown*. [online] Tech Radar. Available from: https://www.techradar.com/news/mobdro-the-app-that-wants-to-take-on-kodi-for-a-shot-at-the-streaming-crown [Accessed 28 November 2022].

DOI 10.5817/MUJLT2023-2-4

PATENT-ELIGIBLE INVENTION REQUIREMENT UNDER THE EUROPEAN PATENT CONVENTION AND ITS IMPLICATIONS ON CREATIONS INVOLVING ARTIFICIAL INTELLIGENCE

by

LIVA RUDZITE-CELMINA *

Artificial Intelligence and its subfield, Machine Learning are areas of computer science; thus, they rely on algorithms, models, computer programs and software applicable in numerous areas. Since respective creations involve resources and shift from hardware to software, there is an incentive to protect them legally. Due to their dual nature, the algorithms, models, computer programs, and software might be too "technical" to avail copyright protection but not "technical" enough for a patent. Whereas trade secret protection might not be sufficient means of protection in all cases. The article explores the issues and, as its main argument, builds further on the academic proposals on the sui generis mechanism. It also suggests certification as the potential approach to avail the desired protection instead of diluting the existing protection frameworks. An alternative would be to lie on the complete availability or trade secret protection, none of which would be an adequate balance.

KEY WORDS

Artificial Intelligence, Invention, Patent, Certification

1. INTRODUCTION

Under the Convention on the Grant of European Patents [1] (hereinafter - the EPC), for the claimed subject to be deemed an "invention", it should

* livarud@ut.ee, Ph.D. student at the School of Law of the University of Tartu, Ülikooli 18, 50090 Tartu, Estonia

1 *The Convention on the Grant of European Patents*, 5 October 1973.

relate to a "technical" field or "technology".[2] "Technology" is understood in its conventional meaning relating to industrial methods of production, preparation and trade,[3] also comprising areas that emerge from the established "technical" fields, such as biotechnology.[4]

Artificial Intelligence[5] (hereinafter – AI) and its subfield Machine Learning (hereinafter – ML), due to their specifics, have applications in numerous fields and facilitate the switch from hardware to software. AI and ML are also based on programming models and algorithms and are an area of computer science.[6] Besides, the core value of programming models and algorithms is their behaviour or functional effect that might involve considerable resources, including know-how, to be built from scratch.[7]

The European Parliament has stated that patent protection is a key mechanism for incentivizing innovation for creations involving ML and facilitating their interoperability.[8] The Boards of Appeal of the European Patent Office (hereinafter – EPO BA) have stipulated that treating creations involving ML differently than other computer-implemented inventions would require convincingly demonstrate their difference that has not been presented yet but is not excluded in the future.[9] In this regard, the article mainly focuses on the patentability of the outlined aspects of ML in their

---

2 Nack, R. (2014) Inventions and their amenability to patent protection. In: Haedicke, M. W., Timmann, H. (eds.) *Patent Law: A Handbook on European and German Patent Law*, München: Beck, p. 81.

3 *Ibid*.

4 Decision of 9 December 2010, Broccoli/PLANT BIOSCIENCE, G0002/07, EP:BA:2010:G000207.20101209, paragraphs 6.4.1.-6.4.2.3.

5 There is no united definition of Artificial Intelligence; however, see, for instance: The Joint Institute for Innovation Policy, IViR – University of Amsterdam (2020) Trends and Developments in Artificial Intelligence. Challenges to the Intellectual Property Rights Framework. Final Report for the European Commission. Publication Office of the European Union. Available from: `https://op.europa.eu/en/publication-detail/-/publication/394345a1-2ecf-11eb-b27b-01aa75ed71a1/language-en` [Accessed 30 December 2022], pp. 21-27.

6 The European Patent Office. *Guidelines for Examination G-II, 3.3.1 Artificial intelligence and machine learning*. Available from: `https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_ii_3_3_1.htm` [Accessed 10 December 2022].

7 Samuelson, P. et al. (1994) A Manifesto Concerning Legal Protection of Computer Programs. *Columbia Law Review*, 94, Available from: `https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1783\&context=faculty_scholarship` [Accessed 30 December 2022], pp. 2316.-2326, 2333.

8 European Parliament (2020). *Motion for a European Parliament Resolution on intellectual property rights for the development of artificial intelligence technologies (2020/2015(INI))*. Available from: `https://www.europarl.europa.eu/doceo/document/A-9-2020-0176_EN.html` [Accessed 14 May 2023], paragraph 11.

9 Müller, M., EPO BA (2023). *EPO Boards of Appeal case law on AI-related inventions*. Presentation in: The European Patent Office. Conference on AI-related technologies: regulation, inventorship and patenting (JC01-2023). Available from: `https://www.epo.org/learning/training/details.html?eventid=16092` [Accessed 14 May 2023].

current capacity under the EPC and touches upon other intellectual property (hereinafter – IP) mechanisms to conclude on the comprehensiveness of the respective protection.

Creations and features that do not suffice the "technicality" requirement under Article 52 EPC are treated as abstract, analogous to mathematical methods rather than "technical". Furthermore, Article 52(2) and (3) EPC excludes algorithms "as such" from patentability. Creations involving ML that have applications in "non-technical" fields might also fall under the mentioned exceptions.

Algorithms that underlie ML are of dual nature, namely, entail both intellectual and functionality-facilitating aspects and may fall under exclusions stated in Article 52(2) and (3) EPC. The remaining IP mechanisms (copyright and related rights, database rights and trade secrets) might be used in some cases, but, at the same time, not provide sufficient protection in other occasions. Thus, the alternative is not to rely on IP protection, which might not be an incentive to innovate or to opt for protection as a trade secret, if possible, that would not incentivize technological progress.

The article explores these issues and follows the academic proposals of a *sui generis* mechanism as the potential approach to avail the desired protection.[10] Ideas expressed in those proposals are still relevant due to the rapid technological development and the existing IP framework. The article elaborates on the mentioned proposals and, as the main argument, with a preliminary overview, suggests the implementation of the certification, which would not require amending the EPC or copyright framework or diluting them. Instead, it would, in a technologically neutral manner, address an incentive to obtain the protection of the most valuable part of creation – behaviour or functional value – that reflects the intended effect and reason for building them. Additionally, it would protect creations involving ML in "non-technical" fields. Further preliminary details of the suggested certification mechanism are explored in the paper that is built upon this article.[11]

[10] Samuelson, P. et. al. (1994). A Manifesto Concerning Legal Protection of Computer Programs. *Columbia Law Review*, 94, Available from: `https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1783\&context=faculty_scholarship` [Accessed 15 December 2022]; Hughes, A. (2019) *The Patentability of Software. Software as Mathematics*. New York: Routledge, p.228; Norvig, P. (2020). Bridging AI's trust gaps, fireside chat 'Responsible AI'. Reuters Events Virtual Forum Momentum "Overcome Global Challenges and Build a Better Future through Technology". Available from: `https://www.dirse.es/events/momentum-virtual-forum/` [Accessed 14 May 2023] suggesting that certification, similarly to the electricity market, could be a solution for availing protection for creations involving ML.

[11] For further preliminary details of the proposed *sui generis* certification mechanism, see, Rudzite, L. (2023). Implications for the Inventive Step under the European Patent Convention

The article relies on descriptive, analytical and historical legal methods. The primary and secondary legal sources and case law are referred to evaluate the principal argument of the article. The paper is divided into six sections and sub-sections. The article starts with analyzing the specifics of ML in their current developmental stage to obtain an insight into technical aspects that might be seeking IP protection. The following sections observe the scope of the available protection under the current IP regimes, mainly focusing on the patent eligibility requirement under the EPC. Eventually, the article comes to the section where the proposed preliminary certification mechanism is analyzed as an alternative protection instrument.

The article, as its scope, addresses the patentability under the EPC. The analysis of copyright and trade secret regimes is limited to the law of the European Union (hereinafter - EU) that harmonizes them since the EU member states are parties to the EPC[12]. The article also does not elaborate on inventions created by AI, which falls into another analysis.[13]

2. MACHINE LEARNING

AI and its sub-field ML are a branch of computer science.[14] Because of the ability to process complex, large-scale, various data sets rapidly and due to the level of abstractness or generalization, ML have applications in numerous fields.[15] For instance, in economics,[16] linguistics[17] and others.

Contrary to traditional programming, a program is formed in ML when an algorithm iterates input and underlying statistical correlations between input and output.[18] Respectively, data and output form the program. In this

Related to the Increasing Application of Artificial Intelligence and Certification as *Sui Generis* Protection Mechanism for Creations Involving Artificial Intelligence. *International Comparative Jurisprudence*, 9(1), pp. 145-150.

[12] The European Patent Office (2022). *Member states of the European Patent Organisation*. Available from: https://www.epo.org/about-us/foundation/member-states.html [Accessed 30 December 2022].

[13] See, for example, Rudzite, L. (2022) Certifications as a Remedy for Recognition of the Role of AI in the Inventive Process. *International Comparative Jurisprudence*, 8(1), pp. 112-128.

[14] The European Patent Office. (2022) *Artificial Intelligence*. Available from: https://www.epo.org/news-events/in-focus/ict/artificial-intelligence.html [Accessed 10 December 2022].

[15] Sevahula, R. K. et al. (2020) State-of-the-Art Machine Learning Techniques Aiming to Improve Patient Outcomes Pertaining to the Cardiovascular System. *Journal of the American Health Association*, 9 (4), pp. 3. Available from: doi: 10.1161/JAHA.119.013924 [Accessed 10 December 2022].

[16] Decision of 6 March 2013, Marketing simulations/SAP, T 1954/08, EP:BA:2013:T195408.20130306, paragraph 6.

[17] Decision of 21 November 2014, Classification/BDGB ENTERPRISE SOFYWARE, T 1358/09, EP:BA:2014:T135809.20141121, paragraph 5.2.

[18] Esteva, A., Robisquet, A., Ramsundar, B. (2019) A guide to deep learning in healthcare. *Nature Medicine*, 25 (1), p. 24. Available from: doi: https://doi.org/10.1038/s41591-018-0316-z [Accessed 10 December 2022].

regard, an effect of the intended program or its behaviour, particularly in ML, is a representation not solely of the code but instead reflects the correlation between the data and coded procedures of using data.[19] The more complex form of ML, such as neural networks and deep learning, the more abstract the effect of a program becomes, moving away from narrowly coded outcomes.[20]

Delineating, the basis of the ML or a "core"[21] is an algorithm.[22] An algorithm is a sequence of methodological, cognitive commands to reach the outcome.[23] In other words, an algorithm dictates an internal logic of operations.[24] In ML, algorithms serve as steps taken to enable learning from data and to perform a resulting model.[25] Types of ML algorithms are, for instance, logistic regression, artificial neural network, and others.[26] An algorithm might involve mathematical activities and can be expressed mathematically[27] and in a programming language.[28] In this regard, algorithms, including ML algorithms, are commonly referred to as "mathematical algorithms" or "computational models."[29] Nevertheless, the behaviour of a system lies in an algorithm, the essence of which exceeds

[19] Lee, J. A., Hilty, R. M., Liu, K.C. (eds.) (2021) *Artificial Intelligence & Intellectual Property*. Oxford: Oxford University Press, pp. 1, 26.

[20] Kuman, U. et al. (2019) Deep Learning for Healthcare Biometrics. In: Kisku, D. R., Gupta, P., Sing, J. K. *Design and Implementation of healthcare biometric systems*. Pennsylvania: IGI Global. Available from: doi: 10:4018/978-1-5225-7525-2.ch004 [Accessed 10 December 2022], pp. 79.

[21] The European Patent Office. (2018) *Patenting Artificial Intelligence*. Conference Summary, EPO Munich, 30 May, pp. 5-6. Available from: https://documents.epo.org/projects/babylon/acad.nsf/0/D9F20464038C0753C125829E0031B814/$FILE/summary_conference_artificial_intelligence_en.pdf [Accessed 10 December 2022].

[22] Luginbuehl, S. (2021) Patent Protection of Inventions Involving Artificial Intelligence. In: Niklas Bruun et al. (eds.) *Transition and Coherence in Intellectual Property Law. Essays in Honour of Annette Kur*. Cambridge: Cambridge University Press, p. 192.

[23] Chisum, D. S. (2013) The Patentability of Algorithms. In: Richard S. Gruner (ed.) *Intellectual Property and Digital Content. Critical Concepts in Intellectual Property Law*. Volume II. Northampton: Edward Elgar Publishing Ltd., p.43.

[24] Fisher, M. (2020) Software-related inventions. In: Tanya Aplin (ed.) *Research Handbook on Intellectual Property and Digital Technologies*. Northampton: Edward Elgar Publishing Ltd., p. 278.

[25] Sevahula, R. K. et. al. (2020). State-of-the-Art Machine Learning Techniques Aiming to Improve Patient Outcomes Pertaining to the Cardiovascular System. *Journal of the American Health Association*, 9(4), 18 February. Available from: doi: 10.1161/JAHA.119.013924 [Accessed 10 December 2022]. p. 1.

[26] *Ibid*.

[27] Maini, V., Sabri, S. (2017) *Machine Learning for Humans*. Available from: https://everythingcomputerscience.com/book/Machine\%20Learning\%20for\%20Humans.pdf

[28] Newell, A. (1986) Response: The Models are Broken, the Models are Broken. *University of Pittsburg Law Review*, 47 (1023), pp. 1029.

[29] Pilger, J., Gall, I. (2022) AI and CI simulations: prospects for patenting inventions in Europe. In Adam Jolly (ed.) *Winning with IP: Managing Intellectual Property Today. Value and Growths from Ideas and Improvements*, 2nd. ed. Coventry: Novaro Publishing, p. 65.

solely abstract mathematics.[30] Namely, non-numerical or non-mathematical elements or know-how might impact the behaviour of a system.[31]

The algorithm is incorporated into a computer program to enable algorithms to be run on a computer to execute specific commands.[32] Since algorithms are more abstract than computer programs,[33] a computer program might be formed from multiple algorithms, each of which serves its task.[34] Albeit an algorithm expressed in a source code is an integral aspect of a computer program, other components enable a physical medium (a computer) to execute a task, for example, files, compilers and others. Hence, a computer program implements the logic of an algorithm in a manner that a physical medium (hardware) can execute.[35]

The term "computer program" sometimes is interchangeably defined in literature as "software",[36] but they are not the same.[37] The software usually combines numerous computer programs. Hence, the software can be a single computer program but not *vice versa*.[38] Not all ML applications are *prima facie* related to technical sciences but also comprise other disciplines. Since ML algorithms might form part of a software or a computer program, they might be interchangeably associated with abstract mathematics.[39] However, not all aspects of a computer program or software, as previously mentioned,

[30] Turkevich, L. R. (1995) An end to the 'Mathematical Algorithm' Confusion. *European Intellectual Property Review*, 17 (2), p. 92.

[31] Hughes, A. (2019) *The Patentability of Software. Software as Mathematics*. New York: Routledge, p.23.

[32] Zeidman, B. (2011) *The Software IP Detective's Handbook. Measurement, Comparison and Infringement Detection*. Boston: Pearson Education Inc., p. 35.

[33] Newell, A. (1986) Response: The Models are Broken, the Models are Broken. *University of Pittsburg Law Review*, 47 (1023), p. 1029.

