MASARYK UNIVERSITY JOURNAL OF LAW AND TECHNOLOGY

VOLUME 13 | NUMBER 2 | FALL 2019 | ISSN 1802-5943

PEER REVIEWED

CONTENTS:

www.journals.muni.cz/mujlt

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

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

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

licensed as peer-reviewed scientific journal by the Research and Development Council of the Government of the Czech Republic
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 **13** | NUMBER **2** | FALL **2019**

LIST OF ARTICLES

LIST OF COMMENTARIES

LIST OF BOOK REVIEWS

DOI 10.5817/MUJLT2019-2-1

CLOUD COMPUTING CONTRACTS AS CONTRACTS FOR THE SUPPLY OF DIGITAL CONTENT: CLASSIFICATION AND INFORMATION DUTY[*]

by

KRZYSZTOF ŻOK[**]

Cloud computing contracts are among the most frequently concluded contracts over the Internet. Until now, however, they have been considered mainly from the perspective of data protection and intellectual property laws. Although these analyses provide valuable insights, they do not fully cover an important area, i.e. consumer protection. The article focuses on the latter issue, taking Consumer Rights Directive as a reference point. The Directive is one of the latest acts concerning consumer protection in the European Union. It also introduces a new type of agreement that should cover cloud computing contracts. In addition, characteristically for European law, it provides for an information duty as a means of consumer protection. The article examines these two aspects by seeking an answer to the following questions: (1) do cloud computing contracts classify as contracts for the supply of digital content? And (2) do the provisions on information duty suit well cloud computing contracts? The analysis includes the results of empirical studies of these contracts. In the conclusion, the article states that the new type of contract may not significantly improve consumer protection, mainly due to the ambiguity resulting from recital 19 of the Directive. On the other hand, consumers may benefit from the provisions on information duty, though it does not directly address the main problems connected with cloud computing contracts.

[*] The article is the result of a research project implemented under the grant No. 2015/19/D/HS5/00006 financed by the National Science Centre, Poland.

[**] krzysztof.zok@amu.edu.pl, assistant professor (adjunct) at the Faculty of Law and Administration of Adam Mickiewicz Univeristy in Poznań, Poland.

The article is divided into four parts. The first provides an introduction to the topic. The second discusses cloud computing contracts as contracts for the supply of digital content. The third analyses the provisions on information duty from the point of view of the contracts under consideration. Finally, the fourth summarises previous comments.

KEY WORDS

Cloud Computing Contracts, Consumer Protection, Digital Content, Information Duty

1. INTRODUCTION

Technical progress has an important influence on private law. This is particularly evident in the case of the Internet which has changed the way contracts are concluded and performed. A similarly revolutionary impact is also attributed to cloud computing.[1] This IT-solution offers various advantages, including costs reduction, access to previously unavailable functionalities or simply greater convenience.[2] Consequently, the question arises how clouds will affect private law. So far, cloud computing contracts have been primarily considered from the perspective of copyright and data protection. Such reference points are understandable, given that a computer program and information it processes constitute an intangible asset. The analysis undoubtedly leads to insightful conclusions. However, there is also another important issue that has not yet been addressed, i.e. the question of consumer protection in cloud computing contracts. Some authors even claim that focusing on contractual rights and duties is characteristic of the American rather than the European approach to cloud computing.[3] I believe that the following considerations can at least partially fill the gap.

---

1 See European Commission. (2012) *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions 'Unleashing the Potential of Cloud Computing in Europe'*. (COM(2012) 529 final). [online], pp. 2–6. Available from: http://ec.europa.eu/transparency/regdoc/rep/1/2012/EN/1-2012-529-EN-F1-1.Pdf [Accessed 14 March 2019].

2 Bradshaw, D. et al. (2014) *Uptake of Cloud in Europe Follow-up of IDC Study on Quantitative estimates of the demand for Cloud Computing in Europe and the likely barriers to take-up*. [online] Luxembourg: Publications Office of the European Union, pp. 8, 13. Available from: https://publications.europa.eu/en/publication-detail/-/publication/cfe5a91c-85cf-4c64-99e9-1b5900c8529a/language-en/format-PDF/source-search [Accessed 14 March 2019].

3 Celestine, C. M. (2013) "Cloudy" Skies, Bright Futures? In Defense of a Private Regulatory Scheme for Policing Cloud Computing. *Journal of Law, Technology and Policy*, 1, p. 157.

European law protects consumers in several acts, forming a patchwork of regulations.[4] I would like to focus the following considerations mainly on Consumer Rights Directive ("CRD" or "the Directive").[5] There are two reasons for choosing this frame of reference. Firstly, it is one of the most recent acts related to consumer protection. Therefore, it should respond to legal challenges arising from the use of new technologies.[6] Moreover, the *European Commission* pointed out in 2012 that the rules of the draft Common European Sales Law Regulation ("CESL Regulation")[7] address *"some aspects of cloud computing"*[8]. The statement was then upheld in the decision on setting up an expert group on cloud computing contracts.[9] Though the Regulation was never adopted, its ideas influenced the provisions of Consumer Rights Directive. Secondly, the Directive develops the *acquis* of its predecessors by introducing a contract for the supply of digital content.[10] This new type of agreement seems specifically tailored for the delivery of intangible assets. Consequently,

---

4 See Weatherill, S. (2012) The Consumer Rights Directive: How and Why a Quest for "Coherence" Has (Largely) Failed. *Common Market Law Review,* 4, pp. 1281–1286; Weatherill, S. (2013) *EU Consumer Law and Policy.* 2nd ed. Cheltenham-Northampton: Edward Elgar, p. 141.

5 Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council. *Official Journal of the European Union* (2011/L-304/64) 22 November. Available from: http://data.europa.eu/eli/dir/2011/83/oj [Accessed 14 March 2019].

6 See Markou, Ch. (2017) Directive 2011/83/EU on Consumer Rights. In: Arno R. Lodder and Andrew D. Murray (eds.). *EU Regulation on E-Commerce.* Cheltenham-Northampton: Edward Elgar, pp. 181–182; Weatherill, S. (2013) *EU Consumer Law and Policy.* 2nd ed. Cheltenham-Northampton: Edward Elgar, p. 112.

7 European Commission. (2011) *Proposal for a Regulation of the European Parliament and of the Council on a Common European Sales Law.* (COM(2011) 635 final). [online] Available from: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52011PC0635 [Accessed 14 March 2019].

8 European Commission. (2012) *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions 'Unleashing the Potential of Cloud Computing in Europe'.* (COM(2012) 529 final). [online], pp. 9, 11–12. Available from: http://ec.europa.eu/transparency/regdoc/rep/1/2012/EN/1-2012-529-EN-F1-1.Pdf [Accessed 14 March 2019].

9 Recital 6 – Commission Decision of 18 June 2013 on setting up the Commission expert group on cloud computing contracts. *Official Journal of the European Union* (2013/C-174/6) 20 June. Available from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:174:0006:0008:EN:PDF [Accessed 14 March 2019].

10 Council Directive 85/577/EEC of 20 December 1985 to protect the consumer in respect of contracts negotiated away from business premises. *Official Journal of the European Communities* (1985/L-371/31). Available from: https://eur-lex.europa.eu/eli/dir/1985/577/oj [Accessed 14 July 2019]; Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts. *Official Journal of the European Communities* (1997/L-144/19) 20 May. Available from: https://eur-lex.europa.eu/eli/dir/1997/7/oj [Accessed 14 July 2019].

the question arises as to how it applies to cloud computing contracts. The answer is important to understand the way clouds work and the risks they pose.

This is in turn connected with the information duty, viewed as *"the core of the Directive"*[11]. The duty aims at correcting the imbalance of the bargaining process by removing information asymmetry, a source of consumer's weaker position.[12] The approach is market-neutral since it respects the autonomy of the parties and their private negotiations.[13] In American literature, it is even seen as a distinctively European perspective on cloud computing contracts.[14] The survey from 2012 confirms the need for such a regulation, indicating that middle and low value (i.e. consumer-oriented) cloud markets are still limited in information.[15] However, the consumer should be "properly" informed, which means that they receive information relevant to the transaction. The elaboration (sometimes regarded as the overgrowth[16]) of the information duty raises the question if the Directive covers the areas that should be balanced in favour of the consumer.

2. CONTRACTS FOR THE SUPPLY OF DIGITAL CONTENT

2.1. GENERAL OVERVIEW

The concept of a contract for the supply of digital content dates back to the CESL Regulation. However, the draft did not clarify the nature of this agreement, even though several provisions referred to it. Consumer Rights Directive adopts a similar approach. Its provisions do not define the contract for the supply of digital content. Nevertheless, recital 19 of the CRD offers some insight into the essence of this agreement. In my opinion, there are two basic elements of this contract.

---

[11] Weatherill, S. (2013) *EU Consumer Law and Policy.* 2nd ed. Cheltenham-Northampton: Edward Elgar, p. 112.

[12] Markou, Ch. (2017) Directive 2011/83/EU on Consumer Rights. In: Arno R. Lodder and Andrew D. Murray (eds.). *EU Regulation on E-Commerce.* Cheltenham-Northampton: Edward Elgar, p. 195.

[13] Weatherill, S. (2013) *EU Consumer Law and Policy.* 2nd ed. Cheltenham-Northampton: Edward Elgar, p. 92.

[14] Celestine, C. M. (2013) "Cloudy" Skies, Bright Futures? In Defense of a Private Regulatory Scheme for Policing Cloud Computing. *Journal of Law, Technology and Policy*, 1, p. 156.

[15] Hon, W. K., Millard, Ch. and Walden, I. (2012) Negotiating Cloud Contracts: Looking at Clouds from both Sides Now. *Stanford Technology Law Review*, 16 (1), p. 127.