[34] Foss-Solbrekk, K. (2021) Three routes to protecting AI systems and their algorithms under IP laws: The good, the bad and the ugly. *Journal of Intellectual Property Law & Practice*, 16 (3), pp. 254.

[35] Zeidman, B. (2011) *The Software IP Detective's Handbook. Measurement, Comparison and Infringement Detection*. Boston: Pearson Education Inc., p.36., 43, 94.

[36] Pilger, J., Gall, I. (2022). AI and CI simulations: prospects for patenting inventions in Europe. In Adam Jolly (ed.) *Winning with IP: Managing Intellectual Property Today. Value and Growths from Ideas and Improvements*, 2nd. ed. Coventry: Novaro Publishing, p. 63.

[37] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, *Official Journal of the European Union* (32009L0024) 5 May, Recital 10. Available from: `https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX\%3A32009L0024` [Accessed 12 December 2022].

[38] Hughes, A. (2019) *The Patentability of Software. Software as Mathematics*. New York: Routledge, p. 20-21.

[39] Hughes, A. (2019) *The Patentability of Software. Software as Mathematics*. New York: Routledge, p. 165-200.

are formed by numerical algorithms. Thus, the unique behaviour of the ML algorithm might also be related to non-mathematical aspects.[40]

It can be concluded that the application of ML is possible in various fields, not all of them being, *prima facie*, "technical". Additionally, building ML requires numerous steps that could involve mathematical, non-mathematical aspects, "technical" and "non-technical" steps. Nonetheless, they all form a ML algorithm. Application of ML in the resulting creation, for instance, building a computer program or software, forms their resulting behaviour (functional value). Due to the dual nature of algorithms, application of them in building an end product might accord difficulties in availing IP protection. Thus, having explored the essence of ML, the legal protection opportunities under the existing IP regimes have to be observed.

3. PROTECTION UNDER REGIMES OF COPYRIGHT AND ITS RELATED RIGHTS, AND *SUI GENERIS* DATABASE RIGHTS FOR CREATIONS INVOLVING ML

Copyright protection in the EU pertains to "literary and artistic works"[41] comprising computer programs but excluding algorithmic behaviour (functional value).[42] Copyright protection in the EU pertains to the form of expression of a computer program (a textual part or a source code, object code and an assembly code), not to the protection of a functionality of a computer program that would rather reflect an idea.[43] Besides, copyright protection accords only to own original creation by an author (a person),

[40] Newell, A. (1986) Response: The Models are Broken, the Models are Broken. *University of Pittsburg Law Review*, 47 (1023). pp. 1024, 1033.

[41] 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 Union* (32001L0029) 22 June. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex\%3A32001L0029` [Accessed 12 December 2022]; Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, *Official Journal of the European Union* (32019L0790) 17 May. Available from: `https://eur-lex.europa.eu/eli/dir/2019/790/oj` [Accessed 12 December 2022]; *the Berne Convention for the Protection of Literary and Artistic Works*, 9 September 1886 (TRT/Berne/001). Available from: `https://www.wipo.int/wipolex/en/text/283693` [Accessed 12 December 2022], Article 2(1); Hugenholtz, B., Quintais, J., P. (2021) Copyright and Artificial Creations: Does EU Copyright Law Protect AI-Assisted Output? *IIC – International Review of Intellectual Property and Competition Work*, 52(01), pp. 5.

[42] Directive 2009/24/EC, Article 1, Recital 11.

[43] Judgement of 22 December 2010, Bezpečnostní softwarová asociace, C-393/09, EU:C:2010:816, paragraphs 28-42; Judgement of 2 May 2012, SAS Institute, C-406/10, EU:C:2012:259, paragraphs 38-46.

excluding mathematical concepts *per se*[44] and realizations directed solely by "technical" functionality without aesthetic and individual choices.[45]

Concluding, the "technicality" of the algorithm is a matter on a case-by-case basis. ML algorithms can be built not with aesthetic but "technical" considerations behind that, even though applied in a "non-technical" field. Furthermore, there might also be cases where some computer programs or software algorithms serve "technical" purposes, some do not, and the application is in a "non-technical" field. Hence, these algorithms might be too "technical" and lack copyright protection which could also influence the protection of a computer program or software. Clarity towards copyright protection of algorithms is essential since the decompilation of computer programs for interoperability purposes in the EU is allowed and deprives only building similar computer programs[46] but does not protect from building a similar expression (behaviour).

It is essential to protect not only the copying of a code, a computer program, or software but also the replication of their behaviour (building of which involves know-how or an actual value of creation) and used for commercial purposes. Namely, building the said creation from scratch involves resources. However, it is not arduous to clone the effect after it has been expressed.[47] The issue with ML algorithms and models, especially if generalizable, is the cloning of their functionality by other ML algorithms[48] and applications in non-protected areas.

Furthermore, *sui generis* database rights[49] protect only the compilation of data but not processing tools that are algorithms in the case of ML. In this regard, even though trained on data, the ML model might not accord the respective protection, even as a "work".[50] Nevertheless, in the case of the

[44] Judgement of 13 November 2018, Levola Hengelo, C-310/17, EU:C:2018:899, paragraph 39.

[45] Judgement of 11 June 2020, Brompton Bicycle, C-833/18, EU:C:2020:461, paragraphs 22-27.

[46] Directive 2009/24/EC, Article 6.

[47] Samuelson, P. et. al. (1994). A Manifesto Concerning Legal Protection of Computer Programs. *Columbia Law Review*, 94, Available from: `https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1783\&context=faculty_scholarship` [Accessed 15 December 2022], pp. 2316.-2326, 2333.

[48] Teitelman, D., Naeh, I., Mannor, S. (2020) Stealing Black-Box Functionality Using the Deep Neural Tree Architecture. ArXiv. Available from: `https://doi.org/10.48550/arXiv.2002.09864`[Accessed 30 December 2022].

[49] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, *Official Journal of the European Union* (31996L0009) 27 March. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A01996L0009-20190606` [Accessed 30 December 2022], Article 1(2), (3).

[50] Kelli, A. et al. (2020) Impact of Legal Status of Data on Development of Data-Intensive Products: Example of Language Technologies. In: Carlo Amatucci et. al. (eds.). Legal Science: Functions, Significance and Future in Legal Systems II, the 7th International Scientific

ML model, only the resulting composition when an algorithm iterates data is protected not its constituting parts as the algorithm *per se*.

Additionally, trade secret protection is also not a practical option for software, a computer program, or an algorithm because their behaviour (actual commercial value), when rendered public as a product or part of it, is visible; thus, mimicable.[51] Besides, there is no *consensus* of whether trade secret protection belongs to IP realm.[52] Thus, trade secret protection might not provide an adequate compensation mechanism in these cases. Furthermore, non-disclosure of software, a computer program, or an algorithm might hinder technological progress.

Hence, considering the resources involved in creations that apply ML, an adequate compensatory mechanism is necessary.[53] Since copyright and trade secret protection might not in all cases serve as an effective mechanism, protection opportunities under the patent protection of the EPC should be considered.

4. ELIGIBLE INVENTION UNDER THE EUROPEAN PATENT CONVENTION

4.1. ARTICLE 52 OF THE EPC

Under Article 52, the EPC does not *expressis verbis* define the term "invention" but states the list of exclusions. According to Travaux Préparatoires,[54] the term "computer program" was not defined *verbatim* but associated more with the "mathematical application of a series of logic" and not more than an exclusion of a mathematical method. Later a separate paragraph unequivocally excluding all of the listed exclusions "as such" (intellectual

Conference of the Faculty of Law of the University of Latvia, Riga, 16-18 October. Riga: University of Latvia Press, pp. 390.

51 Samuelson, P. et. al. (1994). A Manifesto Concerning Legal Protection of Computer Programs. *Columbia Law Review*, 94, Available from: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1783\&context=faculty_scholarship [Accessed 15 December 2022], pp. 2333.

52 Foss-Solbrekk, K. (2021) Three routes to protecting AI systems and their algorithms under IP laws: The good, the bad and the ugly. *Journal of Intellectual Property Law & Practice*, 16 (3)., pp. 256-258.

53 Op. cit., p. 258.

54 The European Patent Office. (1973) *Article 52 E Travaux Préparatoires*. Available from: http://webserv.epo.org/projects/babylon/tpepc73.nsf/0/719AC39AA49A7563C12574270049EB9E/$File/Art52eTPEPC1973.pdf [Accessed 15 December 2022], pp. 58-59.

creations) was proposed.[55] Overall, the process of including the negative definition and exclusions was rather political than legal.[56]

For a creation to be identified as an "invention", it has to have a "technical character" – 1) relates to a "technical" field; 2) is related to a "technical" problem; 3) has "technical" features that are intrinsically linked with the patent claims.[57] The same also applies to inventions involving ML.[58]

4.1.1 Technical Field

The "technical field" is attributable only to "technology". Namely, an "invention" has to present novel skills that evolve from the conventional "technical" fields related to industrial methods of production, preparation and trade, like biotechnology[59] that require craftsmanship instead of intellectual activity. Hence, "non-technical" fields (economics, social sciences and others) fall outside the EPC.[60] The aspect has been outlined, for instance, in the case T 0931/95,[61] where the claim of the innovative actuarial algorithm was rejected since it was related to the field of economics that is not a "technical" field under the EPC.

However, an invention only has to be "technical in character" regardless of the field of technology (even graphical design if it comprises "hardware" or other "technical" means). Thus, the criterion of the "technical" invention is rather formal in comparison to the "inventive step" (Article 56 EPC).[62]

As was outlined previously, ML have applications in "technical" fields and other areas. Thus, as also the EPO confirms,[63] regardless of whether a creation involving ML has inventive nature, despite the level of generalization and scope of applications, it will not be granted patent

[55] Decision of 5 October 1988, Document abstracting and retrieving, T 0022/85, EP:BA:1988:T002285.19881005, paragraph 2.

[56] Nack, R. Inventions and their amenability to patent protection. In: Haedicke, M. W., Timmann, H. (eds.) *Patent Law: A Handbook on European and German Patent Law*, pp. 124; Nägerl, J. S. H., Walder-Hartmann, L. Inventions and their amenability to patent protection. In: Haedicke, M. W., Timmann, H. (eds.) *Patent Law: A Handbook on European and German Patent Law*, pp 148.

[57] The European Patent Office. *Guidelines for Examination G-I, 2 (ii). Further requirements of an invention*. Available from: `https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_i_2.htm` [Accessed 15 December 2022].

[58] The European Patent Office. *Artificial Intelligence*.

[59] Nack, R. Inventions and their amenability to patent protection. In: Haedicke, M. W., Timmann, H. (eds.) *Patent Law: A Handbook on European and German Patent Law*, p. 81.

[60] *Op. cit.*, pp. 102.-103.

[61] Decision of 8 September 2000, Control of a Pension System/PBS Partnership, T 0931/95, EP:BA:2000:T093195.20000908, paragraph 8.

[62] Nack, R. Inventions and their amenability to patent protection. In: Haedicke, M. W., Timmann, H. (eds.) *Patent Law: A Handbook on European and German Patent Law*, pp. 73.

[63] The European Patent Office. *Artificial Intelligence*.

protection if an application of the said creation pertains to the field that is not "technical".[64] Namely, the patent claim cannot be too general. The claim should be narrow and specific enough to fulfil another patentability requirement - sufficient disclosure according to Article 83, 84 of the EPC.[65] In other words, even if a creation involves, for instance, the processing of data in a "technical" field, but the application of creation is not specific enough, patent protection might be denied as falling in the ambit of an algorithm, computer program or software "as such".[66]

4.1.2 Technical Problem

Inventions solving a "technical" problem result from a task given by a creator that can be solved by "technical" means.[67] Namely, decisive are distinguishing features of an invention that are deemed to be new, inventive in a "technical" field.[68] Besides, only the presence of an "improvement of teaching technique" is not considered "technical" under the EPC.[69] Furthermore, the distinction should be made between the "commercial application of an invention" and an underlying solvable problem since one of them might not be "technical".[70]

To evaluate the "technicality" of the claimed invention, the EPO follows the "achievement-related approach" (contribution to the art in a "technical" field).[71] It means that, for instance, in the computer-related field, the invention presents an effect that goes beyond the basic interaction between software and hardware on which it is run in cases where control over

[64] In contrast, Decision of 15 July 1986, Computer-related invention/VICOM, T 0208/84, EP:BA:1986:T020884.19860715, paragraphs 5-6; Decision of 5 September 1988, Computer-related invention/IBM, T 0115/85, EP:BA:1988:T011585.19880905, paragraphs 9-11.

[65] Decision of 19 January 2017, T 0625/11, EP:BA:2017:T062511.20170119, paragraphs 7.2.6., 8.1.

[66] Decision of 21 September 2012, Classification method/COMPTEL, T 1784/06, EP:BA:2012:T178406.20120921, paragraphs 4-6.

[67] Nack, R. Inventions and their amenability to patent protection. In: Haedicke, M. W., Timmann, H. (eds.) *Patent Law: A Handbook on European and German Patent Law*, pp. 77.

[68] The European Patent Office. *Guidelines for Examination G VII 5.4.1. Formulation of the objective technical problem for claims comprising technical and non-technical features*. Available from: `https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_vii_5_4_1.htm` [Accessed 5 August 2023]; Decision of 25 April 1989, Coloured disk jacket, T 0119/88, EP:BA:1989:T011988.19890425, paragraph 4.

[69] Decision of 3 July 1990, Marker, T 0603/89, EP:BA:1990:T060389.19900703, paragraph 2.8.

[70] EPO BA T 0119/88, paragraph 4.2. B.

[71] Nack, R. Inventions and their amenability to patent protection. In: Haedicke, M. W., Timmann, H. (eds.) *Patent Law: A Handbook on European and German Patent Law*, pp. 72-73; Decision of 10 March 2021, Pedestrian Simulation, G0001/19, EP:BA:2021:G000119.20210310, paragraph 125.

the computer is claimed.[72] In other words, "any device", including the computer, has a "technical character"; thus, without a further achievement or "further technical effect", all respective creations would be deemed as patent eligible under the EPC.[73] However, this "further technical effect" might be fulfilled by adding, for example, another physicality element (like a storage medium) that, substance-wise, is not necessarily novel or improving an inner functioning of the computer.[74]

In this regard, it is deemed that the "further technical effect" aspect is not cumbersome for computer programs to comply with because the reference to the involvement of any physical item apart from the computer in the claim is sufficient.[75] Hence, it might be concluded that difficulty for computer programs appears in the further aspect (second hurdle) of patentability, such as an "inventive step".[76] However, the EPO, in its latest landmark case that is also relevant to computer-implemented inventions, has identified an intermediary step, the purpose of which is to determine the existence of "technical teaching" of a claimed creation and prevent them from the further evaluation (state of the art).[77] Nevertheless, the approach entails the mentioned contributions to a "technical" field; hence, only those claims that relate to specific fields might reach the stage where their inventiveness will be evaluated.[78]

Additionally, the claimed invention should comprise a "technical" problem that is solved by innovative "technical" means.[79] There must be a causal link between an inventive solution by "technical" means and a previously existing problem in a related field. In other words, claimed "technical" means cannot only solve a "non-technical" issue.[80] Nonetheless, "non-technical" means such as mathematical algorithms might be involved to solve a "technical" problem to yield a "technical character".[81] Besides, even

[72] Decision of 12 May 2010, Programs for computers, G 0003/08, EP:BA:2010:G000308.20100512, paragraph 10.2.4-10.4.