[16] Weatherill, S. (2012) The Consumer Rights Directive: How and Why a Quest for "Coherence" Has (Largely) Failed. *Common Market Law Review*, 4, pp. 1293–1294.

Firstly, Article 2 (11) of the Directive broadly defines digital content as data produced and supplied in digital form. Recital 19 of the CRD develops this concise explanation by listing examples of digital content such as computer programs, music, videos or texts. From this perspective, cloud computing contracts easily fit into the category of contracts related to digital content. The NIST recommendations, a document often cited in the context of cloud computing, support the conclusion.[17] As indicated therein, three main cloud service model, i.e. *Software as a Service ("SaaS")*, *Platform as a Service ("PaaS")* and *Infrastructure as a Service ("IaaS")*, focus on remote use of computer programs.

Secondly, the data should be transferred by one party to the other. The word "supply" in the name of the contract indicates this requirement. Moreover, Article 2 (11) and recital 19 of the Directive treat the supply of data as an intrinsic element of the concept of digital content. Moreover, according to recital 19 of the CRD, data stored on a tangible medium constitutes goods within the meaning of Article 2 (11) thereof. As a result, the supply of such digital content is subject to the provisions on delivery of goods, which in turn confirms the above requirement to transfer the data. The conclusion also corresponds with the technical aspect of using digital content. Computers can present the data only if it is loaded into their storage, even if it is transient as in the case of *Random Access Memory (RAM)*.[18] Therefore, the transfer of the content is necessary for the other party to perceive the data. Similarly, recital 19 of the Directive recognises that the supply of the digital content can be permanent (i.e. a consumer downloads a file) or temporary (i.e. a consumer only accesses the content, e.g. in the form of streaming).

However, the Directive does not explicitly state that data should be supplied by the trader. As a result, one could argue that the classification of a contract as a contract for the supply of digital content does not depend on the person who delivers the data. On the other hand, several provisions indirectly contradict this statement. The rules on digital content concern mainly the obligations of the trader who is treated as having the best

[17] Mell, P. and Grance, T. (2011) *The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology.* Gaithersburg: National Institute of Standards and Technology, pp. 2–3. [online] Available from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf [Accessed 14 March 2019].

[18] Wikipedia. (2019) *Software*. [online] Available from: https://en.wikipedia.org/wiki/Software [Accessed 21 July 2019].

information about the subject matter of the contract.[19] Consequently, it can be assumed that this knowledge arises from possessing the data, which leads to the conclusion that the trader is the party who should supply digital content. This is further supported by Articles 17 (1) and 18 regulating the delivery of the content by the trader. Besides, the right of withdrawal generally refers to the situations in which the consumer is the person who received or should have received the data.[20]

The assumption that the trader should supply the data is also supported by the analysis of the legislative process in which the Directive has been adopted. Except for a minor reference to *"data files download by the consumer"*, the *European Commission* initially did not create a set of provisions on contracts for the supply of digital content.[21] This was later criticised by the MEPs who introduced the terms "digital content" and "intangible moveable item" of which only the first one was adopted in the Directive.[22] As indicated in their report, the content was to be "transmitted" and "downloaded".[23] Similarly, during the debate on the proposal for the Directive, MEPs said that consumers would be downloading and purchasing digital content.[24] In addition, *Directorate--General for Justice* presents the same stance in the Guidance to the CRD.[25] This document also states that

---

[19] Article 5 (1) and (2), 6 (1) and (2) as well as recital 19 of the CRD.

[20] Article 9, 14 and recital 40, 46, 49, 51, 55 of the CRD with the exception in Article 16 (m) and recital 19 thereof concerning the supply of digital content on an intangible medium.

[21] European Commission. (2008) *Proposal for a Directive of the European Parliament and of the Council on consumer rights.* (COM(2008) 614 final). [online] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2008:0614:FIN [Accessed 20 July 2019].

[22] European Parliament. (2011) *Report on the proposal for a directive of the European Parliament and of the Council on consumer rights.* [online] Available from: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2011-0038+0+DOC+PDF+V0//EN [Accessed 20 July 2019].

[23] Proposals of amendments of Article 10 (1) (ha) and recital 11e – op. cit. See also the amendment of recital 10a proposed by the Committee on Legal Affairs and recital 12a proposed by Committee on Economic and Monetary Affairs – op. cit.

[24] European Parliament. (2011) *Debates: Wednesday, 23 March 2011 – Brussels.* [online] Brussels: European Parliament. Available from: http://www.europarl.europa.eu/sides/getDoc.do?type=CRE&reference=20110323&secondRef=ITEM-020&language=EN&ring=A7-2011-0038 [Accessed 15 July 2019]; European Parliament. (2011) *Debates: Thursday, 23 June 2011 – Brussels.* [online] Brussels: European Parliament. Available from: http://www.europarl.europa.eu/sides/getDoc.do?type=CRE&reference=20110623&secondRef=ITEM-014&language=EN&ring=A7-2011-0038#4-223-000 [Accessed 15 July 2019].

[25] Directorate-General for Justice. (2014) *DG Justice Guidance Document concerning Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council.* [online] pp. 64–65. Available from: https://ec.europa.eu/info/sites/info/files/crd_guidance_en_0.pdf [Accessed 16 July 2019].

> *"the Directive does not seem to apply to contracts under which it is the consumer who transfers goods to the trader".*[26]

The conclusion has been subsequently accepted by some authors.[27] Therefore, one can conclude that digital content should be supplied by the trader. A contract that obliges a consumer to provide data does not constitute a contract for the supply of digital content. However, it may be qualified as a service contract within the meaning of Article 2 (6) thereof.

From this perspective, one may ask how do cloud computing contracts fit into the category of contracts for the supply of digital content. The above scheme fits well with *SaaS* contract. In this case, the consumer is interested in using a computer program in the cloud.[28] The provider supplies the application through a thin client (e.g. a web browser) or a program interface. Consequently, the transfer of data is requested by the consumer. It also forms the subject matter of *SaaS* contract. Moreover, the assumption remains valid when it comes to *PaaS* contract. This time, the consumer wants to get a software environment to host his applications.[29] The provider supplies it as digital content. Nevertheless, the consumer, not the provider, installs the applications in the cloud environment. Therefore, the transfer of digital content forms the subject matter of *PaaS* contract, though only a certain amount of data is uploaded at the request of the consumer.

On the other hand, the supply of digital content seems questionable in the case of *IaaS* contract. In this cloud service model, the consumer is not interested in accessing the applications supplied by the provider. Instead, the consumer wants to use provider's hardware resources, such as data processing or storage.[30] From this perspective, there is no digital content relevant for the parties which could be treated as the subject matter of *IaaS* agreement. However, the conclusion can be challenged by stating that cloud management involves the use of computer programs mentioned in recital 19 of the CRD as digital content. The argument seems even more

---

[26] Op. cit., pp. 5–6.

[27] Markou, Ch. (2017) Directive 2011/83/EU on Consumer Rights. In: Arno R. Lodder and Andrew D. Murray (eds.). *EU Regulation on E-Commerce.* Cheltenham-Northampton: Edward Elgar, p. 186.

[28] Mell, P. and Grance, T. (2011) *The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology.* Gaithersburg: National Institute of Standards and Technology, p. 2. [online] Available from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf [Accessed 14 March 2019].

[29] Op. cit., pp. 2–3.

[30] Op. cit., p. 3.

convincing, given the demonstrative character of a list provided for in the recital. In my opinion, this view does not seem correct. While software as such constitutes digital content within the meaning of Article 2 (11) and recital 19 of the Directive, its use in the cloud is only instrumental for *IaaS* contract. A computer program does not form the main subject matter of this agreement. This suits the purpose of *IaaS* contract. A consumer concludes this agreement to fill the cloud with the digital content arbitrarily selected by them, not to exploit data supplied by the provider. Moreover, digital content is supplied by the consumer, which contradicts the previous conclusion that contracts for the supply of digital content require the trader to supply the data.

It is also worth noting that currently many items are equipped with software (e.g. various smart devices). However, these computer programs often do not form the main subject matter of a contract. Their role is only instrumental as they are needed for proper use of the item. If one assumes that even minimal amount of data is sufficient to classify a contract as a contract for the supply of digital content, then one has also to conclude that this qualification will apply to a significant number of everyday contracts. This is contrary to the idea put forward by the lawmakers as well as the guidelines issued by the *Directorate-General for Justice*. From both these points of view, contracts for the supply of digital content concern primarily the data (e.g. music or film files), not hardware. In my opinion, the questioned stance would seem also counter-intuitive to consumers. For this reason, *IaaS* contracts should not be classified as contracts for the supply of digital content. It is necessary to emphasise that this conclusion does not leave consumers unprotected. *IaaS* contract can be still regarded as a service contract within the meaning of Article 2 (6) of Consumer Rights Directive.

2.2. INTANGIBILITY OF THE MEDIUM

Although recital 19 of the CRD states that digital content can be supplied in any form, its medium is not irrelevant for consumer protection. This is also the perspective from which the Directive address the question of the classification of contracts related to digital content. Their nature has been a subject of legal controversy as to whether they should be regarded

as sales contracts or service contracts.[31] A detailed analysis of this matter would certainly exceed the volume limits for this article. However, such presentation is not necessary because the Directive has resolved this controversy by distinguishing two types of contracts for digital content. The distinction is based on the type of medium used to convey the data.

On the one hand, recital 19 of the CRD provides that digital content on a tangible medium should be perceived as goods within the meaning of Article 2 (4) thereof. This is an important statement in the light of Article 2 (7) of the Directive. According to this provision, a distance contract should be concluded under *"organised distance sales or service--provision scheme"*. The organisation requirement is usually met in the case of traders who act as professionals. Moreover, as indicated in Article 2 (5) of the CRD, a sales contract is a contract under which the trader transfers or undertakes to transfer the ownership of goods to the consumer in exchange for the payment of the price. Therefore, a contract for the supply of digital content on a tangible medium can be classified as a sales contract. Alternatively, if the contract for the supply of digital content on a tangible medium does not transfer ownership, it can be qualified as a service contract within the meaning of Article 2 (6) of the Directive. The latter conclusion also corresponds to the broad understanding of services in European law.[32]

On the other hand, the Directive does not specify the status of digital content supplied otherwise than on a tangible medium (for the purpose of this article, the term "digital content on an intangible medium" is used to designate such data). Instead, recital 19 of the CRD indicates that a contract for the supply of this type of digital content should not be treated as a sales contract or a service contract. Consequently, it cannot be classified as a distance contract. Some provisions on distance contracts explicitly refer also to contracts for the supply of digital content on an intangible medium.[33] However, in my opinion, this does not substantiate the identification of both contracts. Otherwise, it is difficult to justify separate rules for contracts for the supply of digital content on an intangible medium. If they

[31] See Bezáková D. (2013) The Consumer Rights Directive and its Implications for Consumer Protection Regarding Intangible Digital Content. *Masaryk University Journal of Law and Technology*, 7 (2), pp. 181–183.

[32] Article 50 – Consolidated version of the *Treaty on the Functioning of the European Union*, 13 December 2007 (2012/C-326/1). [online] Available from: https://eur-lex.europa.eu/eli/treaty/tfeu_2012/oj [Accessed 20 July 2019].

[33] See Articles 6 (2), 9 (2) (c), 14 (4) (b), 16 (m) of the CRD.

were simply distance contracts, there would be no need for additional provisions.

Moreover, sales and service contracts require a monetary remuneration from the consumer. As a result, the contracts in which the consumer does not pay for the goods or services as well as the contract in which they provide the trader with a non-monetary remuneration are excluded from the scope of Article 2 (5) and (6) of the CRD.[34] Consequently, consumer protection would be weakened if contracts for the supply of digital content on an intangible medium were classified as sales or service contracts. This results from the fact that consumer-oriented providers frequently do not charge a fee but instead derive their income from a non-monetary remuneration (see part 3.2.2.).

It should be emphasised that excluding contracts for the supply of digital content on an intangible medium from the notion of distance contracts is often more theoretical than practical. The situation of a consumer who has concluded a contract for the supply of digital content on an intangible medium is significantly similar to the situation of a consumer who has concluded a distance contract, in particular a distance service contract.[35] This results from the fact that the Directive in many provisions on the contracts for the supply of digital content on an intangible medium refers to the rules concerning the distance contracts. Therefore, the current regulation can be seen as a way of solving the problem of the classification of contracts related to digital content, even if it is somewhat counter-intuitive at first sight.

Although the term "digital content on an intangible medium" is only an expression of a conceptual convention used to describe the subject matter of a contract for the supply of data otherwise than by transferring the carrier on which it is stored, it needs some additional clarification.

---

[34] Markou, Ch. (2017) Directive 2011/83/EU on Consumer Rights. In: Arno R. Lodder and Andrew D. Murray (eds.). *EU Regulation on E-Commerce.* Cheltenham-Northampton: Edward Elgar, pp. 187. See also Directorate-General for Justice. (2014) *DG Justice Guidance Document concerning Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council.* [online] pp. 8, 64. Available from: https://ec.europa.eu/info/sites/info/files/crd_guidance_en_0.pdf [Accessed 16 July 2019].

[35] Markou, Ch. (2017) Directive 2011/83/EU on Consumer Rights. In: Arno R. Lodder and Andrew D. Murray (eds.). *EU Regulation on E-Commerce.* Cheltenham-Northampton: Edward Elgar, pp. 187–188.

In the context of electronic commerce and intellectual property, the word "medium" is usually understood as

> *"a particular form of storage material for computer files, such as magnetic tape or discs"* or more generally as *"the material or form used by an artist, composer or writer"*.[36]

Consequently, the term implies physicality of the item containing the data. Similarly, recital 23 of the CRD defines the expression "durable medium" as a corporeal thing storing the information. The recital also lists examples of the medium which includes

> *"paper, USB sticks, CD-ROMs, DVDs, memory cards […], hard disk of computers as well as e-mails"*.

As a result, when taken literally, the expression "intangible medium" may seem self-contradictory, particularly if one considers that data is almost always stored on some kind of a tangible medium (e.g. a server), even though the user might not have direct access to this device. Therefore, it is necessary to highlight that the term "digital content on an intangible medium" is just a construct created in opposition to a more common notion of "digital content a (tangible) medium". It aims to cover various ways in which the consumer can access the data without receiving goods within the meaning of Article 2 (3) of the Directive.

In my opinion, the main difference between contracts for the supply of digital content does not depend on the type of medium on which the data is stored, but rather on the way in which the consumer has access to it. If they can directly use digital content, then the situation is similar to possessing a good. The condition is met, for instance, in the case of a computer program stored on a CD, DVD or a USB stick which was given to a consumer. Recital 19 of the CRD further confirms this conclusion by treating digital content on a tangible medium as goods. However, if the consumer has only indirect access to data, the similarity to possessing a good becomes questionable. The consumer does not enjoy the full control of data because the use of it is always mediated by somebody else (e.g. a provider). The situation poses serious risks for them such as being

[36] Oxford University Press. (2019) *Oxford Dictionaries.* [online] Oxford University Press. Available from: https://en.oxforddictionaries.com/definition/medium [Accessed 14 March 2019].

locked in the contract or losing confidential information. These drawbacks also justify a separate regulation of this type of agreements.

2.3. CLOUD COMPUTING AS "INTANGIBLE MEDIUM"

The question arises how to classify *SaaS* and *PaaS* contracts. In both cases, the consumer does not manage or control the cloud.[37] When it comes to *SaaS* contracts, the restriction also extends to the application used by the consumer. He can only change some of the settings to adjust the program to his needs. The provider in turn controls not only executable files, but also data files. The consumer is more independent in the case of *PaaS* contracts. They can manage the applications they deployed onto the cloud. However, the provider controls the environment in which the consumer runs their software. As a consequence, the consumer has only indirect access to digital content in *SaaS* and *PaaS* contracts. Therefore, they should be qualified as contracts for the supply of digital content on an intangible medium. The risks typical for these agreements confirm this conclusion (see part 3.2. of the article).

Moreover, the consumer accesses digital content in the cloud in a way similar to streaming, a method mentioned in recital 19 of the CRD. The latter process is characterised by dividing digital content into smaller parts which are sent to the user.[38] Due to the high speed of data transmission, the user can perceive the full content, though he never acquired it as a whole (e.g. he never gets a complete film or music file). In the case of cloud computing, the division of digital content is not necessary. However, the exploitation of the content also employs the process of transmission. The input data is sent to the provider's server which performs computational tasks and transmits the output back to the consumer. The exchange of the data is rapid enough to make the process seem as if the consumer used the main computer program in the cloud without any intermediaries. Despite this difference, I believe that cloud computing may be compared to streaming because both ways of exploiting digital content rely on data transmission and they do not allow the consumer to fully and directly access the content.

[37] Mell, P. and Grance, T. (2011) *The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology.* Gaithersburg: National Institute of Standards and Technology. [online] pp. 2–3. Available from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf [Accessed 14 March 2019].

[38] Lu, Th. Y. (2018) Understanding Streaming and Copyright: A Comparison of the United States and European Regimes. *Journal of Business and Technology Law*, 13 (2), pp. 187–188.

Finally, recital 19 of the CRD treats contracts for the supply of digital content on an intangible medium as similar to contracts for the supply of water, gas or electricity. The conclusion operates on the assumption that the delivery of these items takes place in parts, i.e. by selling them in a limited volume or set quantity. The same reasoning applies to cloud computing contracts because the access to the computer program in the cloud is usually counted into units of time or amount of data sent through the Internet. It is worth noting that the metaphor of utility services is often employed to describe cloud services.[39]

3. INFORMATION DUTY

3.1. GENERAL OVERVIEW

The Directive provides for two kinds of information duty depending on the type of contract concluded by the consumer. As indicated in Article 5 of the CRD, basic information duty applies to contracts other than distance contracts or off-premises contracts. Otherwise, if the consumer concludes a distance contract, Article 6 thereof imposes a detailed information duty on the trader. From this perspective, the classification of cloud computing contracts plays a decisive role in determining the proper information duty. The case of *IaaS* contracts is the easiest. Since they do not qualify as contracts for the supply of digital content, they should be treated as service contracts within the meaning of Article 2 (6) of the CRD and consequently also as distance contracts. However, a literal reading of recital 19 thereof could lead to a conclusion that *SaaS* and *PaaS* contracts do not fall under Article 2 (7) of the Directive. This would lead to a paradoxical outcome: the consumer would benefit from more intense protection in the agreements he concludes relatively rarely (*IaaS* contracts). At the same time, his protection would weaken when concluding cloud agreements typical for the consumer (*SaaS* and *PaaS* contracts). Fortunately, this stance is countered in Article 6 (2) of the CRD, according to which the rules on information duty in the case of distance contracts also apply

[39] Bradshaw, S., Millard, Ch. and Walden, I. (2011) Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. *International Journal of Law and Information Technology*, 19 (3), p. 190; Calloway, T. J. (2011) Cloud Computing, Clickwrap Agreements, and Limitation on Liability Clauses: A Perfect Storm? *Duke Law and Technology Review*, 11 (1), pp. 166–167; McCorry, D. (2014) With Cloud Technology, Who Owns Your Data?. *The Federal Courts Law Review*, 8 (1), p. 129; McGillivray, K. (2014) Conflicts in the Cloud: Contracts and Compliance with Data Protection Law in the EU. *Tulane Journal of Technology and Intellectual Property*, 17, pp. 252–253.

to contracts for the supply of digital content on an intangible medium. This reference should be considered accurate. Some of the information listed in Article 6 (1) of the CRD concern the general description of the contract (e.g. the main characteristics of the subject matter of the agreement, trader's identity or the price and the method of payment). In my opinion, in this respect, cloud computing contracts do not differ significantly from other contracts. Therefore, I would like to focus the considerations on the areas specific to cloud computing contracts. In addition, to better illustrate the specificity of information duty in the context of the above contracts, I would also like to refer to the surveys published in 2011 and 2012. Findings in these studies are consistent and remain valid. Thus, they constitute a valuable source of information.