[73] Decision of 19 March 2021, Natural language to machine language translator/RAVENFLOW, T 2825/19, EP:BA:2021:T282519.20210319, paragraphs 5.1-5.4.

[74] EPO BA G 0003/08, paragraph 10.4.

[75] The European Patent Office. *Guidelines for Examination, G-II, 3.6. Programs for Computers*. Available from: `https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_ii_3_6.htm` [Accessed 14 May 2023].

[76] Nack, R. Inventions and their amenability to patent protection. In: Haedicke, M. W., Timmann, H. (eds.) *Patent Law: A Handbook on European and German Patent Law*, pp. 73; EPO BA G 0001/19, paragraph 38, 125.

[77] EPO BA G 0001/19, paragraphs 38-39.

[78] EPO BA T 0931/95, paragraph 7.

[79] Decision of 26 September 2002, Two identities/COMVIK, T 0641/00, EP:BA:2002:T064100.20020926, paragraph 5.

[80] *Ibid.*, paragraph 5.

[81] EPO BA T 1784/06, paragraphs 2.3., 3.3.

if features that can be deemed "technical" *per se* may still not contribute to an inventive step if they do not add to the solution of a "technical" problem.[82] Moreover, the prerequisite is not met if the claimed feature contributes to the "technical character" only for certain specific embodiments of the claimed invention.[83]

"Technical effects" can occur within the computer-implemented process (for instance, by specific adaptations of the computer or data transfer) and at the input and output stages. Input and output may appear at the beginning and end of a computer-implemented process and during its execution (namely, by receiving measurement data and sending control signals to a "technical" system).[84] Also, permissible is a "potential technical effect" unrelated to physical reality.[85]

"Technical contribution" is evaluated in each case separately since the EPO is not willing to concretize the term "technical" to leave room for future development.[86] In this regard, an invention might have "non-technical" features that are excluded from patentability under the EPC "as such" like algorithms, computer simulations (pure numerical input and output), without real or potential effect on the physical world and others.[87] However, these seemingly "non-technical" features might also contribute to the "technicality" of the invention that has to be evaluated in relation to the entire claimed invention (estimated "technical effect" impacted by each feature individually).[88] An invention might presumably have "technical" features that contribute or do not contribute to the "technical teaching" of the invention ("technical" solution for a "technical" problem).[89] Thus, only those "technical" and "non-technical" features are deemed "technical" that bring added value to creating the claimed invention.[90] The EPO does not relate to purely formal wording of a claim of "technical" and "non-technical" but evaluates their contribution in a substantive manner.[91]

[82] EPO BA G 0001/19, paragraph 80.
[83] *Ibid*., paragraph 84.
[84] Decision of 14 March 1989, Colour television signal, T 0163/85, EP:BA:1989:T016385.19890314, paragraph 2.
[85] EPO BA G 0001/19, paragraph 85, 88.
[86] *Ibid*., paragraphs 75, 141.
[87] EPO BA G 0003/08, paragraph 10.13.1; EPO BA T 1358/09, paragraph 5.5; EPO BA T 0163/85, paragraph 2.
[88] EPO BA G 0001/19, paragraph 33.
[89] *Ibid*., paragraph 61.
[90] *Ibid*., paragraphs 140, 142.
[91] The European Patent Office. *Guidelines for Examination G VII 5.4.1. Formulation of the objective technical problem for claims comprising technical and non-technical features*.

4.2. IMPLICATIONS FOR ML

From the previously mentioned derives that the creations involving ML, although inventive, may not be patent eligible. Thus, those creations fall outside the scope of the EPC. As further demonstrated, another issue for creations involving ML might be compliance with the "invention" and "technicality" requirements since they involve algorithms.

The terms "invention" and "technical" has not been implemented as explicitly explanatory within the EPC. The same pertains to standards such as the "technical" problem and the "further technical effect" that have been developed in case law.[92] As mentioned previously, the "technicality" of each feature, including algorithms, is evaluated on a case-by-case basis concerning the entire claimed invention because it not feasible to provide an exhaustive list of conditions under which "technicality" of the computer-implemented creation might solve "technical" problem.[93] For example, "improving reliability and predictability of data" is not a "technical effect".[94] Similarly, establishing a model *per se* is a mental act or a mathematical equation.[95] Novel structure of ML algorithm does not serve "technical" purpose.[96] In contrast, models and algorithms might produce a "technical effect" if, for instance, they are responsible for aiding to adapt the computer or its *modus operandi*, or on the "technical effect" of the produced results as well as on the accuracy of the model.[97] Besides, algorithms and software might be deemed contributing to "technical teaching" if there are "technical" considerations behind their design - they serve a "technical" purpose for the claimed invention.[98] An example would be an algorithm and software features contributing to the internal working of the computer, adapted to the internal functioning of a computer or its network.[99]

Albeit the EPO requires that the "technicality" of features is assessed in the context of the entire claimed invention[100], as the case law[101] of the EPO BA demonstrates, there might not be a *consensus* on the "technical" contribution of features, including algorithms. For instance, in case T 697/17,

[92] EPO BA G 0001/19, paragraphs 33, 65, 75.
[93] *Ibid*., paragraphs 33, 61, 67, 85, 140-142.
[94] Decision of 25 May 2020, Forecasting the value of a structured financial support/SWISS, T 1798/13, EP:BA:2020:T179813.20200525, paragraphs 2.10-2.11.
[95] EPO BA G 0001/19, paragraphs 105-106.
[96] Decision of 7 November 2022, Sparsely connected neural network/MITSUBISHI, T 0702/2020, EP:BA:2022:T070220.20221107, paragraphs 12., 12.1.
[97] EPO BA G 0001/19, paragraphs 110-111.
[98] *Op. cit*., paragraphs 112-113.
[99] Decision of 17 October 2019, SQL extension/MICROSOFT TECHNOLOGY LICENCING, T 0697/17, EP:BA:2019:T069717.20191017, paragraph 5.3.4.
[100] EPO BA G 0001/19, paragraph 33.
[101] EPO BA T 0697/17, paragraphs 5.3.3.-5.3.4

initially, the algorithm was evaluated as to be "non-technical" concerning the logical structure of the data in the database without physical implementation. However, afterwards, the "technicality" of the algorithm was admitted as adding value to the overall "technical teaching" of the claimed invention.

The "technicality" was also lacking for the classification algorithms due to the absence of "technical" implementation regardless of their individual properties.[102] The same applies to the pure calculation of the behaviour of a "technical" system. If the "technical effect" is claimed as numerical output, the distinguishing aspect is not the type of data[103] but their further application.[104]

Thus, functional (technical) aspects of a claimed invention should be explicitly described. "Non-technical" features *per se* do not contribute to the "technical teaching" of an invention.[105] In this regard, another or the "functionality approach", is suggested, according to which the "technicality" of each feature should be evaluated not in isolation but as a functional, sequential chain of steps that all lead towards the claimed invention. The approach is suggested as how the issue with "non-technical" aspects should be viewed and, probably, resolved.[106]

The EPO has stipulated that the already established and long-standing "contribution" or "problem-solution approach" should be applied to assess the "technicality" of features constituting a claimed invention.[107] Besides, the "technicality" of each element, as previously stated, should be evaluated concerning the invention as a whole.[108] Thus, the approach by the EPO already considers the evaluation of elements towards invention as a whole and already corresponds to the "functionality approach".

In this regard, components of a claimed computer-implemented invention (also comprises ML) that cannot be tied with the arrogated "technical teaching" will not be subject to patent. An example are the features relating to excluded subject matters under the EPC, like algorithms *per se*. There is a stand that the creation of an algorithm always involves "technical"

[102] EPO BA T 1784/06, paragraph 3.1.4.
[103] Decision of 31 May 1994, General purpose management system, T 0769/92, EP:BA:1994:T076992.19940531, paragraphs 3.2-3.3., 3.7-3.8, 3.10.
[104] EPO BA G 0001/19, paragraphs 120, 124, 137.
[105] *Op. cit.*, paragraph 30.
[106] Baldus, O. (2019) A practical guide on how to patent artificial intelligence (AI) inventions and computer programs within the German and European patent system: much ado about little. *European Intellectual Property Review*, 41(12), pp. 752.
[107] EPO BA G 0001/19, paragraph 61.
[108] *Op. cit.*, paragraph 32.

considerations.[109] However, the EPO has stated that "technical" concerns behind underlying algorithms and models are deemed "technical" only to the extent they facilitate a "technical contribution" to the particular (claimed) "technical" invention.[110]

The case law shows[111] that the EPO has developed the third approach, "mathematical equation", at least for computer-implemented inventions that consider the possibility of expressing the creation in mathematical formulations. Nonetheless, the mechanism appears to be self-opposing. Firstly, in T 1326/06, the EPO BA stated that even though the process is purely mathematical, there is a "technical effect" because it ensures a secure exchange of documents or is related to the specific use case; thus, renders the underlying mathematical algorithm "non-ordinary".[112]

Whereas, in T 702/2020, the EPO BA rejected the argument that the model differs from the prior structures and *per se* is a "technical effect" because it reduces the needed storage space and deemed that the claimed creations were "non-inventive". The EPO BA also stated that the behaviour of the modified model would be different and less generalizable than that of the fully-connected neural network.[113] The argument, however, does not follow the stand by the EPO that ML algorithms currently are hardly ever generalizable;[114] thus, the conclusion derives that currently there is almost always a specific purpose for that algorithm. Hence, it appears that the decisive factor is the "technicality" of the end product, not the algorithm, since the final claimed use case might change the perception of the algorithm.[115] The EPO BA did not accept the argument that the ML model "as such" fulfils the "technical" purpose because it facilitates the automation of tasks.[116] On the one hand, it appears that the issue was rather related to

[109] Foss-Solbrekk, K. (2021) Three routes to protecting AI systems and their algorithms under IP laws: The good, the bad and the ugly. *Journal of Intellectual Property Law & Practice*, 16 (3), pp. 252.

[110] EPO BA G 0001/19, paragraphs 63-64.

[111] For instance, EPO BA T 0702/2020, paragraph 14; Decision of 30 November 2010, RSA Schlüsselpaarberechnung/GIESECKE & DEVRIENT, T 1326/06, EP:BA:2010:T132606.20101130, paragraph 6.1.; Decision of 17 October 2007, Software distribution/FUJITSU, T 0953/04, EP:BA:2007:T095304.20071017, paragraph 3.3.; Decision of 30 May 2000, Crypthographie à clés publiques/FRANCE TELECOM, T 0027/97, EP:BA:2000:T002797.20000530, paragraph 3.

[112] EPO BA, T 1326/06, paragraphs 6.3., 7.2., 8.1., 9.1., 9.2.

[113] EPO BA, T 0702/2020, paragraph 14.1.

[114] Klenner-Bajaja, A., EPO (2023). What is AI and how does it work. Presentation in: The European Patent Office. Conference on AI-related technologies: regulation, inventorship and patenting (JC01-2023). Available from: `https://www.epo.org/learning/training/details.html?eventid=16092` [Accessed 14 May 2023].

[115] EPO BA, T 1326/06, paragraphs 9.1., 9.2.

[116] EPO BA, T 0702/2020, paragraphs 3-6.3., 12., 18.

the description of claims, not the inventiveness since the EPO BA was not persuaded by the information provided in a case at hand not that there might be general "technicality" of neural networks.[117] On the other hand, the EPO BA did not support that ML algorithms belong to "technical" field *per se* and indicated that a concrete "technical" implementation was necessary.

Secondly, there has yet to be a *consensus* on whether an ML model has been created with artistic, mathematical or technical/functional considerations behind that.[118] It might depend on each case. For instance, if the main goal is to build an esthetically pleasing, non-functioning model, it would rather be artistic. If the task is not to draw but to express the model on its mathematical functions, then mathematical considerations are behind. Even so, aesthetics might play a minor part if the purpose is functionality. Additionally, just because the model might be expressed in various ways – by drawing, mathematical formula, or described by functions cannot be the decisive factor of classification.

The opposite conclusion would be contrary to the general perception of things. For example, the chair might be an invention based on the problem it solves – relieves sitting and other. Just because the chair might be depicted in various ways – as a drawing, by the function or even by a mathematical formula, does not automatically classify it as a mathematical function. Analogous goes for the computer-implemented invention where creation involves ML, but inventiveness is present, for instance, due to the final product. The end product could also be expressed in mathematical formula but does not change the fact that an invention is present.

It has been stated that only the execution of software in the end product does not reflect its true nature (symbolic aspect).[119] In other words, nowadays, the software is no longer limited to or built for concrete hardware but is created with a high level of abstraction.[120] On the one hand, as mentioned before, the EPC legal framework protects concrete inventions that have to involve "technicality"; hence, not addressing trivial creations or too general claims. On the other hand, since software nowadays entails a level of abstraction, obtaining a patent for a concrete use case does not protect from mimicking its behaviour or functional value in another expression.

The case law[121] of the EPO BA demonstrates that the EPO does not support suggestions to alter the scope of the EPC and comprise protection for

[117] *Op. cit.*, paragraphs 13.1., 16.2.-18.
[118] Hughes, A. (2019) *The Patentability of Software. Software as Mathematics*. New York: Routledge, p. 184, 199.-201.
[119] *Op. cit.*, p. 199.
[120] *Op. cit.*, p. 200.
[121] For instance, EPO BA G 0001/19.

algorithms[122] "as such" or to treat algorithms from the perspective of mental acts.[123] Additionally, the EPO BA has stipulated that applying creations involving ML differently than other computer-implemented inventions would require to convincingly demonstrate their distinction that has not been presented yet but is not excluded in the future.[124] Probably, this could be the use case if ML algorithm reaches the level of generalization; hence, embody "technicality" *per se*. Nonetheless, until then, as the analysis mentioned above demonstrates, creations involving ML can only obtain patent protection under the EPC if they comply with the "invention" and, consequently, "technicality" requirements. As a result, creations that cannot suffice those conditions (for instance, algorithms) fall outside the scope of the EPC. Albeit not "technical" enough for patent protection, creations, for example, algorithms, as mentioned before, might be too "technical" to avail copyright protection.

The EPO has stated that even a software process could be associated with or result in a "design".[125] In this regard, the visual design of software might be considered for protection. Nonetheless, as the EPO has stated, only the patent provides the protective framework for the respective behaviour.[126] The same applies to the "technicality" of designing programs (to attain functional results efficiently).[127] Hence, even if creations involving ML that cannot qualify for the patent protection, might avail protection under, for instance, copyright, their true value (behaviour or functional effect) would not be protected. Nonetheless, amending the said regimes would require fundamental changes in the core of the EPC, especially regarding "technical" fields and "technicality" of the invention that might not be preferred.

There is an incentive by creators to gain patent protection for computer-implemented inventions.[128] Besides, another vital aspect of algorithms, computer programs, and software is their "openness" as a

[122] EPO. *Patenting Artificial Intelligence*. Conference Summary, p. 6.