3.2. FUNCTIONALITY AND RELEVANT INTEROPERABILITY

According to Article 6 (1) (r) and (s) of the CRD, the trader should inform the consumer about the functionality and the relevant interoperability of digital content. Consequently, some authors stress the significance of this provision, stating that otherwise it would be difficult to infer a similar information duty under Article 6 (1) (a) of the Directive.[40] Moreover, recital 19 thereof states information on the functionality and relevant interoperability "in addition" to general information duty. This seems to support the autonomy of the above requirements. However, in my opinion, the description of the main characteristics of cloud service contract – provided for in Article 6 (1) (a) of the CRD – could also partly include information about functionality and interoperability or at least their most important elements. As indicated in recital 19 of the Directive, the term "functionality" means the ways in which digital content can be used, while the expression "relevant interoperability" refers to the standard hardware and software environment with which digital content is compatible. Typical cloud computing contracts describe how the consumer can use the cloud and what actions are prohibited.[41] Moreover, the contracts often determine the availability of the cloud, either guaranteeing a specified

[40] Markou, Ch. (2017) Directive 2011/83/EU on Consumer Rights. In: Arno R. Lodder and Andrew D. Murray (eds.). *EU Regulation on E-Commerce.* Cheltenham-Northampton: Edward Elgar, p. 200.

[41] Bradshaw, S., Millard, Ch. and Walden, I. (2011) Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. *International Journal of Law and Information Technology*, 19 (3), pp. 200–202, 214–215.

level of performance or excluding such expectations.[42] Nevertheless, I agree that an explicit listing of this information requirement in Article 6 (1) (r) and (s) of the Directive is more consumer-friendly.

However, the information in Article 6 (1) (r) and (s) of the CRD is generic in nature. The explanation in recital 19 thereof also remains vague. More detailed requirements have been provided for in the guidelines issued by the *Directorate-General for Justice*, although it is also not cloud-specific but applies to digital content in general.[43] Therefore, the main obstacle lies in applying these concepts to cloud computing contracts. In particular, one may ask how detailed the information should be to provide the consumer with adequate knowledge and at the same time to not overwhelm them with information. In my opinion, the provider should notify the consumer at least about the type of cloud service model, the use of the cloud (including the list of prohibited actions), the minimal and optimal requirements to run software and the level of service availability.[44] Besides, the information about the functionality and the relevant interoperability should also refer to the data in the cloud. As indicated in Article 2 (11) of the Directive, data is the core element of the definition of digital content. In my opinion, five key areas need to be covered by the information duty, i.e. data integrity, portability, preservation, confidentiality and location. These are also the issues cloud users often struggle with. Interestingly, the *European Commission* in 2012 and 2015 emphasised the significance of most of the above areas.[45] Nonetheless, the Directive does not name them directly.

---

[42] Op. cit., pp. 214–215.

[43] Directorate-General for Justice. (2014) *DG Justice Guidance Document concerning Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council.* [online] p. 64–68. Available from: https://ec.europa.eu/info/sites/info/files/crd_guidance_en_0.pdf [Accessed 16 July 2019].

[44] Ibid.

[45] See European Commission. (2012) *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions 'Unleashing the Potential of Cloud Computing in Europe'.* (COM(2012) 529 final). [online], p. 12. Available from: http://ec.europa.eu/transparency/regdoc/rep/1/2012/EN/1-2012-529-EN-F1-1.Pdf [Accessed 14 March 2019]; European Commission. (2015) *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'A Digital Single Market Strategy for Europe'* (COM(2015) 192 final). [online], pp. 14–15. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN [Accessed 14 March 2019].

3.2.1. DATA INTEGRITY

The survey from 2011 shows that cloud service providers often refrain from ensuring data integrity.[46] Instead, they pass on the task to the users.[47] Sometimes the provider may agree to perform backup services in exchange for an additional fee. Another study from 2012 also confirms that providers are reluctant to oblige to backup data.[48] Interestingly, the study indicates that providers usually backup twice or thrice data in the cloud. However, they do not want to undertake a contractual obligation. Probably, it results from the fact that severe failures happen even to the largest cloud service providers, such as *Google* or *Microsoft*.[49] If they had ensured that the data will not be corrupted due to a completely secure backup of files, they would be exposed to excessive liability that could prevent them from operating business. Moreover, the conclusion of a contract that does not oblige the provider to backup the data can sometimes be a reasonable decision for the consumer (for example, if the fee provided for in the contract is significantly lower).

On the other hand, the lack of backup obligation potentially leads to a situation where the consumer may not achieve the purpose for which he concluded the contract (e.g. reliable data storage). While avoiding taking on a general obligation to backup the data by the provider seems understandable, the consumer has to be aware of the risk of losing the data. Only then can they properly consider the situation, in particular the profitability of the agreement. Therefore, clear information about risks connected with cloud services plays a crucial role in the assessment of the contract.

3.2.2. DATA PORTABILITY

To switch the provider or to use a different computer program to process the information in the cloud, the consumer has to recover the data. However, it can be much more difficult than uploading the files in the first

---

[46] Bradshaw, S., Millard, Ch. and Walden, I. (2011) Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. *International Journal of Law and Information Technology*, 19 (3), pp. 203–204.

[47] Similarly Foster, T. N. (2013) Navigating Through the Fog of Cloud Computing Contracts. *John Marshall Journal of Information Technology and Privacy Law*, 30, p. 19.

[48] Hon, W. K., Millard, Ch. and Walden, I. (2012) Negotiating Cloud Contracts: Looking at Clouds from both Sides Now. *Stanford Technology Law Review*, 16 (1), pp. 94–95.

[49] See Calloway, T. J. (2011) Cloud Computing, Clickwrap Agreements, and Limitation on Liability Clauses: A Perfect Storm? *Duke Law and Technology Review*, 11 (1), pp. 170–171.

place. Some providers even try to disclaim any obligation to return the data.[50] The market itself also does not provide sufficient incentives for providers cooperation in the field of interoperability.[51] From this perspective, the information duty can prevent locking the consumer in the contract, which is a serious risk related to cloud computing.[52] There are two aspects of data portability that should be covered by the duty.

Firstly, some providers demand an extra fee for returning the data.[53] Although the survey from 2011 does not register this practice,[54] it is reported in the study from 2012.[55] Alternatively, the providers offer a new contract for assisted migration. Such practices may be justified by additional costs incurred by the provider to transfer the data from the cloud. Particularly, if the format in which the information is stored is not standardised or the amount of information that would be reformatted is significant for the provider. To illustrates this statement one can point out to *Facebook* which in 2012 collected over 1,5 petabytes (i.e. 1 million gigabytes) of photos or *Pinterest* which stored over 7,9 zettabytes (i.e. 1 trillion gigabytes) of data distributed between at least 18 million users.[56] However, the study from 2012 indicates that enterprise-oriented providers sometimes guarantee the return of the data in a standard format or a format chosen by the customer, especially if the amount of data is not significant.[57] Although this remark applies to business-to-business contracts, it points key factors that can be taken into account in the context of agreements concluded with consumers (i.e. the quality and quantity of returned data). Nevertheless, in the latter contracts, it can be expected

[50] Foster, T. N. (2013) Navigating Through the Fog of Cloud Computing Contracts. *John Marshall Journal of Information Technology and Privacy Law*, 30, p. 24.

[51] Soma, J. et al. (2011) Chasing the Clouds without Getting Drenched. A Call for Fair Practices in Cloud Computing Services. *Journal of Technology Law and Policy*, 16, p. 209.

[52] Hon, W. K., Millard, Ch. and Walden, I. (2012) Negotiating Cloud Contracts: Looking at Clouds from both Sides Now. *Stanford Technology Law Review*, 16 (1), pp. 115–116.

[53] Carpenter, R. H. Jr. (2010) Walking from Cloud to Cloud: The Portability Issue in Cloud Computing. *Washington Journal of Law, Technology & Arts*, 6 (1), pp. 3, 5–7.

[54] Bradshaw, S., Millard, Ch. and Walden, I. (2011) Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. *International Journal of Law and Information Technology*, 19 (3), pp. 204–205.

[55] Hon, W. K., Millard, Ch. and Walden, I. (2012) Negotiating Cloud Contracts: Looking at Clouds from both Sides Now. *Stanford Technology Law Review*, 16 (1), p. 97.

[56] McCorry, D. (2014) With Cloud Technology, Who Owns Your Data?. *The Federal Courts Law Review*, 8 (1), pp. 129–130.

[57] Hon, W. K., Millard, Ch. and Walden, I. (2012) Negotiating Cloud Contracts: Looking at Clouds from both Sides Now. *Stanford Technology Law Review*, 16 (1), p. 117.

that imbalance in bargaining power will make providers less inclined to meet consumers requests regarding the data format.

Another important factor to consider is the payment. If the contract provides for a fee, it seems reasonable for the consumer to expect that they will be able to download the data in a format readable by commonly used software, at least in a format similar to the one in which the data was uploaded. Therefore, in opinion, if the provider does not return the data in this format, they should at least inform the consumer. It should also be noted that cloud computing contracts often do not require the consumer to pay a fee.[58] However, this statement does not mean that the provider remains without any benefit from these agreements. He receives non--momentary remuneration from the consumer, for example by deriving income from creating a contextual advertisement.[59] From this point of view, it is important to reliably inform the consumer about the limitations of data portability, particularly about the costs of recovering digital content. Otherwise, the practice of cloud service providers can create an unjustified obstacle for the consumer to leave the contract. Moreover, such information is also beneficial for the provider because it eliminates potential doubts concerning the consumer's request to return the data in a specific form.

Secondly, retrieving the data can be difficult for the consumer. The survey from 2012 shows that the simplicity of switching may be a factor taken into account when choosing the provider.[60] However, the study also points out that most providers do not help in the transition. From a technical point of view, the consumer should know the format in which he will receive the files. The information is necessary to assess the readability of the data. Otherwise, he may recover the files that no other computer program will be able to process. Moreover, the providers often offer short timetables for returning data.[61] As a result, the consumer should consider a proper exit strategy. In particular, he should know if he can download the data after the contract has ended or if he has to do it in advance.

---

[58] Bradshaw, S., Millard, Ch. and Walden, I. (2011) Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. *International Journal of Law and Information Technology*, 19 (3), p. 196.

[59] Op. cit., p. 196. Similarly McCorry, D. (2014) With Cloud Technology, Who Owns Your Data? *The Federal Courts Law Review*, 8 (1), p. 146.

[60] Hon, W. K., Millard, Ch. and Walden, I. (2012) Negotiating Cloud Contracts: Looking at Clouds from both Sides Now. *Stanford Technology Law Review*, 16 (1), p. 116–117.

[61] McGillivray, K. (2014) Conflicts in the Cloud: Contracts and Compliance with Data Protection Law in the EU. *Tulane Journal of Technology and Intellectual Property*, 17, pp. 236–237.

3.2.3. DATA DELETION

In addition to the doubts resented above, the survey from 2011 shows that not all providers undertake to erase digital content after the contract has ended.[62] Consequently, the consumer risks that unauthorised persons will access his data. Moreover, it is difficult to determine if the data has actually been deleted from the cloud. The study from 2012 indicates that providers often only remove "pointers" to the data location, not the data itself.[63] Although the process leads to a gradual overwriting of the data over time, it is possible, at least to some extent, to recover the information after such deletion. It is well illustrated by the case of *Digitalocean* which did not delete the data of its customer.[64] Due to a malfunction, the files became viewable by other customers. The survey from 2012 also calls for educating consumers about the removal of data in the cloud.[65] I believe that detailed information on data deletion can be too complicated for an average user, particularly if it concerned purely technical aspects of data storage. This is important because the aim of information duty can be achieved only if the consumer can understand the information.[66] Nevertheless, he should be aware that the termination of the contract will not necessarily erase the data uploaded to the cloud.

3.2.4. DATA CONFIDENTIALITY

A number of cloud computing contracts extensively limit the protection of data confidentiality.[67] The survey from 2011 also found that the provider often obtains a licence for user-created content.[68] In most cases, such a licence is necessary for the proper functioning of the cloud. This results from the fact that efficient management of the cloud involves dynamic

[62] Bradshaw, S., Millard, Ch. and Walden, I. (2011) Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. *International Journal of Law and Information Technology*, 19 (3), pp. 204–205.

[63] Hon, W. K., Millard, Ch. and Walden, I. (2012) Negotiating Cloud Contracts: Looking at Clouds from both Sides Now. *Stanford Technology Law Review*, 16 (1), p. 118.

[64] McGillivray, K. (2014) Conflicts in the Cloud: Contracts and Compliance with Data Protection Law in the EU. *Tulane Journal of Technology and Intellectual Property*, 17, pp. 235–236.

[65] Hon, W. K., Millard, Ch. and Walden, I. (2012) Negotiating Cloud Contracts: Looking at Clouds from both Sides Now. *Stanford Technology Law Review*, 16 (1), p. 119.

[66] Weatherill, S. (2013) *EU Consumer Law and Policy.* 2nd ed. Cheltenham-Northampton: Edward Elgar, p. 93.

[67] Bradshaw, S., Millard, Ch. and Walden, I. (2011) Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. *International Journal of Law and Information Technology*, 19 (3), pp. 205–206.

[68] Op. cit., pp. 208–209.

movement of the files between servers, which requires them to be copied to the destination and deleted at the source location. However, the scope of such licences can be broadly formulated and in some cases it includes, for example, the use of the content to advertise the provider.[69] This remark corresponds to the previous observation, according to which cloud service providers can also generate income from non-monetary remuneration. Some authors claim that the consumer should try to stipulate that the data in the cloud is his property and he forbids sharing it with provider's subsidiaries or third parties.[70] Although I agree with the clear definition of the person holding the rights to digital content, I am also sceptic about the possibility of actually imposing such a provision on the provider. The consumer often does not have sufficient bargaining power to discuss contractual terms. Nevertheless, he should be aware of these risks, at least to consciously choose the provider.

3.2.5. DATA LOCATION

Uncertainty of data location additionally reinforces the above doubts about cloud computing contracts. Not all providers inform consumers about the place where the data is stored or the information they give is not complete.[71] General Data Protection Regulation addresses some of these difficulties.[72] In particular, the Regulation, like its predecessor the Directive 95/46/EC, limits the transfer of protected data to third countries.[73] Some cloud service providers organisations even regard this as a contractual opportunity.[74] To attract users from Europe, they recommend disclosing the information if the data is located in the *European Economic Area*. Consequently, not only consumers, but also cloud service providers may

[69] Similarly also McGillivray, K. (2014) Conflicts in the Cloud: Contracts and Compliance with Data Protection Law in the EU. *Tulane Journal of Technology and Intellectual Property*, 17, p. 234.

[70] Foster, T. N. (2013) Navigating Through the Fog of Cloud Computing Contracts. *John Marshall Journal of Information Technology and Privacy Law*, 30, p. 25.

[71] McGillivray, K. (2014) Conflicts in the Cloud: Contracts and Compliance with Data Protection Law in the EU. *Tulane Journal of Technology and Intellectual Property*, 17, pp. 232–233.

[72] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union* (2016/L-119/1). Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj [Accessed 14 March 2019].

[73] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities* (1995/L-281/31). Available from: http://data.europa.eu/eli/dir/1995/46/oj [Accessed 14 March 2019].

benefit from the information duty. However, it is necessary to stress that digital content is a broader concept than data protected under the Regulation. In my opinion, indicating the exact location of the data may be burdensome at least for some providers. Often files are transferred between several servers to optimise the use of the cloud. Therefore, a precise indication of the data location can be expensive for the providers, although, in practice, it depends on many factors (such as software used by the provider, cloud infrastructure or a number of users). Moreover, the information may also be of limited importance to the consumer due to the potential for its quick depreciation. Nevertheless, the consumer should be at least aware that his files may be stored in a foreign country, particularly if the country offers a lower level of protection, for example in the field of copyright. An optimal solution would be to oblige the provider to inform about the data location at the consumer's request. However, once again, consumers do not often have sufficient bargaining power to impose such provisions on the other party.

3.3. CODES OF CONDUCT AND ARBITRATION

According to Article 6 (1) (n) of the Directive, the trader should inform the consumer about the codes of conduct they use. The information may be valuable in the case of cloud computing contracts. In American literature, the development of "best practices" guidelines is seen as a potential way to effectively regulate these agreements,[75] particularly to facilitate data portability in the cloud.[76] In my opinion, the codes of conduct can be also helpful to define provider's policy on data preservation. This shows a connection to the information about the functionality and the relevant interoperability of digital content.

In addition, Article 6 (1) (t) of the CRD lists information about the possibility of recourse to an out-of-court complaint and redress

---

[74] Hon, W. K., Millard, Ch. and Walden, I. (2012) Negotiating Cloud Contracts: Looking at Clouds from both Sides Now. *Stanford Technology Law Review*, 16 (1), p. 100–101; McGillivray, K. (2014) Conflicts in the Cloud: Contracts and Compliance with Data Protection Law in the EU. *Tulane Journal of Technology and Intellectual Property*, 17, pp. 233–234.

[75] Celestine, C. M. (2013) "Cloudy" Skies, Bright Futures? In Defense of a Private Regulatory Scheme for Policing Cloud Computing. *Journal of Law, Technology and Policy*, 1, p. 159; Soma, J. et al. (2011) Chasing the Clouds without Getting Drenched. A Call for Fair Practices in Cloud Computing Services. *Journal of Technology Law and Policy*, 16, p. 212.

[76] Carpenter, R. H. Jr. (2010) Walking from Cloud to Cloud: The Portability Issue in Cloud Computing. *Washington Journal of Law, Technology & Arts*, 6 (1), pp. 12–13.

mechanism. The consumer may benefit from these procedures, particularly if they are less expensive of less formalised than court proceedings. However, they also pose a risk for them. At least at first sight, the consumer may be forced to enter the litigation initiated in a foreign forum. The survey from 2011 shows that cloud computing contracts often provide for such clauses.[77] Some agreements require arbitration for all disputes. Others specify cases where redress mechanism is mandatory. I agree that these provisions may be unfair within the meaning of Article 3 and Annex 1 (q) of the *Unfair Term* in Consumers Contracts Directive.[78] Consequently, even if the provider did not disclose the information about the mechanism, the consumer can defend himself against the resulting negative consequences.