[123] Koorndijk, J. (2021) Adapting to innovations in artificial intelligence: AI as mental steps under the EPO. *European Intellectual Property Review*, 43(12), pp. 773.

[124] Müller, M., EPO BA (2023). *EPO Boards of Appeal case law on AI-related inventions*. Presentation in: The European Patent Office. Conference on AI-related technologies: regulation, inventorship and patenting (JC01-2023). Available from: `https://www.epo.org/learning/training/details.html?eventid=16092` [Accessed 14 May 2023].

[125] EPO BA G 0001/19, paragraphs 138, 143-144.

[126] The European Patent Office (2019). *Hardware and software*. Available from: `https://www.epo.org/news-events/in-focus/ict/hardware-and-software.html` [Accessed 14 May 2023].

[127] Samuelson, P. et. al. (1994). A Manifesto Concerning Legal Protection of Computer Programs. *Columbia Law Review*, 94, Available from: `https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1783\&context=faculty_scholarship` [Accessed 15 December 2022], pp. 2328-2329.

[128] EPO BA G 0001/19, paragraphs 63-64.

catalyst for scientific development, which is the opposite incentive of trade-secret protection or an overprotective patent regime.[129] Thus, a *sui generis* regime could be favoured.[130]

5. CERTIFICATION AS AN ALTERNATIVE APPROACH

Scholars have proposed building a *sui generis* mechanism to protect program behaviour[131] and AI systems.[132] The article builds on the suggested mechanisms and preliminarily develops them further. The author calls the proposed system "certification" since the term is known in other areas, as further explained, and it captures the essence of the approach.

The following should be considered as an initial and potential point of departure to address the problems described. As an intellectual endeavour, the author suggests that certification could be implemented as an alternative self-standing "patent-like" approach and provide enforceable rights paralleled with existing IP mechanisms similar to, for example, the utility models.[133] Namely, the certification depending on the aim to undergo this mechanism could provide the exclusive right to deter others from exploiting the protected creation commercially or, if chosen, serve as an only non-binding opinion that aids in proof-reviewing the creation (particularly, for intended patent claim under the EPC).

It could be conducted by an independent centralized or decentralized body or even rendered united with the proposed mechanism for AI in the EU.[134] From the procedural perspective, the proposed certification could be integrated into the existing IP mechanisms or, most likely, by an international agreement (covering Member States of the EPC) recognized as separate IP rights with its framework or as a hybrid approach combing both the

[129] Hughes, A. (2019) *The Patentability of Software. Software as Mathematics*. New York: Routledge, p.226.

[130] Samuelson, P. et. al. (1994). A Manifesto Concerning Legal Protection of Computer Programs. *Columbia Law Review*, 94, Available from: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1783\&context=faculty_scholarship [Accessed 15 December 2022], pp. 2421.

[131] *Op. cit.*, pp. 2426-2431.

[132] For example, Picht, G., Thouvenin, P. (2022) AI&IP: Theory to Policy and Back Again Policy and Research Recommendations at the Intersection of Artificial Intelligence and Intellectual Property. *SSRN*, 16 November. Available from: http://dx.doi.org/10.2139/ssrn.4278819 [Accessed 16 December 2022].

[133] The World Intellectual Property Organization. *Utility models*. Available from: https://www.wipo.int/patents/en/topics/utility_models.html [Accessed 16 December 2022].

[134] European Commission. (2021) Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. COM(2021)206 final (52021PC0206). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A52021PC0206 [Accessed 14 May 2023].

previously mentioned. Certification could be introduced in parallel with the EPC, like utility models, and copyright, like *sui generis* database rights, but in a hybrid form for protection in the desired region. The procedure for evaluating creation could be built upon the respective mechanism for the utility models with necessary individualization for the needs of the respective certification framework.

Namely, the certification could be a procedure that, in a non-binding manner, evaluates a creation for potential patentability (similarly to *mutatis mutandis* utility models) that, at the same time, also considers the possibility of protection under copyright and its related rights, *sui generis* database rights (whether creation (particularly an algorithm based on "technical" considerations) can be adjusted to attain such rights). In this regard, certification could have two approaches: 1) serve, if desired, purely as an impartial, expert opinion for protection purposes under the existing regimes (like Article 83 EPC[135]); 2) as an alternative protection mechanism if none of the existing ones could be an opportunity (EPC, copyright and its related rights, *sui generis* database rights). As a result, the respective transferable certificate could be issued. Rights arising from the certification would be granted after the evaluation and registration, which is different from copyright protection (which exists from the creation of the work).[136] Enforcement of the certifications could be most preferably based on the existing mechanism in the EU to avoid repetition.[137]

Considering that developments in computer science are rapid,[138] certification should not be lengthy. This would facilitate technological progress since it would, in a quick manner, allow obtaining protection against cloning. Trusting the certification for the EPO could be too cumbersome. In other words, the proposed certification foresees considering the necessity to

[135] For a more detail, see Rudzite, L. Certifications as a Remedy for Recognition of the Role of AI in the Inventive Process, pp. 132-135.

[136] Samuelson, P. et. al. (1994). A Manifesto Concerning Legal Protection of Computer Programs. *Columbia Law Review*, 94, Available from: `https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1783\&context=faculty_scholarship` [Accessed 15 December 2022], pp. 2426.

[137] Rudzite, L. (2022) Certifications as a Remedy for Recognition of the Role of AI in the Inventive Process. *International Comparative Jurisprudence*, 8(1), pp. 124. For a more detailed insight into procedural aspects of the proposed preliminary *sui generis* certification mechanism, see, Rudzite, L. (2023). Implications for the Inventive Step under the European Patent Convention Related to the Increasing Application of Artificial Intelligence and Certification as *Sui Generis* Protection Mechanism for Creations Involving Artificial Intelligence, *International Comparative Jurisprudence*, 9(1), pp. 147-148.

[138] Samuelson, P. et. al. (1994). A Manifesto Concerning Legal Protection of Computer Programs. *Columbia Law Review*, 94, Available from: `https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1783\&context=faculty_scholarship` [Accessed 15 December 2022], pp. 2376.

evaluate a creation quicker than used for a patent and determine, amongst others, whether other protection mechanisms exist. Thus, authorizing an independent body would be preferred.

Outlining the certification preliminarily, it would serve numerous independent purposes that could be opted for as exclusive or mutual upon the choice of the applicant:

1) It would allow the evaluation of the "technicality" of features of a creation confidentially. Namely, the certification would not require the deposit of an algorithm and underlying data. Instead, the certification would be based on the system of registration in a database and allow choosing between the protection under the said mechanism or serving as an opportunity to, in a non-binding manner, verify the creation. Depending on the chosen aim of the certification, the entry would be made public or kept non-disclosed.[139] The approach would enable obtaining beforehand information on the necessity to adjust the proposed patent application (also the sufficiency of description) or even involved elements if desired (in other words, to aid in proof-reviewing the already drafted application). Hence, it could facilitate both provisional patent protection and the patent granting (that gives long-term IP rights upon deciding on approving the application) under the EPC that otherwise could be lengthy if alterations in the patent application turned out as needed. The speed of granting a patent, especially in the framework of computer-implemented inventions, is essential since the technological progress is rapid and outperforms the period of the patent granting process.[140] The certification could also provide an impartial, written (expert) non-binding statement that the EPC allows on the workability (realizability) of the invention for sufficient disclosure purposes.[141] That might be particularly important for claims with "potential" or even "virtual technical effect".[142] The result of certification, undergone with the mentioned aim, will only be disclosed to the applicant. If, based on the evaluation, the applicant

[139] For a more detail, see Rudzite, L. (2023). Implications for the Inventive Step under the European Patent Convention Related to the Increasing Application of Artificial Intelligence and Certification as *Sui Generis* Protection Mechanism for Creations Involving Artificial Intelligence, *International Comparative Jurisprudence*, 9(1), pp. 148-150.

[140] Samuelson, P. et. al. (1994). A Manifesto Concerning Legal Protection of Computer Programs. *Columbia Law Review*, 94, Available from: `https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1783\&context=faculty_scholarship` [Accessed 15 December 2022], pp. 2376.

[141] Decision of 4 April 2012, Trace data/ SAP, T 1336/08, EP:BA:2012:T133608.20120404, paragraph 3.16.

[142] EPO BA G 0001/19, paragraph 97.

chooses not to seek protection under other IP mechanisms but opts only for certification as a self-standing right, the certified creation will be rendered public.[143]

2) It would protect features of a creation that cannot be subject to the existing regimes in the EU (copyright, *sui generis* database rights) and patent protection under the EPC (evaluated under the previous point or chosen in the certification application). These would primarily address creations involving ML in areas that *per se* are "non-technical", according to the understanding under the EPC. Secondly, the approach would allow obtaining protection for features of ML that could not be protected under copyright in the EU or patent under the EPC, such as the design of a computer program involving "technical" concerns. The protection could also relate to components that would be an invention *per se* (if claimed differently) but not to the claimed invention in the patent application, like algorithms as embedded tools[144] and others. Additionally, creators could opt only for protection by the certification as self-standing rights instead, for instance, a patent, if they desire so.[145]

3) Protection under the EPC covers only a concrete invention but does not deter cloning its behaviour (functionality) by applying a different methodology.[146] Moreover, there has been a proposal to establish an analogous regime for using ML models in inventions as is in second medical use cases.[147] Certification could address an incentive against cloning the actual value of creation or its resulting behaviour. This is particularly important if ML algorithms are generalizable or explainable[148] and could only partially avail the patent protection under the EPC.

[143] For a more detail, see Rudzite, L. (2023). Implications for the Inventive Step under the European Patent Convention Related to the Increasing Application of Artificial Intelligence and Certification as *Sui Generis* Protection Mechanism for Creations Involving Artificial Intelligence, *International Comparative Jurisprudence*, 9(1), pp. 148-150.

[144] EPO. *Patenting Artificial Intelligence*. Conference Summary, p. 6.

[145] For more detail see Rudzite, L. (2023). Implications for the Inventive Step under the European Patent Convention Related to the Increasing Application of Artificial Intelligence and Certification as *Sui Generis* Protection Mechanism for Creations Involving Artificial Intelligence, *International Comparative Jurisprudence*, 9(1), pp. 148-150.

[146] EPO. *Hardware and software*.

[147] EPO. *Patenting Artificial Intelligence*. Conference Summary, p. 6.

[148] Hashiguchi, M. (2017) The Global Artificial Intelligence Revolution Challenges Patent Eligibility Laws. *Journal of Business& Technology Law*, 13(1), 1 February, pp. 30-31.

Certificates would be registered and kept in the public registry. Namely, instead of storing algorithms as suggested in the repository[149] that, on the contrary, might disrupt the market,[150] the registration could be established building upon the certification in the electricity market (certificate acknowledges generation and ownership of a certain amount of electricity)[151] or approving the existence of creation, its creator, owner and other aspects. It could be combined with some sort of catalogue system (a database with documentation concerning the addressed creations) like under the EPC. Hence, if chosen, the certificate will confirm public disclosure in a protected form. Namely, once certified, creation will become prior knowledge. Thus, due to lack of novelty, the creation could not be, for instance, patented. The certified creation could be used only with a previous license (for a fee or gratuitous) from the certificate owner. Besides, certification could aid in keeping track of respective developments, like the resulting behaviour of the addressed creations.

Additionally, the current patent term is too long for computer-implement inventions because it is disrupting the developmental process.[152] Hence, in order not to affect the progress of the industry and to provide adequate protection, the certification term would be shorter than for patent under the EPC or utility models. There has been a suggestion of a term of three years or less for program compilations.[153] It should be noted that the significant aspect of building software and its components of it (that determine behaviour) is that most creations are incremental and result from the necessity to ensure interoperability.[154] Thus, provisionally, the multi-term (ranges of protection

[149] Samuelson, P. et. al. (1994). A Manifesto Concerning Legal Protection of Computer Programs. *Columbia Law Review*, 94, Available from: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1783\&context=faculty_scholarship [Accessed 15 December 2022], pp. 2427-2428.

[150] *Mutatis mutandis*, for example, Rudzite, L. (2022) Algorithmic Explainability and Sufficient Disclosure Requirement Under the European Patent Convention. *Juridica International*, 31/2022, pp. 130.

[151] Karakosta, Q., Petropoulou, D. (2021) The Electricity market: renewables targets, Tradeable Green Certificates and electricity trade. *SSRN*. Available from: http://dx.doi.org/10.2139/ssrn.3828184 [Accessed 30 December 2022], p.2. For more detail, see Rudzite, L. (2023). Implications for the Inventive Step under the European Patent Convention Related to the Increasing Application of Artificial Intelligence and Certification as *Sui Generis* Protection Mechanism for Creations Involving Artificial Intelligence, *International Comparative Jurisprudence*, 9(1), pp. 146, 148-150.

[152] Bainbridge, D. (2019). *Information Technology and Intellectual Property Law*. 7th ed. London: Bloomsbury Publishing, p. 534.

[153] Samuelson, P. et. al. (1994). A Manifesto Concerning Legal Protection of Computer Programs. *Columbia Law Review*, 94, Available from: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1783\&context=faculty_scholarship [Accessed 15 December 2022], pp. 2423.

[154] *Op. cit.*, pp. 2401-2405.

terms depending on the category of a creation) approach could rather be the possible direction. This would allow creators to acquire the fruits of their labour (competitive advantage) in the desired region.

The certification would not require legal amendments for the patent or copyright frameworks but rather legal adjustments to implement the certification. Besides, since the proposed certification would be a voluntary option as opposed to other mandatory systems, no additional, undesired administrative burden would be posed on the industry.[155] Those desiring to maintain the principle of the non-legal protection of their work would not be obliged to undergo the certification. In this regard, the certification would facilitate legal certainty and be technologically neutral and coherent. It would also promote disclosure and enrich general knowledge instead of forcing trade secret protection. It would not be under-protective (like a copyright that protects only limited parts of computer-related works) or overprotective (like a patent under the EPC that grants protection for twenty years, hindering further development, especially in fast-advancing fields like computer science) and aid in attracting investment.

6. CONCLUSION

Algorithms, models, computer programs and software have dual nature. They constitute a carrier of information and a machine *per se*. It places them at the intersection of copyright, trade secrecy in the EU, patent protection under the EPC and incentives for technological progress.

The current regimes under-protect the actual value – behaviour (why they are being built) – of algorithms, models, computer programs and software. In other words, only a patent (not copyright) protects the said behaviour but to the extent of the claimed invention. The stand by the EPO regarding the evaluation of differences between creations involving ML and computer-implemented inventions might change upon reaching generalizability for ML algorithms that, as a result, may embody "technicality" *per se*.

The patent limits protection only to "technology" fields. Thus, without protection, applications in "non-technical" fields, regardless of whether the underlying algorithms, models, computer programs and software otherwise, would aid in forming an invention and accord behavioural (functional value) protection. Furthermore, even application for "technical' fields does not guarantee the said protection.

[155] Rudzite, L. Rudzite, L. (2022) Certifications as a Remedy for Recognition of the Role of AI in the Inventive Process. *International Comparative Jurisprudence*, 8(1), pp. 124.

Besides, the functionality of ML algorithms and models, as well as computer programs and software that incorporate them, might be cloned by other ML algorithms and applications in areas not protected by IP rights. Consequently, protection for the respective behaviour (functional value) might not be availed under the current IP regimes.

Since widening the EPC scope and granting patent protection for algorithms "as such" would require the fundamental changes of the EPC that the EPO has not supported yet, the article preliminarily develops further on the proposed *sui generis* mechanism suggesting the implementation of certification as a self-standing instrument. The certification would allow confidentially and voluntarily to prematurely evaluate the patent eligibility of the creation under the EPC and adjust it accordingly if necessary. Besides, the certification would also avail protection similar to the case with the utility models for those features and creations that might not obtain a patent under the EPC, copyright or other IP mechanism. Thus, the certification would not overprotect the said creations or dilute the existing legal regime but, instead, would provide the mechanism to balance the involved interests.

LIST OF REFERENCES

[1] Bainbridge, D. (2019). *Information Technology and Intellectual Property Law*. 7th ed. London: Bloomsbury Publishing.

[2] Baldus, O. (2019) A practical guide on how to patent artificial intelligence (AI) inventions and computer programs within the German and European patent system: much ado about little. *European Intellectual Property Review*, 41(12).

[3] Chisum, D. S. (2013) The Patentability of Algorithms. In: Richard S. Gruner (ed.) *Intellectual Property and Digital Content. Critical Concepts in Intellectual Property Law*. Volume II. Northampton: Edward Elgar Publishing Ltd.

[4] Decision of 7 November 2022, Sparsely connected neural network/MITSUBISHI, T 0702/2020, EP:BA:2022:T070220.20221107.

[5] Decision of 19 March 2021, Natural language to machine language translator/RAVENFLOW, T 2825/19, EP:BA:2021:T282519.20210319.

[6] Decision of 10 March 2021, Pedestrian Simulation, G 0001/19, EP:BA:2021:G000119.20210310.

[7] Decision of 25 February 2020, Forecasting the value of a structured financial support/SWISS, T 1798/13, EP:BA:2020:T179813.20200525.

[8] Decision of 17 October 2019, SQL extension/MICROSOFT TECHNOLOGY LICENCING, T 0697/17, EP:BA:2019:T069717.20191017.

[9] Decision of 19 January 2017, T 0625/11, EP:BA:2017:T062511.20170119.

[10] Decision of 21 November 2014, Classification/BDGB ENTERPRISE SOFYWARE, T 1358/09, EP:BA:2014:T135809.20141121.
[11] Decision of 6 March 2013, Marketing simulations/SAP, T 1954/08, EP:BA:2013:T195408.20130306.
[12] Decision of 21 September 2012, Classification method/COMPTEL, T 1784/06, EP:BA:2012:T178406.20120921.
[13] Decision of 4 April 2012, Trace data/ SAP, T 1336/08, EP:BA:2012:T133608.20120404.
[14] Decision of 9 December 2010, Broccoli/PLANT BIOSCIENCE, G 0002/07, EP:BA:2010:G000207.20101209.
[15] Decision of 30 November 2010, RSA Schlüsselpaarberechnung/GIESECKE & DEVRIENT, T 1326/06, EP:BA:2010:T132606.20101130.
[16] Decision of 12 May 2010, Programs for computers, G 0003/08, EP:BA:2010:G00 0308.20100512.
[17] Decision of 17 October 2007, Software distribution/FUJITSU, T 0953/04, EP:BA:2007:T095304.20071017.
[18] Decision of 26 September 2002, Two identities/COMVIK, T 0641/00, EP:BA:2002:T064100.20020926.
[19] Decision of 8 September 2000, Control of a Pension System/PBS Partnership, T 0931/95, EP:BA:2000:T093195.20000908.
[20] Decision of 30 May 2000, Crypthographie à clés publiques/FRANCE TELECOM, T 0027/97, EP:BA:2000:T002797.20000530.
[21] Decision of 31 May 1994, General purpose management system, T 0769/92, EP:BA:1994:T076992.19940531.
[22] Decision of 3 July 1990, Marker, T 0603/89, EP:BA:1990:T060389.19900703.
[23] Decision of 25 April 1989, Coloured disk jacket, T 0119/88, EP:BA:1989:T011988. 19890425.
[24] Decision of 14 March 1989, T 0163/85, Colour television signal, EP:BA:1989:T016385.19890314.
[25] Decision of 5 October 1988, Document abstracting and retrieving, T 0022/85, EP:BA:1988:T002285.19881005.
[26] Decision of 5 September 1988, Computer-related invention/IBM, T 0115/85, EP:BA:1988:T011585.19880905.
[27] Decision of 15 July 1986, Computer-related invention/VICOM, T 0208/84, EP:BA:1986:T020884.19860715.
[28] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, *Official Journal of the European*

Union (32019L0790) 17 May. Available from: https://eur-lex.europa.eu/eli/dir/2019/790/oj [Accessed 12 December 2022].

[29] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, *Official Journal of the European Union* (32009L0024) 5 May. Available from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX\%3A32009L0024 [Accessed 12 December 2022].

[30] 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 Union* (32001L0029) 22 June. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex\%3A32001L0029 [Accessed 12 December 2022].

[31] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, *Official Journal of the European Union* (31996L0009) 27 March. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A01996L0009-20190606 [Accessed 30 December 2022].

[32] Esteva, A., Robisquet, A., Ramsundar, B. A guide to deep learning in healthcare (2019) Nature Medicine, Vol. 25(1), January. Available from: doi: https://doi.org/10.1038/s41591-018-0316-z [Accessed 10 December 2022].

[33] European Commission. (2021) Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. COM(2021)206 final (52021PC0206). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A52021PC0206.

[34] European Parliament (2020). *Motion for a European Parliament Resolution on intellectual property rights for the development of artificial intelligence technologies (2020/2015(INI))*. Available from: https://www.europarl.europa.eu/doceo/document/A-9-2020-0176_EN.html [Accessed 14 May 2023].

[35] Fisher, M. (2020) Software-related inventions. In: Tanya Aplin (ed.) *Research Handbook on Intellectual Property and Digital Technologies*. Northampton: Edward Elgar Publishing Ltd.

[36] Foss-Solbrekk, K. (2021) Three routes to protecting AI systems and their algorithms under IP laws: The good, the bad and the ugly. *Journal of Intellectual Property Law & Practice*, 16 (3).

[37] Hashiguchi, M. (2017) The Global Artificial Intelligence Revolution Challenges Patent Eligibility Laws. *Journal of Business& Technology Law*, 13(1), 1 February.

[38] Hugenholtz, B., Quintais, J., P. (2021) Copyright and Artificial Creations: Does EU Copyright Law Protect AI-Assisted Output? *IIC – International Review of Intellectual Property and Competition Work*, 52(01).

[39] Hughes, A. (2019) *The Patentability of Software. Software as Mathematics*. New York: Routledge.

[40] Judgement of 11 June 2020, Brompton Bicycle, C-833/18, EU:C:2020:461.

[41] Judgement of 13 November 2018, Levola Hengelo, C-310/17, EU:C:2018:899.

[42] Judgement of 2 May 2012, SAS Institute, C-406/10, EU:C:2012:259.

[43] Judgement of 22 December 2010, Bezpečnostní softwarová asociace, C-393/09, EU:C:2010:816.

[44] Karakosta, Q., Petropoulou, D. (2021) The Electricity market: renewables targets, Tradeable Green Certificates and electricity trade. *SSRN*. Available from: `https://dx.doi.org/10.2139/ssrn.3828184` [Accessed 30 December 2022].

[45] Kelli, A. et al. (2020) Impact of Legal Status of Data on Development of Data-Intensive Products: Example of Language Technologies. In: Carlo Amatucci et. al. (eds.). Legal Science: Functions, Significance and Future in Legal Systems II, the 7th International Scientific Conference of the Faculty of Law of the University of Latvia, Riga, 16-18 October. Riga: University of Latvia Press.

[46] Klenner-Bajaja, A., EPO (2023). What is AI and how does it work. Presentation in: The European Patent Office. Conference on AI-related technologies: regulation, inventorship and patenting (JC01-2023). Available from: `https://www.epo.org/learning/training/details.html?eventid=16092` [Accessed 14 May 2023].

[47] Koorndijk, J. (2021) Adapting to innovations in artificial intelligence: AI as mental steps under the EPO. *European Intellectual Property Review*, 43(12).

[48] Kuman, U. et. al. (2019) Deep Learning for Healthcare Biometrics. In: Dakshina Ranjan Kisku, Phalguni Gupta, Jamuna Kanta Sing. *Design and Implementation of healthcare biometric systems*. Pennsylvania: IGI Global. Available from: doi: 10:4018/978-1-5225-7525-2.ch004 [Accessed 10 December 2022].

[49] Lee, J. A., Hilty, R. M., Liu, K.C. (eds.) (2021) *Artificial Intelligence & Intellectual Property*. Oxford: Oxford University Press.

[50] Luginbuehl, S. (2021) Patent Protection of Inventions Involving Artificial Intelligence. In: Niklas Bruun et. al. (eds.) *Transition and Coherence in Intellectual Property Law. Essays in Honour of Annette Kur*. Cambridge: Cambridge University Press.

[51] Müller, M., EPO BA (2023). *EPO Boards of Appeal case law on AI-related inventions*. Presentation in: The European Patent Office. Conference on AI-related technologies: regulation, inventorship and patenting (JC01-2023). Available from: https://www.epo.org/learning/training/details.html?eventid=16092 [Accessed 14 May 2023].

[52] Maini, V., Sabri, S. (2017) *Machine Learning for Humans*. Available from: https://everythingcomputerscience.com/books/Machine%20Learning%20for%20Humans.pdf [Accessed 10 December 2022].

[53] Nack, R., Nägerl, J. S. H., Walder-Hartmann, L. Inventions and their amenability to patent protection. In: Haedicke, M. W., Timmann, H. (eds.) (2014) *Patent Law: A Handbook on European and German Patent Law*, München: Beck.

[54] Newell, A. (1986) Response: The Models are Broken, the Models are Broken. *University of Pittsburg Law Review*, 47 (1023).

[55] Norvig, P. (2020). Bridging AI's trust g aps, fireside chat 'Responsible AI' [Panel discussion]. Reuters Events Virtual Forum Momentum "Overcome Global Challenges and Build a Better Future through Technology". Available from: https://www.dirse.es/events/momentum-virtual-forum/ [Accessed 14 May 2023].

[56] Picht, G., Thouvenin, P. (2022) AI&IP: Theory to Policy and Back Again Policy and Research Recommendations at the Intersection of Artificial Intelligence and Intellectual Property. *SSRN*, 16 November. Available from: https://dx.doi.org/10.2139/ssrn.4278819 [Accessed 16 December 2022].

[57] Pilger, J., Gall, I. (2022). AI and CI simulations: prospects for patenting inventions in Europe. In Adam Jolly (ed.) *Winning with IP: Managing Intellectual Property Today. Value and Growths from Ideas and Improvements*, 2nd. ed. Coventry: Novaro Publishing.

[58] Rudzite, L. (2023). Implications for the Inventive Step under the European Patent Convention Related to the Increasing Application of Artificial Intelligence and Certification as *Sui Generis* Protection Mechanism for Creations Involving Artificial Intelligence, *International Comparative Jurisprudence*, 9(1).

[59] Rudzite, L. (2022) Algorithmic Explainability and Sufficient Disclosure Requirement Under the European Patent Convention. *Juridica International*, 31/2022.

[60] Rudzite, L. (2022) Certifications as a Remedy for Recognition of the Role of AI in the Inventive Process. *International Comparative Jurisprudence*, 8(1).

[61] Samuelson, P. et. al. (1994). A Manifesto Concerning Legal Protection of Computer Programs. *Columbia Law Review*, 94, Available from: https:

//scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1783\&context=faculty_scholarship [Accessed 15 December 2022].

[62] Sevahula, R. K. et. al. (2020). State-of-the-Art Machine Learning Techniques Aiming to Improve Patient Outcomes Pertaining to the Cardiovascular System. *Journal of the American Health Association*, 9(4), 18 February. Available from: doi: 10.1161/JAHA.119.013924 [Accessed 10 December 2022].

[63] Teitelman, D., Naeh, I., Mannor, S. (2020) Stealing Black-Box Functionality Using the Deep Neural Tree Architecture. ArXiv. Available from: https://doi.org/10.48550/arXiv.2002.09864[Accessed 30 December 2022].

[64] *The Berne Convention for the Protection of Literary and Artistic Works*, 9 September 1886 (TRT/Berne/001). Available from: https://www.wipo.int/wipolex/en/text/283693 [Accessed 12 December 2022].

[65] The European Patent Office. (1973) *Article 52 E Travaux Préparatoires*. Available from: http://webserv.epo.org/projects/babylon/tpepc73.nsf/0/719AC39AA49A7563C12574270049EB9E/$File/Art52eTPEPC1973.pdf [Accessed 15 December 2022].

[66] The European Patent Office. (2022) *Artificial Intelligence*. Available from: https://www.epo.org/news-events/in-focus/ict/artificial-intelligence.html [Accessed 10 December 2022].

[67] The European Patent Office. *Guidelines for Examination G-II, 3.3.1 Artificial intelligence and machine learning*. Available from: https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_ii_3_3_1.htm [Accessed 10 December 2022].

[68] The European Patent Office. *Guidelines for Examination G-I, 2 (ii). Further requirements of an invention*. Available from: https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_i_2.htm [Accessed 15 December 2022].

[69] The European Patent Office. *Guidelines for Examination G VII 5.4.1. Formulation of the objective technical problem for claims comprising technical and non-technical features*. Available from: https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_vii_5_4_1.htm [Accessed 14 May 2023].

[70] The European Patent Office. *Guidelines for Examination, G-II, 3.6. Programs for Computers*. Available from: https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_ii_3_6.htm [Accessed 14 May 2023].

[71] The European Patent Office (2019). *Hardware and software*. Available from: https://www.epo.org/news-events/in-focus/ict/hardware-and-software.html.

[72] The European Patent Office (2022). *Member states of the European Patent Organisation*. Available from: https://www.epo.org/about-us/foundation/member-states.html [Accessed 30 December 2022].

[73] The European Patent Office. (2018) *Patenting Artificial Intelligence*. Conference Summary, EPO Munich, 30 May. Available from: https://documents.epo.org/projects/babylon/acad.nsf/0/D9F20464038C0753C125829E00\\31B814/$FILE/summary_conference_artificial_intelligence_en.pdf [Accessed 10 December 2022].

[74] The Joint Institute for Innovation Policy, IViR – University of Amsterdam (2020) Trends and Developments in Artificial Intelligence. Challenges to the Intellectual Property Rights Framework. Final Report for the European Commission. Publication Office of the European Union. Available from: https://op.europa.eu/en/publication-detail/-/publication/394345a1-2ecf-11eb-b27b-01aa75ed71a1/language-en [Accessed 30 December 2022].

[75] The World Intellectual Property Organization. *Utility models*. Available from: https://www.wipo.int/patents/en/topics/utility_models.html [Accessed 16 December 2022].

[76] Turkevich, L. R. (1995) An end to the 'Mathematical Algorithm' Confusion. *European Intellectual Property Review*, 17 (2).

[77] Zeidman, B. (2011) *The Software IP Detective's Handbook. Measurement, Comparison and Infringement Detection*. Boston: Pearson Education Inc.