3.4. CONFIRMATION AND BREACH OF INFORMATION DUTY

Apart from describing the content of the duty, the CRD also provides for incentives to inform the consumer. Firstly, in accordance with Article 8 (7) of the Directive, the trader should confirm the conclusion of the contract and all the information listed in Article 6 (1) thereof. The confirmation plays an important role in the case of contracts for the supply of digital content on an intangible medium. As stated in Article 14 (4) (b) (iii) of the CRD, the consumer who withdraws from the contracts bears no costs for the supply of the content, if the trader did not provide confirmation in line with Article 8 (7) thereof. The confirmation may have an even greater role in the case of cloud computing contracts. The study from 2011 shows that some providers actively change the agreements in a relatively short period of time.[79] More importantly, the providers often modify them unilaterally with only limited or no consumer knowledge.[80] Therefore, the possibility of proving the original text of the contract can be crucial from the point

[77] Bradshaw, S., Millard, Ch. and Walden, I. (2011) Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. *International Journal of Law and Information Technology*, 19 (3), pp. 200, 222.

[78] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts. *Official Journal of the European Communities* (1993/L-95/29). Available from: http://data.europa.eu/eli/dir/1993/13/oj [Accessed 14 March 2019]. See Bradshaw, S., Millard, Ch. and Walden, I. (2011) Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. *International Journal of Law and Information Technology*, 19 (3), pp. 200, 222.

[79] Bradshaw, S., Millard, Ch. and Walden, I. (2011) Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. *International Journal of Law and Information Technology*, 19 (3), pp. 190–191, 202, 215–217.

[80] Hon, W. K., Millard, Ch. and Walden, I. (2012) Negotiating Cloud Contracts: Looking at Clouds from both Sides Now. *Stanford Technology Law Review*, 16 (1), pp. 124–125.

of view of potential litigation. Otherwise, the consumer may encounter difficulty in proving the original provisions of the contract, for example the amount of the fee, the period of termination of the contract, the conditions of use or service level agreement.

Secondly, Article 6 (6) of the CRD frees the consumer from the obligation to pay the price if the information he received did not comply with Article 6 (1) (e) thereof. This may prevent the cloud service provider from charging an extra fee hidden in the "pay as you go" remuneration method. Moreover, Article 10 of the Directive extends the grace period if the trader does not inform the consumer about the right of withdrawal. It should also be noted that these provisions are an important step in addressing the problem of effective enforcement of consumer protection.[81]

Finally, Article 6 (9) of the Directive puts the burden of proof on the trader. Consequently, the consumer does not have to prove the information requirements set in Chapter IV of the CRD were not met. This creates an additional incentive for the provider to fulfil his duty. However, I agree that the lack of duty to inform the consumer about the burden of proof is perplexing.[82]

4. SUMMARY

Consumer Rights Directive aims at providing a comprehensive and up-to--date legal framework for consumer protection. To achieve this goal, the Directive requires the trader to inform the consumer about the essential elements of the transaction. Furthermore, the CRD introduces a new type of contract, i.e. a contract for the supply of digital content. Documents issued by the *European Commission* indicate that the concepts underlying the Directive were supposed to address cloud computing contracts. From this point of view, the distinction of contracts for the supply of digital content does not significantly improve consumer protection. Firstly, not all cloud computing contracts provide for an obligation to supply data in digital form. Secondly, recital 19 of the CRD raises unnecessary doubts as to whether *SaaS* and *PaaS* contracts classify as distance contracts. Moreover, the Directive does not expressly respond to the main problems

[81] Markou, Ch. (2017) Directive 2011/83/EU on Consumer Rights. In: Arno R. Lodder and Andrew D. Murray (eds.). *EU Regulation on E-Commerce.* Cheltenham-Northampton: Edward Elgar, p. 182.

[82] Weatherill, S. (2012) The Consumer Rights Directive: How and Why a Quest for "Coherence" Has (Largely) Failed. *Common Market Law Review*, 4, p. 1294.

identified in the context of the above contracts such as the risk of locking a consumer in a contract due to the lack of data portability or the ambiguity as to where the data is located or the persons who can use it.

However, the information duty, including information about the functionality and the relevant interoperability of digital content, can, to some extent, alleviate these deficiencies. The main obstacle to achieving this aim lies in the vagueness of both terms. This characteristic can be the greatest weakness or the greatest strength of the Directive, depending on the interpretation of these requirements. In my opinion, the provisions of the CRD can empower the consumer if the notion of functionality and relevant interoperability extends to the data in the cloud, in particular its confidentiality, integrity, location, portability and preservation. Such knowledge could increase consumers' awareness about the risks and limitations of cloud computing and thus allow them to make a reasonable decision about entering the contract. From this point of view, the Directive does not offer radically new provisions on consumer protection, but rather evolutionarily adapts already existing rules to changed conditions. Time will tell if such continuation will prove to be a sufficient instrument of protection.

LIST OF REFERENCES

[1] Bradshaw, D. et al. (2014) *Uptake of Cloud in Europe Follow-up of IDC Study on Quantitative estimates of the demand for Cloud Computing in Europe and the likely barriers to take-up.* [online] Luxembourg: Publications Office of the European Union. Available from: https://publications.europa.eu/en/publication-detail/-/publication/cfe5a91c-85cf-4c64-99e9-1b5900c8529a/language-en/format-PDF/source-search [Accessed 14 March 2019].

[2] Bradshaw, S., Millard, Ch. and Walden, I. (2011) Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. *International Journal of Law and Information Technology*, 19 (3).

[3] Bezáková D. (2013) The Consumer Rights Directive and its Implications for Consumer Protection Regarding Intangible Digital Content. *Masaryk University Journal of Law and Technology*, 7 (2).

[4] Calloway, T. J. (2011) Cloud Computing, Clickwrap Agreements, and Limitation on Liability Clauses: A Perfect Storm? *Duke Law and Technology Review*, 11 (1).

[5] Carpenter, R. H. Jr. (2010) Walking from Cloud to Cloud: The Portability Issue in Cloud Computing. *Washington Journal of Law, Technology & Arts*, 6 (1).

[6] Celestine, C. M. (2013) "Cloudy" Skies, Bright Futures? In Defense of a Private Regulatory Scheme for Policing Cloud Computing. *Journal of Law, Technology and Policy,* 1.

[7] Commission Decision of 18 June 2013 on setting up the Commission expert group on cloud computing contracts. *Official Journal of the European Union* (2013/C-174/6) 20 June. Available from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:174:0006:0008:EN:PDF [Accessed 14 March 2019].

[8] Consolidated version of the Treaty on the Functioning of the European Union, 13 December 2007. *Official Journal of the European Communities* (2012/C-326/1). Available from: https://eur-lex.europa.eu/eli/treaty/tfeu_2012/oj [Accessed 20 July 2019].

[9] Council Directive 85/577/EEC of 20 December 1985 to protect the consumer in respect of contracts negotiated away from business premises. *Official Journal of the European Communities* (1985/L-371/31). Available from: https://eur-lex.europa.eu/eli/dir/1985/577/oj [Accessed 14 July 2019].

[10] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts. *Official Journal of the European Communities* (1993/L-95/29). Available from: http://data.europa.eu/eli/dir/1993/13/oj [Accessed 14 March 2019].

[11] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council. *Official Journal of the European Union* (2011/L-304/64) 22 November. Available from: http://data.europa.eu/eli/dir/2011/83/oj [Accessed 14 March 2019].

[12] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities* (1995/L-281/31). Available from: http://data.europa.eu/eli/dir/1995/46/oj [Accessed 14 March 2019].

[13] Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts. *Official Journal of the European Communities* (1997/L-144/19) 20 May. Available from: https://eur-lex.europa.eu/eli/dir/1997/7/oj [Accessed 14 July 2019].

[14] Directorate-General for Justice. (2014) *DG Justice Guidance Document concerning Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European*

Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council. [online] Available from: https://ec.europa.eu/info/sites/info/files/crd_guidance_en_0.pdf [Accessed 16 July 2019].

[15] European Commission. (2008) *Proposal for a Directive of the European Parliament and of the Council on consumer rights.* (COM(2008) 614 final). [online] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2008:0614:FIN [Accessed 20 July 2019].

[16] European Commission. (2011) *Proposal for a Regulation of the European Parliament and of the Council on a Common European Sales Law.* (COM(2011) 635 final). [online] Available from: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52011PC0635 [Accessed 14 March 2019].

[17] European Commission. (2012) *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions 'Unleashing the Potential of Cloud Computing in Europe'.* (COM(2012) 529 final). [online] Available from: http://ec.europa.eu/transparency/regdoc/rep/1/2012/EN/1-2012-529-EN-F1-1.Pdf [Accessed 14 March 2019].

[18] European Commission. (2015) *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'A Digital Single Market Strategy for Europe'* (COM(2015) 192 final). [online] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN [Accessed 14 March 2019].

[19] European Parliament. (2011) *Report on the proposal for a directive of the European Parliament and of the Council on consumer rights.* [online] Available from: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2011-0038+0+DOC+PDF+V0//EN [Accessed 20 July 2019].

[20] European Parliament. (2011) *Debates: Wednesday, 23 March 2011 – Brussels.* [online] Brussels: European Parliament. Available from: http://www.europarl.europa.eu/sides/getDoc.do?type=CRE&reference=20110323&secondRef=ITEM-020&language=EN&ring=A7-2011-0038 [Accessed 15 July 2019].

[21] European Parliament. (2011) *Debates: Thursday, 23 June 2011 – Brussels.* [online] Brussels: European Parliament. Available from: http://www.europarl.europa.eu/sides/getDoc.do?type=CRE&reference=20110623&secondRef=ITEM-014&language=EN&ring=A7-2011-0038#4-223-000 [Accessed 15 July 2019].

[22] Foster, T. N. (2013) Navigating Through the Fog of Cloud Computing Contracts. *John Marshall Journal of Information Technology and Privacy Law*, 30.

[23] Hon, W. K., Millard, Ch. and Walden, I. (2012) Negotiating Cloud Contracts: Looking at Clouds from both Sides Now. *Stanford Technology Law Review*, 16 (1).

[24] Lu, Th. Y. (2018) Understanding Streaming and Copyright: A Comparison of the United States and European Regimes. *Journal of Business and Technology Law*, 13 (2).