DOI 10.5817/MUJLT2023-2-5

CYBERSECURITY: NOTORIOUS, BUT OFTEN MISUSED AND CONFUSED TERMS*

by

JAN KOLOUCH † DANIEL TOVÁRŇÁK ‡ TOMÁŠ PLESNÍK § MICHAL JAVORNÍK ¶

The article deals with the issue of the terminology used in the implementation and provision of cyber and information security. Although this terminology is understood as notoriety, practice shows that there are different perspectives on defining "the same". Nowadays, mainly in the context of the adoption of Directive (EU) 2022/2555 of the European Parliament and of the Council on measures to ensure a high common level of cybersecurity in the Union (NIS 2), there is a need for a consistent interpretation and, in particular, understanding of the terminology used so that cybersecurity and information security can be truly ensured. After analyzing and comparing the various definitions, the paper presents clear, general but universally applicable definitions of key terms. The relationship of these terms is presented within a conceptual model and also through a practical example.

KEY WORDS

Cybersecurity, Information security, Event, Threat, Asset, Vulnerability, Risk, Control, Information Security Management System, security terminology

* 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@law.muni.cz, CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence (C4e), MUNI; jan.kolouch@cesnet.cz, CESNET a.l.e., Czech Republic

‡ tovarnak@ics.muni.cz, CSIRT-MU, MUNI, Czech Republic

§ plesnik@ics.muni.cz, CSIRT-MU, MUNI, Czech Republic

¶ javornik@ics.muni.cz, CSIRT-MU, MUNI, Czech Republic

1. INTRODUCTION

In a relatively short period, contemporary society has been exposed to very intense changes related to the massive integration of information and communication technologies[1] into most areas of human activity. Dependence on ICT has reached an imaginary „event horizon" and humanity can no longer able to exist without these technologies. This dependence naturally brings with it a huge scope for cyber threats, attacks, and crime. We can observe a trend of traditional security threats[2] moving into cyberspace, creating new threats specific to this environment. There is also a stronger intermingling of different threats and a hybridization of the security environment, the dynamics and scope of which are enhanced by cyberspace and ICT.

It is necessary to respond to these negative phenomena and create space for the implementation of cybersecurity and information security principles at all levels, in all affected processes, and towards all stakeholders.

When we talk about cyber security, it is important to remember that we are in an area where the terms „information and communication technology security", „cyber security" and „information security" are often confused as synonyms. In practice, it is often possible to try to specify these terms and their boundaries precisely[3], but this is not the aim of the present article, since the terminology discussed in this article can be applied in all these areas.

In very simplistic terms, ICT security is the set of measures, procedures, and practices applied by individuals or organizations to ensure the triad of CIA (confidentiality, integrity, and availability) of these systems and the data they contain. ICT security monitors the security of both the entire ICT infrastructure and individual endpoint devices.

Cybersecurity is a relatively comprehensive system including technical, organizational, and other measures to protect ICT, applications, data, and users. Cybersecurity should also be seen as the ability to respond to cyber threats or attacks and their consequences, as well as planning for the recovery

---

1 Hereinafter referred to as ICT

2 For example: *Cyber-attacks have tripled in past year, says Ukraine's cybersecurity agency* [online]. The Guardian. Available from: `https://www.theguardian.com/world/2023/jan/19/cyber-attacks-have-tripled-in-past-year-says-ukraine-cybersecurity-agency` [Accessed 20 February 2023], *Russia's war on Ukraine: Timeline of cyber-attacks* [online]. European Parliament. Available from: `https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549` [Accessed 20 February 2023], *Industroyer2: Industroyer reloaded* [online]. Eset. Available from: `https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/` [Accessed 20 February 2023]

3 See e.g.: Solms, R.V., & Niekerk, J.F. (2013). *From information security to cyber security. Comput. Secur., 38, 97-102.*

of the functionality of these systems and the services associated with them, including the final learning from a crisis.[4]

Information security is primarily focused on the protection of information, regardless of the type of medium (paper, electronic media, etc.) or the system in which the information is processed. Information security is then applied to information throughout its life cycle.

Even though the term „information security " is more commonly used as a „superordinate " term in the professional literature and technical standards (see Chapter 2), the term „cybersecurity " will be used as a general term in this article, especially because of the EU legislative framework, where this term is the superordinate or umbrella term.[5] Where necessary to present different approaches, both the terms cybersecurity and information security will be used.

An integral part of information and cybersecurity is the terminology that is used in ensuring this security. This terminology is all the more important as it is part of the legislation adopted at both national and international levels. Earlier this year, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity in the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [6] entered into force. This directive uses terminology that is often based on technical standards, but when translated into legal language, the use of this technical terminology is often not entirely appropriate, often even incorrect. In practice, there is a clash between the views of engineers, security personnel, and lawyers, who define a relatively clear concept quite differently.

It is not possible to define all the terms related to cyber security (e.g. cyber attack, cyber threat, significant cyber threat, threat actor, near miss, eventuality, etc.) and to cover in detail all the technical and legal implications

[4] Kolouch, J. and Bašta, P. (2019) *CyberSecurity*. Praha: CZ.NIC. ISBN 978-80-88168-31-7. p. 44-45.

[5] See e.g.: European Commission. (2022)*The Cybersecurity Strategy* [online]. European Commision. Available from: `https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy` [Accessed 8 August 2023], Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity in the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[6] Hereinafter referred to as NIS 2. Available from: `https://eur-lex.europa.eu/eli/dir/2022/2555/oj`

of the terminology used. For this reason, the authors have focused on the "key" terms and their interrelationships (see Chapter 3). The presented outputs can then be further supplemented with additional terminology and interrelationships can also be added to the presented Conceptual Model. Based on the comparison, the authors try to point out the shortcomings and differences in the technological and legal understanding of the terminology used, while their own opinions and de lege ferenda suggestions on individual legal and technical definitions are also presented.

The purpose of the presented article is not to find a single suitable or universal explanation of the given terms, as such a solution de facto does not exist. It is also not to create new terminology or definitions of existing terms, but rather to find a consensus or at least to define a generally accepted framework of the given terminology for technical, legal, and user purposes.

2. EVOLUTION OF THE LEGAL FRAMEWORK FOR CYBERSECURITY REGULATION

One of the first definitional standards that addressed the issue of security as well as defining terminology in the online environment was the RFC (*Request For Comments*)[7]. Although these documents are recommendations rather than standards, they are respected by users as if they were standards.[8]

These standards created a general premise for the creation of other, more detailed technical and legal standards defining the basic terminology of cyber and information security.

Information security is also defined by ISO 27000 standards. Information security standards related to this article include:

- ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary[9]

[7] RFC documents contain technical specifications and organizational notes for the Internet. The RFCs are freely available at: `https://www.ietf.org/rfc/`

[8] Security related RFCs include mainly: RFC 1208 (A Glosary of Networking Terms), RFC 1983 (Internet Users' Glossary), RFC 4949 (Internet Security Glossary), RFC 2196 (Site Security Handbook), RFC 2350 (Expectations for Computer Security Incident Response), RFC 2504 (Users' Security Handbook), RFC 3631 (Security Mechanisms for the Internet), RFC 6040 (Security Architecture for the Internet Protocol), RFC 4778 (Current Operational Security Practices in Internet Service Provider Environments). The RFCs are freely available at: `https://www.ietf.org/rfc/`

[9] Hereinafter referred to as ISO/IEC 27000. Available from: `https://www.iso.org/standard/73906.html`

- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements[10]
- ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls[11]
- ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks[12]

At the level of the European Union, it has long been possible to observe efforts to protect the assets of cyberspace and, at the same time, to harmonize the legislation of individual Member States so that the issue of cybersecurity can be effectively addressed. The first steps in this area can be traced back to the 1990s[13] and then to the beginning of this millennium.[14] The most significant change was brought about by 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[15], which is currently still in force.

The European Parliament adopted on 10 November 2022 and the Council of the European Union on 28 November 2022 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). As this is a Directive, not a Regulation, the legislative process for adopting the Directive is not yet complete. The

[10] Hereinafter referred to as ISO/IEC 27001. Available from: https://www.iso.org/standard/82875.html

[11] Hereinafter referred to as ISO/IEC 27002. Available from: https://www.iso.org/standard/75652.html

[12] Hereinafter referred to as ISO/IEC 27005. Available from: https://www.iso.org/standard/80585.html

[13] E.g. Directive 91/250/EEC of the European Parliament and of the Council on the legal protection of computer programs. Council Decision 92/242/EEC on the security of information systems.

[14] E.g. Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce), Directive 2002/19/EC of the European Parliament and of the Council on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive), Regulation 460/2004/EC of the European Parliament and of the Council establishing the European Network and Information Security Agency, as amended by Regulation 1007/2008, Directive 2008/114/EC of the European Parliament and of the Council on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[15] Hereinafter referred to as NIS 1. Available from: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:32016L1148

Directive entered into force on 16 January 2023 and individual Member States have 21 months from that date to implement the Directive in their legal systems (expected October 2024). The NIS2 Directive aims to strengthen EU cybersecurity and harmonize the rules for ensuring it across the EU. The Directive, therefore, brings modifications to existing requirements and extends regulation to several new organizations and other changes.

In addition to these standards, the terms (typically in the form of explanatory dictionaries) related to the issue of information and cybersecurity are also defined by organizations that, based on their mandate, have a certain privileged position in this area. These organizations include in particular The European Union Agency for Cybersecurity (ENISA)[16], the Cybersecurity & Infrastructure Security Agency (CISA),[17] and the National Institute of Standards and Technology (NIST)[18].

All the technical and legal documents mentioned above very often work with terms that will be defined in the following chapter. However, these terms are not used doctrinally and uniformly. On the contrary, they are often used synonymously and are also often overused in situations where their use is inappropriate. This degree of linguistic creativity can be observed both at the international and, in particular, at the national level in the context of the transposition of EU legal norms into national legislation.

For this article, definitions based on ISO/IEC 27000, NIST, CISA, NIS 1, and NIS 2 will be used in the remainder of this article. The authors are aware of the existence of other standards or technical interpretative dictionaries, but the aim is to highlight the ambiguity in the interpretation of key cyber and information security concepts, both within and outside the European Union. A secondary objective is to highlight the not-always-clear and unambiguous terminology presented within the NIS2.

3. THREAT, ASSET, VULNERABILITY, RISK, EVENT, AND MORE

In this part of the article, attention will first be paid to the characteristics of six key terms (Asset, Event, Threat, Vulnerability, Risk, and Control) related to cybersecurity. The terminology used in both legal and technical

[16] *Glossary* [online]. ENISA. Available from: `https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/glossary` [Accessed 10 January 2023].

[17] *Explore Terms: A Glossary of Common Cybersecurity Words and Phrases* [online]. NICCS. Available from: `https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary` [Accessed 10 January 2023].

[18] *Guide for Conducting Risk Assessments: Information Security* [online]. NIST. Available from: `https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf` [Accessed 10 January 2023].

standards is often imprecise, incomplete, and sometimes contradictory. These shortcomings result in a misunderstanding of security management as a whole.

Based on the comparison made, the authors try to point out the shortcomings and differences in the technological and legal concept of the terminology used, while their own opinions and suggestions de lege ferenda on individual legal and technical definitions are also presented.

The relationship and interrelationship of these key and other concepts will then be presented within the framework of a conceptual model. This model provides a basic framework into which further sub-relationships can be added.

3.1. ASSET

An asset can be a tangible thing (a building, computer system, network, energy, goods, etc.) or intangible (information, knowledge, data, programs, etc.) from the perspective of civil law. However, an asset can also be a property (e.g. availability and functionality of a system and data, etc.) or a good name, reputation, etc. People (users, administrators, etc.) and their knowledge and experience are also an asset from a cybersecurity perspective. ISO/IEC 27000 does not define the term „asset" itself, but states that „information is an asset that, like other important business assets, is essential to an organization's business and, consequently, needs to be suitably protected." [19] It follows, therefore, that the term „asset" is primarily related to the concept of information or other assets important from a business perspective. However, it is questionable whether all assets of an organization must necessarily fulfill the condition of a relationship to information or business.

Another definition of „asset " can be found in ISO/IEC 19770-1 (IT asset management), which states that an „asset " is an item, thing, or entity that has potential or actual value to an organization.

According to NIST the „asset" is a „major application, general support system, high impact program, physical plant, mission-critical system, personnel, equipment, or a logically related group of systems."[20] It is clear that the NIST definition of „assets" is quite inadequate, as it focuses only on systems (hardware and software) and personnel. No consideration is given to the value of data, information, etc.

[19] ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary. p. 12.

[20] CNSS. *Committee on National Security Systems (CNSS) Glossary* [online]. Available from: `https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf` [Accessed 10 January 2023].

NIS 1 and NIS 2 directives do not define the term „asset", although the term asset is used in both legal standards. NIS 2 Article 7, point (9), letter (d) sets out the obligation to establish „a mechanism to identify relevant assets and an assessment of the risks in that Member State". Similarly, Article 9, point (3) provides that Member States are to identify „assets that can be deployed in the case of a crisis for the purposes of this Directive."

CISA states that the asset is „a person, structure, facility, information, and records, information technology systems and resources, material, process, relationships, or reputation that has value." Extensively, an asset can be considered as „anything useful that contributes to the success of something, such as an organizational mission; assets are things of value or properties to which value can be assigned."[21]

Similarly, an asset is defined in ISO/IEC PDTR 13335-1, which states that an asset is „anything that has value to the organization, its business operations, and their continuity, including Information resources that support the organization's mission."

Both definitions are sufficiently general to include assets that are significant to the person who manages or owns them. When it comes to defining or identifying an asset, the determining factor is first and foremost the objectives of the organization, which determine what the primary assets are (processes/activities and information) and then also what the main risks to those assets are from the sources of uncertainty (threats and opportunities).

As NIS 2 does not define the actual concept of an asset, different countries may have different implementations of what will be considered an asset. Thus, for example, information and services may be considered assets in one national legislation and only data and processes in another. This disparity may have a significant impact on the identification of assets, especially if the subject implementing the cybersecurity rules uses, for example, the services of multinational corporations or organizations based abroad, i.e. under different legislation. A separate issue is how the different legal regulations deal with the identification of primary and supporting assets (e.g. ICT technologies, employees, objects, etc.).

Based on a comparison of these definitions and the absence of a general legal definition, we believe that it would be appropriate to provide that an asset is anything that has value and contributes to the achievement of an organization's objectives.

[21] NICCS. *Explore Terms: A Glossary of Common Cybersecurity Words and Phrases* [online]. NICCS. Available from: `https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary` [Accessed 10 January 2023].

In the case of an asset, the authors prefer the definition given in ISO/IEC 19770-1, but in addition, the asset needs to be consistently mapped to the organization's objectives. This is because, according to the authors, it is not possible for an organization's objective to exist without the support of at least one asset and, conversely, an asset is not an asset if it does not support at least one of the organization's objectives.

For example, if the organization in question is in the business of providing data storage services through a privately-owned data center, the typical asset inventory would include the actual data center facility, i.e., the building, and the storage servers.

3.2. EVENT

An event could be defined as a situation that has occurred or is believed to have occurred.

According to ISO/IEC 27000, an event is an „occurrence or change of a particular set of circumstances". Bearing in mind that an event can consist of something not happening. ISO/IEC 27000 states that „an event can sometimes be referred to as an „incident" or „accident".

NIST defines an event as „any observable occurrence in a network or system."[22] CISA defines „event" very similarly, stating that it is an „observable occurrence in an information system or network." Relating an event to the concept of „any observable occurrence" is, in our opinion, misleading for several reasons. There may be a situation where an event is not observable (for whatever reason), and under this interpretation, it would then obviously not be an event. Also, the event is only related to the „network, system, information system" environment thus creating a relatively small ecosystem for the possibility of an event to occur.

NIS 1 Directive does not define the term event in any way, but only states that:

- „Risk means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems"[23];
- „Incident means any event having an actual adverse effect on the security of network and information systems"[24];

[22] Cichonski, P. et al. (2012) Computer Security Incident Handling Guide [online]. *NIST Special Publication (SP)*, 800-61 Rev. 2. Gaithersburg, MA: National Institute of Standards and Technology. Available from: doi: https://doi.org/10.6028/NIST.SP.800-61r2 [Accessed 10 January 2023]. p. 60.

[23] Article 4, point (9) NIS 1.

[24] Article 4, point (7) NIS 1.

based on the above, it can be concluded that both incident and risk (see below) are always an event according to NIS 1.

The definition of „event" is similarly handled in NIS 2, which states in Article 6, point (6) that „**incident means an event** compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems."

Thus, the term „event" becomes synonymous with the term „incident" according to the legislator. The authors do not believe that it is appropriate to draw an equivalence between the term „event" and „incident". The event can lead to action and, at the same time, can cause harm. The event could also pose a potential threat.

An example of an event is a planned entry of the service personnel onto the premises of the organization's data center. However, since the entry was planned and authorized according to the organization's policy, this event cannot be considered an incident.

Based on the above comparison, we believe that the term „event" should be rather defined as a situation that has occurred or is believed to have occurred. This presumption is there because there is a direct or indirect indication that the event has occurred.

In addition to the event, it is also possible to work with the concept of a non-event, i.e., the state or assumption that the situation did not occur. An event can be certain or uncertain.

Based on a comparison of these definitions and the absence of inconsistencies in the legal definition, we believe it would be appropriate to provide that an event is an occurrence or change of a particular set of circumstances within a particular domain; it is something that has happened, or it is contemplated as having happened in that domain.

The authors have extended the definition of the event[25] with two additional ideas as described by Etzion[26]. First, the notion of a domain is added, e.g., cybersecurity. This means that events that are not relevant to a particular domain might not be considered at all, rendering all events relevant. Second, an event is something that has happened or is contemplated as having happened. Thanks to this, it is possible to work with occurrences that are believed to have happened based on some indicators, even though further investigation may indicate the opposite, i.e., a false positive. Please note that an event is something that has already happened, i.e., it is in the

[25] ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection - Guidance on managing information security risks.

[26] Niblett, P., Etzion, O. (2010) *Event Processing in Action*. Manning. ISBN 9781638352624.

past. To refer to a hypothetical or potential event, i.e., one that is in the future, we will use the term **eventuality**. The eventuality is the source of uncertainty, which, as we will explain later, is an important concept underlying a risk. In addition, the event can have one or more **consequences**, i.e., outcomes that are directly or indirectly affecting objectives. Last, but not least, the event can usually denote an atomic occurrence, sometimes referred to as a simple event, or a composition of several events of arbitrary complexity, sometimes referred to as a situation or complex event.

3.3. THREAT

A threat can probably be most simply defined as an eventuality capable of disrupting the normal or orderly state of affairs. It is a negative action that may or may not be completed. For the actual definition, it is sufficient that the possibility of a negative state of affairs is imminent and real.

A somewhat different definition can be found in ISO/IEC 27000, where the threat is defined as a „**potential cause of** an unwanted **incident**, **which can result in harm** to a system or organization." A threat is therefore related to an incident that can lead to harm, which is related only to defined areas: a system or an organization (person or group of people).

According to NIST the threat „is any **circumstance or event** with the **potential to** adversely **impact** organizational operations and assets, individuals, other organizations, or the Nation through an Information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service."[27]

In defining the term threat, another related term is used: „event". The use of this term can be confusing as "threat manifests as an event which causes harm to asset". There is also a flaw in this definition in that the authors have not attempted to provide a general characterization of assets, but have instead defined various protected objects, whereas the phrase „potential to adversely impact assets" would have sufficed. We also have a negative view of the attempt to define the various types of „attack" or „harm type". The above list is exhaustive, but it is clearly not exhaustive.

NIS 1 and NIS 2 directives do not define the term „threat", although the term cyber threats are used in both legal norms. The legislator somewhat works with the term „threat" as a notoriety. NIS 2 in Article 6, point (10) states that „cyber threat" means a cyber threat as defined in Article 2, point (8), of Regulation (EU) 2019/881.

[27] Cichonski, P. et al. (2012) Computer Security Incident Handling Guide [online]. *NIST Special Publication (SP)*, 800-61 Rev. 2. Gaithersburg, MA: National Institute of Standards and Technology 2012. Available from: doi: https://doi.org/10.6028/NIST.SP.800-61r2 [Accessed 10 January 2023]. p. 8.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) defines „cyber threat" as any **potential circumstance, event** or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons.

In defining the term threat, the term „event" is again used inappropriately. At the same time, the term „action" is used, from which it is possible to infer an active action of, for example, an attacker. If we were to define the relationship between threat and action, it would be correct to state that „threat manifests as event and can lead to action".

The use of the adjective „cyber" in defining the term led the authors to believe that „threat" refers only to the impact on „network, information systems and the users of those systems". However, the question is whether the use of the prefix „cyber" is appropriate or whether, on the contrary, it further complicates the established, albeit largely inaccurate, terminology. The word cyber refers primarily to the relationship to cybersecurity, but the area that is protected against threats is at least in the scope of information and cybersecurity, but in a broader sense it can also protect against physical threats that do not originate from the digital environment but are capable of negatively affecting this environment.

The impact on „other persons" can then be seen as an expansive interpretation of the impact of this cyber threat. On the negative side, the attempt to define the different types of „harm type" can again be seen, although the use of the phrase „or otherwise adversely impact" makes it a more appropriate classification than in the previous case.

According to CISA, a „threat" is a „circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society."[28]

As in the previous cases, the term „event" is inappropriately used, but „potential to exploit vulnerabilities and to adversely impact assets" is appropriately used. This definition is probably the closest to a general and non-deceptive definition of „threat".

[28] NICS. *Explore Terms: A Glossary of Common Cybersecurity Words and Phrases* [online]. NICCS. Available from: `https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary` [Accessed 10 January 2023].

A typical example of a threat is the eventuality of a fire. A threat may also be, for example, unauthorized access to data center premises.

Comparing all these definitions, it can be concluded that a threat is an eventuality that can be expected to have negative consequences for the objectives.

At the same time, the negative consequences, or **harm, always act on objectives** through the underlying assets. It should also be noted at this point that in practice the terms threat and threat agent/actor are often confused. The realization of a threat can only occur if there is a corresponding vulnerability that it exploits and a threat actor that can exploit it. Although a threat represents a source of uncertainty, its existence is de-facto immutable. This means that to reduce the likelihood of a threat materialization, or its consequences, appropriate measures are addressing the vulnerability, and the harm, respectively, but never directly the threat itself.

3.4. VULNERABILITY

Vulnerability refers to a weakness in an asset or security that is exploited by one or more threats. Vulnerability defined in this way more or less corresponds to the definition according to ISO/IEC 27000, but instead of the term security, the term „control" is used, which is characterized as „a measure that is modifying risk". According to a semantic interpretation, it would be possible to accept the interpretation that the term „measure that is modifying risk" is de facto a certain security measure.

Another definition of „vulnerability" can be found in ISO/IEC 27005, which defines „vulnerability" as a weakness of an asset or control that can be exploited so that an event with a negative consequence occurs.

NIST defines a vulnerability as „a weakness in a system, system security procedure, internal controls, or implementation that could be exploited by a threat source."[29] This definition is based on the assertion that „most information system vulnerabilities can be associated with security controls that either have not been applied (either intentionally or unintentionally), or have been applied, but retain some weakness. However, it is also important to allow for the possibility of emergent vulnerabilities that can arise naturally over time as organizational missions/business functions evolve, environments of operation change, new technologies proliferate, and new threats emerge. In the context of such change, existing security controls may become inadequate and may need to be reassessed for effectiveness. The

[29] Cichonski, P. et al. (2012) Computer Security Incident Handling Guide [online]. *NIST Special Publication (SP)*, 800-61 Rev. 2. Gaithersburg, MA: National Institute of Standards and Technology. Available from: doi: https://doi.org/10.6028/NIST.SP.800-61r2 [Accessed 10 January 2023]. p. 9.

tendency for security controls to potentially degrade in effectiveness over time reinforces the need to maintain risk assessments during the entire system development life cycle and also the importance of continuous monitoring programs to obtain ongoing situational awareness of the organizational security posture."[30]

Directive NIS 1 uses the term vulnerability only in Recital 59, which states that „CSIRTs should pay particular attention to the need to keep information about product vulnerabilities strictly confidential, prior to the release of appropriate security fixes." This interpretation, therefore, suggests that the legislator applies the concept of vulnerability only to „products" in the current and effective Directive. Such a characterization of vulnerability is inadequate and certainly does not help to create legal certainty.

In the NIS 2 directive, the actual concept of vulnerability is mentioned in Article 6, point (15), where it is stated that „vulnerability means weakness, susceptibility or defect in ICT products or ICT services that can be exploited by a cyber threat".

The question is why the legislator is introducing a new concept of „susceptibility", which is to a large extent even broader than the concept of „weakness". The term „susceptible" generally means that a person, thing, or situation tends to be more susceptible or more prone to a particular type of behavior or event. For example, a person may be prone to being overweight, meaning they are more likely to become obese if they do not take care of their diet and physical activity. Similarly, an area may be prone to earthquakes, which means that there is a greater likelihood of earthquakes occurring there compared to other areas. The term „weakness" usually means a deficiency or weakness in a particular area. For example, a person may have a weakness in mathematics, which means they have difficulty understanding and solving mathematical problems. Similarly, a person may have a weakness in a security system, which means that the system has deficiencies or vulnerabilities that could be exploited for attack or attack. Both terms refer to specific flaws or problems, but the term „susceptibility" focuses on the tendency for a particular behavior or event to occur, while „weakness" focuses on specific flaws or vulnerabilities in a system or area.

As regards the definition of the range of assets, i.e. „ICT products or ICT services", we believe that such a significant narrowing of the potential impact of the vulnerability is completely inappropriate. It would certainly be more appropriate to use the more general term „asset" instead of „ICT products

[30] *Op. cit.* p. B-13. Also see: *Committee on National Security Systems (CNSS) Glossary* [online]. Available from: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf [Accessed 10 January 2023] p. 131.

or ICT services". The narrowing down to only „cyber threat" should also be criticized (see the analysis of the definition of a threat).

CISA describes vulnerability as a „weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source."

Even this definition shows a not entirely logical narrowing of the possible impact of vulnerability to only „information system, system security procedures, internal controls, or implementation".

A typical case of weakness is improper access control, when, for example, a software product does not restrict or incorrectly restrict access to a resource from an unauthorized actor. It becomes a vulnerability when the malicious actor finds an actual way to compromise the security of the product by gaining privileges, reading sensitive information, or executing commands, i.e., the weakness becomes exploitable.

Based on a comparison of these definitions, we believe that vulnerability should be understood as a weakness of an asset or control that can be exploited by a threat.

In the case of vulnerabilities, authors follow ISO/IEC 27005 almost verbatim but emphasize the relationship between the eventuality (threat) and the event. By the standard, it is needed to consider that both assets, e.g., processes, software, or hardware, and applied controls themselves, e.g., policies and rules, can be vulnerable (weak) concerning some threat. One can also say that vulnerability weakens assets and/or controls just enough so that some threat can materialize.

3.5. RISK

Risk is usually assessed as a combination of the probability that an adverse event (a harmful impact on a person, thing, or process, i.e., an asset) will occur and its impact if it does occur.

The risk assessment is usually based on three basic questions:

- What bad (undesirable) things can happen? What can fail?
- What is the possibility/probability of this happening?
- How severe (intensity, magnitude, etc.) can the effects (impacts, consequences) be?

Risk is also defined by various authors as the equation: **risk = impact * threat * vulnerability**. While this simplification is commonly used, it can be highly misleading and in the context of this article is rather discouraging.

A meaningful, defensible, and realistically applicable risk quantification principle for risk management can be a very complicated matter. It must

be understood that vulnerability and threat generally refer to a different asset than the impact of the potential exploitation of that vulnerability. An institution with a trivial asset structure will hopefully be able to get by with a simple formula; a more complicated institution will require more complex considerations.

Uncertainty plays a crucial role in quantifying risk. Based on the structure of the assets, it is necessary to infer which assets representing the organization's objectives will be impacted by the potential exploitation of vulnerabilities in the assets representing the supporting assets and what the level of such impacts will be. The second component of uncertainty that enters into the risk calculation is determining the probability that the exploitation of the vulnerability will occur.

„Risk is the effect of uncertainty on objectives[31]. In the context of information security management systems, information security risks can be expressed as an effect of uncertainty on information security objectives. Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization." [32]

NIST defines risk as „a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:

(i) the adverse impacts that would arise if the circumstance or event occurs; and

(ii) the likelihood of occurrence."[33]

In defining risk, both definitions work consistently with the concept of „uncertainty". Uncertainty is the deficiency of information, understanding, or knowledge related to a potential event (eventuality). This may include the specific nature of the event, its consequences, or likelihood.[34]

[31] Objectives are results which should be achieved. Objectives can be strategic, tactical, or operational and can to different disciplines (e.g safety, financial, health) and can apply at different levels (strategic, organization-wide, project, product and process).

[32] ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary. p. 8.

[33] Cichonski, P. et al. (2012) Computer Security Incident Handling Guide [online]. *NIST Special Publication (SP)*, 800-61 Rev. 2. Gaithersburg, MA: National Institute of Standards and Technology. Available from: doi: `https://doi.org/10.6028/NIST.SP.800-61r2` [Accessed 10 January 2023]. p. B-9.

[34] See also: NIST. (2019) Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. [online]. *NIST Special Publication (SP)* 800-37 Rev. 1 Gaithersburg, MA: National Institute of Standards and Technology.

According to Article 4, point (9) of the NIS 1, risk means „any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems."

In cyberspace, both users and the computer systems and applications that use them, as well as other ICT elements, are at risk. In our opinion, a narrow definition of risk only concerning the security of networks and information systems is therefore insufficient.

NIS 2 defines the concept of risk in a significantly different and to some extent „innovative" but at the same time quite confusing way. Article 6, point (9) states that risk means „the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident".

The risk itself relates only to the possibility of loss or disruption, presumably of an asset, following an incident. The question is whether only assets can be affected by risk or also objectives, as specified in ISO/IEC 27000. Quite inappropriately, then, the legislator directly associates risk only with the incident.