[25] Markou, Ch. (2017) Directive 2011/83/EU on Consumer Rights. In: Arno R. Lodder and Andrew D. Murray (eds.). *EU Regulation on E-Commerce.* Cheltenham-Northampton: Edward Elgar.

[26] McCorry, D. (2014) With Cloud Technology, Who Owns Your Data?. *The Federal Courts Law Review*, 8 (1).

[27] McGillivray, K. (2014) Conflicts in the Cloud: Contracts and Compliance with Data Protection Law in the EU. *Tulane Journal of Technology and Intellectual Property*, 17.

[28] Mell, P. and Grance, T. (2011) *The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology.* Gaithersburg: National Institute of Standards and Technology. [online] Available from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf [Accessed 14 March 2019].

[29] Oxford University Press. (2019) *Oxford Dictionaries.* [online] Oxford University Press. Available from: https://en.oxforddictionaries.com/definition/medium [Accessed 14 March 2019].

[30] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union* (2016/L-119/1). Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj [Accessed 14 March 2019].

[31] Soma, J. et al. (2011) Chasing the Clouds without Getting Drenched. A Call for Fair Practices in Cloud Computing Services. *Journal of Technology Law and Policy*, 16.

[32] Weatherill, S. (2012) The Consumer Rights Directive: How and Why a Quest for "Coherence" Has (Largely) Failed. *Common Market Law Review*, 4.

[33] Weatherill, S. (2013) *EU Consumer Law and Policy.* 2nd ed. Cheltenham-Northampton: Edward Elgar.

[34] Wikipedia. (2019) *Software.* [online] Available from: https://en.wikipedia.org/wiki/Software [Accessed 21 July 2019].

DOI 10.5817/MUJLT2019-2-2

CONSEQUENCES OF THE USE OF PERSONALIZATION ALGORITHMS IN SHAPING AN OFFER – A PRIVATE LAW PERSPECTIVE[*]

by

KATARZYNA POŁUDNIAK-GIERZ[**]

Personalization mechanisms in consumer e-commerce allow for the adjustment of the time, form and manner of contact, the way of concluding the contract and the availability and content of the offer. Subsequently concluded agreements can be seen as a new phase of development of the consumer transaction model – secondary individualization replaces standardization. The possibility of concluding contracts on a massive scale is retained, but with added granularity and flexibility that mimic the individualisation of transactions. Special provisions for personalized contracts are missing on the EU level and within the Polish legal system.

The starting point is an analysis of the reaction of the traditional private instruments of Polish law towards the personalization of offers – case law and doctrinal approach towards the concept of a standard contract and an individually negotiated one are examined. Next, the pre-contractual stage is investigated – the personalization process is explored from the perspective of unfair practices regulation, and the legal basis for the personalization process in the context of the GDPR is discussed. While Polish national law focuses on combating the undesired results of personalization, the EU initiatives aim at granting ex-ante protection. The mechanism in directive 2005/29/EC is being supplemented with an information protection mechanism (consent requirement). The limitations of this model are identified and some alternative solutions are proposed.

[*] The following paper is a part of the research conducted within the framework of the project no. 2016/21/N/HS5/00167 *Personalized agreements in the light of civil law* grant-financed by the National Science Centre of Poland.

[**] katarzyna.poludniak@uj.edu.pl, PhD Candidate at the Department of Civil Law, Jagiellonian University in Kraków, Poland.

KEY WORDS
Consumer Protection, GDPR, Personalization, Unfair Commercial Practices

1. INTRODUCTION

An initial assumption of the study is that contracts concluded using personalization mechanisms[1] are a new step in the development of consumer contracts. Private law emerged as an individualised system, giving its subjects broad autonomy in the contractual sphere.[2] Since the beginning of mass production in the 19th century, the model of the individual contract has become obsolete.[3] Individually negotiated contracts were replaced by unilaterally formulated standard contracts.[4] The other party, as a rule being the weaker one, could either consent or resign from concluding a contract.[5] In response, the legislature introduced protective standards aimed at diminishing the undesired effects of the growing asymmetries in private relations.[6]

---

[1] In the paper broad understanding of the term is adopted – it covers all the adjustments of the content that are perceived by the addressee as adopted individually for him, to match his personal needs. Personalization should not be confused with customization in case of which modification of standard content are introduced by the addressee himself.

[2] Mularski, K. and Radwański, Z. (2019) Zagadnienia ogólne czynności prawnych. In: Zbigniew Radwański (ed.). *System prawa prywatnego*, 2, Zbigniew Radwański, Andrzej Olejniczak (eds.). *Prawo cywilne – część ogólna.* 3rd ed. Warszawa: C.H. Beck, pp. 7–8, 13.

[3] Łętowska, E. (1974) Problematyka ogólnych warunków i wzorów umów w świetle poglądów doktryny obcej. *Studia Prawnicze*, 3, pp. 152–153; Bednarek, M. (2013) Wzorce umów. In: Zbigniew Radwański (ed.). *System Prawa Prywatnego*, 5, Ewa Łętowska (ed.). *Prawo zobowiązań – część ogólna.* 2nd ed. Warszawa: C.H. Beck, pp. 604–605; Pyrzyńska, A. (2019) In: *Kodeks cywilny. Tom II. Komentarz. Art. 353–626*, Maciej Gutowski (ed.). 2nd ed. Warszawa: C.H. Beck, Art. 384, point I.1.

[4] This notion used in Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts. Art. 384–385, 385 (4) of Polish Civil Code (Dz.U.2018.1025) refer to the same phenomenon under the notion of *"a contract concluded with the use of standard terms"*. Polish legislator differentiates also contracts with unilaterally imposed provisions (art. 385 (1)–385 (3) PCC). Hondius, E. (1995) The Reception of Directive on Unfair Terms in Consumer Contracts by Member States. *European Review of Private Law*, 3, p. 245; Pyziak-Szafnicka, M. (1994) Kilka uwag na temat ochrony przed narzucaniem nieuczciwych warunków umowy. *Przegląd Prawa Handlowego*, 9, p. 1; Łętowska, E. (2004) *Nieuczciwe klauzule w prawie umów konsumenckich*. Warszawa: C. H. Beck, p. 2.

[5] Łętowska, E. (1974) Op. cit., pp. 123–124; Bednarek, M. (2005) *Wzorce umów w prawie polskim*. Warszawa: Monografie Prawnicze, pp. 10–11; Mikłaszewicz, P. (2008) *Obowiązki informacyjne w umowach z udziałem konsumentów na tle prawa Unii Europejskiej*. Warszawa, Kraków: Wolters Kluwer Polska, pp. 211–216.

[6] Twigg-Flesner, C. (2010) In: Hans-W. Micklitz, Jules Stuyck and Evelyne Terryn (eds.). *Cases, materials and Text on Consumer Law*. Oxford, Portland, Oregon: Hart Publishing, pp. 321–322; Schulze, R. and Zoll, F. (2018) *European Contract Law.* München: C. H. Beck; Oxford: Hart; Baden-Baden: Nomos, pp. 153–155; Zoll, F. (2018) *Rękojmia. Odpowiedzialność sprzedawcy.* Warszawa: Wydawnictwo C. H. Beck, Legalis, Chapter II § 1 point II; Hellwege, P. (2018) Right of Withdrawal in Distance and Off-Premises Contracts. In: Nils Jansen, Reinhard Zimmermann (eds.). *Commentaries on European contract laws*. Oxford: Oxford University Press, pp. 509, 511–513.

Personalization technologies allow for the re-individualization of contracts. Contracts are designed by the entrepreneur to match the individual characteristics, preferences or situation of the consumer, which gives him the impression that his relationship with the entrepreneur is based on trust and knowledge – the personalized contract model emerges. The main research questions are if and is how does the legal system react towards the use of personalization algorithms in shaping offers?

To avoid presenting fragmentary, distorted analysis the paper is divided into three sections. In each one a regulatory framework with different methodology approach is discussed – can it be applied, what are the most problematic issues that emerge during its application and does it fulfil its aim in case of personalized agreements? The first regime (contract law provisions on standard contracts[7]) provides protection by intervening in the content of legal relationship – *ex post*, by modifying the final result of applying personalization techniques during pre-contractual stage. The second [norms[8] introduced to national private law as an implementation of *Unfair Commercial Practices Directive (UCPD)*[9]] grants protection by setting requirements around the process of personalization – it outlines rules on entrepreneurs' actions that lead to conclusion of personalized agreement. Within the last group of norms (GDPR[10]) information based protection model is adopted – based on the assumption that individuals (usually consumers) are able to make a rational decision on consenting to personalization if they have access to relevant information.[11] The possible effectiveness of these regimes is assessed – their weaknesses are identified and possible solution proposed.

---

7 Art. 384–3854 of PCC.

8 Act on Competition and Consumer Protection (Dz.U.2018.798 j.t.) and the Act on Counteracting Unfair Market Practices (Dz.U.2017.2070 j.t.).

9 Directive 2005/29/EC of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council. *Official Journal of the European Union* (2005/L 149/22).

10 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union* (L 119/1). Available from: http://data.europa.eu/eli/reg/2016/679/oj [Accessed 16 September 2019].

11 Busch, C. (2019) Implementing Personalized Law: Personalized Disclosures in Consumer Law and Data Privacy Law. *The University of Chicago Law Review*, 86 (2), p. 310.