CISA defines risk as a „potential for an unwanted or adverse outcome resulting from an incident, event, or occurrence, as determined by the likelihood that a particular threat will exploit a particular vulnerability, with the associated consequences." Similar to NIS 2, there is a linking of risk with „incident, event, or occurrence", but the above is linked to a particular threat. Such a definition is certainly more appropriate and accurate, even though it is not entirely correct.

The concept of risk itself is probably the most difficult to define. In terms of generality, the most appropriate definition is derived from ISO/IEC 27000, i.e., which states that „risk is the effect of uncertainty on objectives".

Having analyzed the above, we believe that risk can be understood as the effect of uncertainty, resulting from the lack of information related to the specific nature, likelihood, and consequences of an eventuality on the objectives.

The above-mentioned definition is based on the ISO/IEC 27000 and ISO 31000 Risk Management standards, where we only refine our understanding of the source of uncertainty, i.e., the eventuality. It should be pointed out that the abovementioned understanding, like the intent of the original definition, allows to work with positive risk, i.e., also with eventualities that can be expected to have positive consequences for the organization's objectives. In contrast with threats, such eventualities are commonly referred to as opportunities.

For example, a successful standardization of a new cryptography standard might be an opportunity with positive consequences for an organization's information security objectives, e.g., the confidentiality and integrity of data at transit/at rest. However, at the same time, an eventual vulnerability (presently unknown) of the standard might be considered potentially exploitable, thus giving rise to risk.

3.6. CONTROL

The control modifies either the consequences of the event or the vulnerability (reducing the likelihood of exploiting the vulnerability or possibly the impact and scope).

ISO/IEC 27000 states that „control is a measure that is modifying risk."[35] The control includes any process, policy, device, practice, or other actions which modify risk. The control itself may not always have the intended or anticipated modifying effect.

NIST defines common control „as part of the information security architecture, organizations are encouraged to identify and implement security controls that can support multiple information systems efficiently and effectively as a common capability (i.e., common controls). When these controls are used to support a specific information system, they are referenced by that specific system as inherited controls. Common controls promote more cost-effective and consistent information security
across the organization and can also simplify risk management activities."[36]

The NIS 1 and NIS 2 directives do not define the term „ control" although they work with this term. For example, NIS 2 in Recital 79 states that „...and have in place appropriate access control policies. Those measures should be consistent with Directive (EU) 2022/2557". In both directives, either the term control is used synonymously instead of „security requirements" or „measures".

CISA also does not characterize the concept of control and, similarly to the above-mentioned legal norms, uses the terms: measure, protective measure, and countermeasure in various forms. It is possible to assume that this is an attempt to describe the term „control" in a different manner.

[35] ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary. p. 3.

[36] Cichonski, P. et al. (2012) Computer Security Incident Handling Guide [online]. *NIST Special Publication (SP)* 800-61 Rev. 2. Gaithersburg, MA: National Institute of Standards and Technology. Available from: doi: `https://doi.org/10.6028/NIST.SP.800-61r2` [Accessed 10 January 2023]. p. 16. See also: NIST. (2019) Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. [online]. *NIST Special Publication* (SP) 800-37 Rev. 1 Gaithersburg, MA: National Institute of Standards and Technology. p. B-9.

A typical example of a measure is the introduction of access control to the data center by authorizing authorized persons, granting access cards, controlling access to the data center using a camera system, etc.

By comparing these definitions, it can be concluded that control is a measure that maintains and/or modifies risk.

In this case, we comply with the definition given in ISO/IEC 27005. We consider that the measures act either on vulnerabilities, thereby reducing the likelihood of the threat occurring or on the consequences (harm) that the realization of the threat could bring about, thereby mitigating them. For the sake of completeness, let us add that controls are not the only category of risk treatment. According to ISO/IEC 27005, risk can be accepted, shared with a third party, or eliminated entirely by removing the assets it affects, albeit with objectives it supports.

3.7. VISUALIZATION OF KEY TERMS OF CYBER AND INFORMATION SECURITY

Based on the characteristics of the six concepts described above, the authors present a simplified conceptual model that graphically depicts the interaction of the key concepts and entities in the field of basic risk management, and consequently cyber and information security management. In addition to the conceptual model, a basic example is presented based on the terminology discussed.

The conceptual model in Figure 1 describes the entities and their relationship cardinalities using a so-called Crow's foot notation. This notation allows for the description of one-to-one, one-to-many (many-to-one), and many-to-many relationships. The conceptual model and the relationships are supposed to be read as follows (the list is not complete):

- Objective is supported by one or more assets.
- Asset supports one or more objectives. (Otherwise, it would not be an asset.)
- Event is a manifestation of exactly one threat (eventuality). (And vice versa.)
- Threat causes one or more instances of harm (negative consequences). (Otherwise, it would not be considered a threat.)
- An instance of harm harms exactly one asset. (This means that an instance of harm is always scoped to a particular asset.)
- Control treats zero or more vulnerabilities.

- Control treats zero or more instances of harm.
- Risk instance is informed by exactly one threat.
- Risk instance is informed by exactly one harm instance.

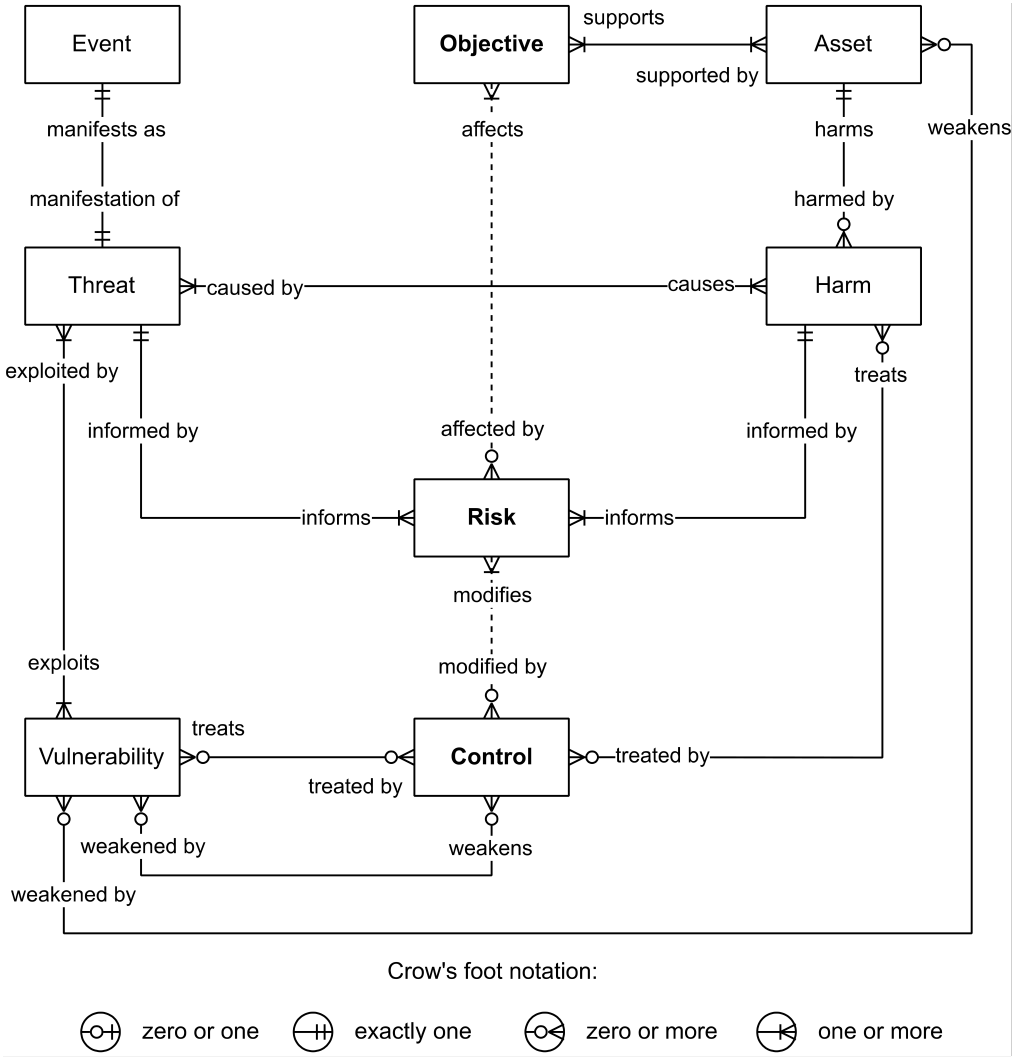

Figure 1: Conceptual model

The conceptual model can be explained by a relatively simple example:
Objective: Living in a house.

Asset: House of straw.
Threat: Structural damage due to strong wind.
Vulnerability: Straw is an extremely light material.
Harm: The house being destroyed (destruction).
Risk to asset: House being blown away (destroyed) by a strong wind.
Risk to the objective: Having nowhere to live.
Threat actor: The Wolf.
Event: The Wolf blew once.
Consequences: House was blown away.
Control (treating vulnerability): Use of better building materials, e.g., sticks or bricks.
Control (treating harm): Having plenty of straw to build a new house.
Risk treatment (avoiding risk): Not wanting to live in a house.
Risk treatment (removing the source of risk): Getting rid of the Wolf.
If this fairy tale story is applied to the field of cybersecurity, it could be demonstrated as follows:
Objective: Maintaining a good reputation among customers concerning data protection.
Asset: List of customers with personal details.
Threat
Threat: Access to data on lost storage medium.
Vulnerability: No encryption on storage media.
Harm: Disclosure of a list of customers with personal details (information disclosure).
Risk to the asset: Disclosure of a list of customers with personal details due to the access to data on lost storage medium.
Risk to the objective: Loss of reputation due to information disclosure.
Threat actor: Random finder.
Event: Storage medium lost, then found and accessed; information publicly disclosed.
Consequences: Asset confidentiality lost. Reputation lost.
Control (treating vulnerability): Storage media encryption.
Risk treatment (avoiding risk): Do not use portable media.
Risk treatment (removing the source of risk): Not applicable.

4. CONCLUSION

Therefore, to successfully and effectively apply and implement cyber and information security, it is necessary to understand the basic principles and concepts used in this area. The present paper specifically focused on the

legislative and technical characteristics of the most commonly used cyber and information security terms that are often considered notoriety.

From the presented analysis it is clear that these terms can be interpreted quite differently in different situations by different actors. This can lead to their inappropriate or even incorrect use. This misuse can be highly misleading and may result in a misconfigured information and cybersecurity management system.

All technical and legal documents which have been used within the article work with terms that are not used doctrinally and uniformly. On the contrary, they are often used synonymously and are also often overused in situations where their use is inappropriate. This degree of linguistic creativity can be observed both at the international and, in particular, at the national level in the context of the transposition of EU legal norms into national legislation.

For this article, definitions based on ISO/IEC 27000, NIST, CISA, NIS 1, and NIS 2 have been used. In this article, the authors sought to highlight the ambiguity in the interpretation of key cyber and information security concepts, both within and outside the European Union. A secondary aim was to highlight the not-always-clear and unambiguous terminology used in the NIS2 framework.

The purpose of this article was to highlight the differences described above and to suggest a possible starting point that would provide a generally accepted framework for the terminology in question for technical, legal, and user professionals alike.

Based on the comparisons of both technical and legal standards and the subsequent presentation of the links between the key concepts of cybersecurity within the Conceptual Model, the authors present the following conclusions:

- An asset is anything that has value and contributes to the achievement of an organization's objectives.
- An event is an occurrence or change of a particular set of circumstances within a particular domain; it is something that has happened, or is contemplated as having happened in that domain. We refer to a potential event as an eventuality.
- The threat is an eventuality that can be expected to have negative consequences for the objective.
- Vulnerability can be concluded as a weakness of an asset or control that can be exploited by a threat.

- Risk can be understood as the effect of uncertainty, resulting from the lack of information related to the likelihood and consequences of an eventuality, on the objectives.
- Control is a measure that maintains and/or modifies risk.

The presented Conceptual Model represents the basic framework, to which further sub-relations can be added. The article and its conclusions can therefore be used in further unification of technical and legal terminology.

The authors are convinced that the analysis, comparisons, and findings presented can contribute to a better understanding of the whole issue of cyber and information security. They can also contribute to a better transposition of European legal standards into national legislation, especially by using sufficiently general, non-confusing terminology.

LIST OF REFERENCES

[1] Cichonski, P. et al. (2012) Computer Security Incident Handling Guide [online]. *NIST Special Publication (SP)*, 800-61 Rev. 2. Gaithersburg, MA: National Institute of Standards and Technology. Available from: doi: https://doi.org/10.6028/NIST.SP.800-61r2

[2] *Committee on National Security Systems (CNSS) Glossary* [online]. Available from: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf [Accessed 10 January 2023].

[3] Council Decision 92/242/EEC on the security of information systems.

[4] *Cyber-attacks have tripled in past year, says Ukraine's cybersecurity agency* [online]. The Guardian. Available from: https://www.theguardian.com/world/2023/jan/19/cyber-attacks-have-tripled-in-past-year-says-ukraine-cybersecurity-agency [Accessed 20 February 2023].

[5] *The Cybersecurity Strategy* [online]. European Commission. Available from: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy [Accessed 8 August 2023].

[6] 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.

[7] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[8] Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce).

[9] Directive 2002/19/EC of the European Parliament and of the Council on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive).

[10] Directive 2008/114/EC of the European Parliament and of the Council on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[11] Directive 91/250/EEC of the European Parliament and of the Council on the legal protection of computer programs.

[12] *Explore Terms: A Glossary of Common Cybersecurity Words and Phrases* [online]. NICCS. Available from: https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary [Accessed 10 January 2023].

[13] *Glossary* [online]. ENISA. Available from: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/glossary [Accessed 10 January 2023].

[14] Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. [online]. NIST Special Publication (SP) 800-37 Rev. 1 Gaithersburg, MA: National Institute of Standards and Technology 2019.

[15] *Guide for Conducting Risk Assessments: Information Security* [online]. NIST. Available from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf [Accessed 10 January 2023].

[16] *Industroyer2: Industroyer reloaded* [online]. Eset. Available from: https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ [Accessed 20 February 2023].

[17] ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary.

[18] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

[19] ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls.

[20] ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks.

[21] Kolouch, J. and Bašta, P. *CyberSecurity*. Praha, 2019: CZ.NIC. ISBN 978-80-88168-31-7.

[22] Niblett, P., Etzion, O. (2012) *Event Processing in Action*. Manning. ISBN 9781638352624.

[23] Regulation 460/2004/EC of the European Parliament and of the Council establishing the European Network and Information Security Agency, as amended by Regulation 1007/2008.

[24] *Russia's war on Ukraine: Timeline of cyber-attacks* [online]. European Parliament. Available from: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549 [Accessed 20 February 2023].

[25] Solms, R.V., & Niekerk, J.F. (2013). *From information security to cyber security. Comput. Secur., 38, 97-102*.

MUJLT Official Partner (Czech Republic)

ROWAN LEGAL, advokátní kancelář s.r.o
https://rowan.legal

Cyberspace 2022 Partners

Zákony pro lidi - AION CS
https://www.zakonyprolidi.cz

CODEXIS - ATLAS consulting
https://www.codexis.cz

Právní prostor
https://www.pravniprostor.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