2. PERSONALIZATION – BETWEEN A STANDARD AND AN INDIVIDUALLY NEGOTIATED CONTRACT

The starting point of the analysis are the traditional private law instruments inherent for the core of national contract law [*Polish Civil Code (PCC)*], shaped under the influence the EU legislator in the last decade of 20th century.[12] These norms allow for determination of the content of the contractual relationship (final result of personalization within consumer market). There are no provisions that explicitly regulate personalization. Such agreement has characteristics typical of an individually negotiated contract, a unilaterally imposed set of provisions and a standard contract. Each one of the aforementioned is governed by a different set of norms. Discrepancies appear in regard to *inter alia* rules of the incorporation of provisions, their interpretation and the legal reaction towards the lack of equivalency of those relations.[13] Therefore, qualification of a personalized contract as a standard contract, a set of imposed provisions or an individually negotiated contract may significantly affect the position of the consumer in the contractual relationship. As a result, it is crucial to determine under which regime personalized contracts fall. Consequently, despite the fact that PCC does not recognise personalized agreements as a new model of contracting within consumer e-commerce, the use of personalization mechanisms cannot be disregarded at the stage of applying the law.

As a legal definition for a contract concluded with the use of standard terms is missing from the PCC,[14] there have been numerous attempts to define these contracts in case law[15] and doctrine.[16] Definitions of standard terms are based on the quantitative premise (number of contracts

[12] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts. *Official Journal of the European Union* (L 95/29). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31993L0013 [Accessed 16 September 2019].

[13] Discrepancies appear in regard to: rules on whether behaviour of the parties can be seen as reaching consensus as to the inclusion of certain elements to the legal relationship, possibility of interpretation of the content of contract in accordance with legitimate expectations against the wording of the contract, requirements to successfully set the characteristics of the subject of contract as being below the standard quality, the binding power of provisions that shape rights and duties of one party in a manner contrary to good practices with gross violation of his interests.

[14] Rejdak, M. (2005) Definicja terminu „wzorzec umowy konsumenckiej". *Ruch Prawny, Ekonomiczny i Socjologiczny*, LXVII (3), p. 116.

[15] Judgement of Constitutional Tribunal (8.12.2003), K 3/02, OTK-A 2003/9/99; judgements of Polish Supreme Court: (5.09.1991) III CZP 75/91, OSNC 1992/5/ 67; (7.07.2005) V CK 855/04, PUG 2005/10, p. 33; (26.03.2010) I CSK 444/09 Legalis no 362191; (20.07.2017) I CSK 704/16, Legalis no 1668805; (1.03.2017), IV CSK 285/16, LEX no 2308321.

concluded) or the objective premise (normative provisions regarding the scope of business or professional activity of the entrepreneur). Yet, these distinction prove to be unsuitable when assessing whether a personalized contract may constitute a standard one. It is reasonable to use descriptive definitions based on the enumeration of the standard terms features.

Standard terms in Polish law are (2.1.) a set of provisions prepared unilaterally by one party (2.2.) used for mass contracting (2.3) which shapes the content of these contracts in a uniform way.

2.1. A SET OF PROVISIONS PREPARED UNILATERALLY BY ONE PARTY

The authorship of the contract template is considered irrelevant. A standard contract can be written by the entrepreneur *in persona*, by a third party or compiled automatically by an electronic system. Thus, the fact that the customer profiling or compilation of contractual provisions is automated, without the actual participation of an entrepreneur, or in a way chosen by him (electronic agents), is irrelevant when assessing the nature of contracts.

The unilateral nature of the standard contract is understood as the lack of influence of the other party on its content. However, personalization can be performed only if at least one of prerequisites of Art. 6 GDPR is fulfilled – typically, if the consumer agreed to profiling in advance.[17] The *modus operandi* of personalization mechanisms depends on the entrepreneur, but the amount and content of data processed is a derivative of consumer behaviour. Thus, the consumer, through specific behaviours, can prevent the use of personalization or influence the personalization data through appropriate actions.[18]

In the case of personalized contracts, there are no negotiations between the entrepreneur and the customer. The adjustment of the content takes place before making an offer. The use of personalization mechanisms leads

[16] Łętowska, E. (2002) *Prawo umów konsumenckich*. 2nd ed. Warszawa: Wydawnictwo C.H. Beck, p. 320; Rejdak, M. (2005) Op. cit., p. 127; Bednarek, M. (2013) Op. cit., p. 596; Radwański, Z. and Olejniczak, A. (2018) *Zobowiązania: część ogólna*. 13th ed. Warszawa: C. H. Beck, p. 144.

[17] The issue discussed in: *4. Initiation of the personalization process.*

[18] When the model of consumers' strategic behaviour is used, the risk of data manipulation skyrockets. See a case of calculating creditworthiness based on the fact that people who buy furniture pads to protect their floors are considered trustworthy debtors. Duhigg, C. (2009) What Does Your Credit-Card Company Know About You? *The New York Times Magazine*. [online] Available from: http://www.nytimes.com/2009/05/17/magazine/17credit-t.html [Accessed 12 December 2018].

to the formation of individual contractual clauses in advance, which excludes the possibility of the other party's influence on their content. There is no room for subsequent modifications in this model. Nevertheless, the content of the offer depends on the individual characteristics of the consumer – it is shaped to correspond with them. The consumer's characteristics and expectations (explicitly or implicitly expressed in the data that is used during personalization process) should, therefore, have a substantial impact on the content of the contract.

Lack of dialogue at the pre-contractual stage may be seen as the effect of using effective tools to adapt the offer to the client's needs. The purpose of personalization is, after all, to enhance the consumer's trust towards the entrepreneur.[19] The need to negotiate in order to adapt the offer to the consumer's requirements disappears, because it is shaped based on his profile.

The use of personalization mechanisms should lead to the same effect as individual negotiations. However, it should be emphasized that the use of profiling and personalization does not automatically mean individualization of each of the potential clients. These tools allow for shaping marketing practices, including offers, to give the consumer the impression of an individual relationship with the entrepreneur. In the case of segmentation-based personalization,[20] such an individual relationship does not arise – it is only imitated. In addition, the fact that provisions are individually designed does not automatically mean that they should be qualified as individually negotiated. Unilaterality means there is a lack of negotiation, not of individual approach.[21]

Therefore, the premise of unilaterality should be understood strictly as the lack of dialogue between the parties, and personalized contracts can be considered unilaterally shaped by the entrepreneur.

---

[19] Borocz, I. (2015) Clash of Interests – Is Behaviour-Based Price Discrimination in Line with the GDPR. *Studia Iuridica Auctoritate Universitatis Pecs Publicata*, 153 (37), p. 42. Use of personalization makes it possible to build trust based on individualisation. Komiak, Sh. and Benbasat, I. (2006) The Effects of Personalization and Familiarity on Trust and Adoption of Recommendation Agents. *MIS Quarterly*, 30 (4), pp. 941–960. However, it should be noted that personalization of certain elements such as price might lead to opposite effects. Furner, Ch. P., Serino, C. M. and Smatt, C. *Making it personal: How personalization affects trust over time.* [online] Available from: http://ieeexplore.ieee.org/document/1385576/ pp. 8–9 [Accessed 1 May 2019].

[20] Firstly customers are grouped together according to identifiable characteristics (e.g. age, geography, gender, favourite brand) and then the content is adjusted to match each group.

[21] Rzetecka-Gil, A. (2011) *Kodeks cywilny. Komentarz. Zobowiązania - część ogólna.* LEX no 8853, Art. 385^1, point 22.

2.2. USED FOR MASS CONTRACTING

Emphasis is placed on the function of standard terms – they serve the proposer to conclude contracts. However, it is not specified whether these provisions concern only the rights and obligations of the parties in the contract,[22] or also the norms governing the conduct of the entrepreneur within the scope of his professional activity (personalization, marketing methods, etc.). According to the latter, to fulfil the rules of the incorporation of requirements, the entrepreneur should disclose the personalizing mechanisms to lawfully use them when shaping the agreement. Yet, this interpretation should be rejected, as the application of personalization mechanisms should be seen as part of the process of contract formation, not the contract itself.

The standard contract can be understood as an agreement for an unlimited number of contracts[23] or which provisions should be applied in at least three legal relationships.[24] Some scholars argue that the fact that there has been only one contract concluded with the use of a set of terms or that these terms are used sporadically impedes classifying them as standard terms.[25]

However, this means that an important role in shaping the nature of a given statement is then left to luck. If the entrepreneur drafts a standard contract with the purpose of applying it repeatedly, but after concluding one agreement decides not to use it again, then this set of provisions will be considered an individually imposed set of provisions, not standard terms. Therefore, the premise ought to be understood as a set of norms prepared to be used when concluding an unlimited number of contracts with an unlimited number of contractors. It is therefore enough that the standard terms were designed to be used repeatedly – their factual application is irrelevant.[26]

---

[22] Rejdak, M. (2015) Op. cit., p. 127; Trzaskowski, R. (2018) In: Jacek Gudowski (ed.). *Kodeks cywilny. Komentarz. Tom III. Zobowiązania. Część ogólna.* Warszawa: Wolters Kluwer, LEX no 10698, Art. 384, point 20.

[23] Zachariasiewicz, M. A. (1995) Niektóre problemy prawne związane z korzystaniem z nienormatywnych wzorców umownych. *Rejent*, 9, p. 122.

[24] Zoll, F. (1997) Potrzeba i kierunek nowelizacji kodeksowego ujęcia problematyki wzorców umownych. *Biuletyn Rady Legislacyjnej*, 1, p. 90.

[25] Rejdak, M. (2005) Op. cit., p. 117.

[26] (2016) Court of Appeal in Warsaw, VI ACa 1285/15, 9 November. [online] Available from: http://orzeczenia.waw.sa.gov.pl/details/$N/154500000003003_VI_ACa_001285_2015_Uz_2016-11-09_002 [Accessed 11 December 2018].

Nevertheless, the fulfilment of this premise in the case of personalized contracts is dubious. There are two possible scenarios: first, segmentation--based personalization – which is the model frequently applied nowadays – and second, triggered real-time adjustment. In the case of the segmentation of profilees the same model of contract is applied to all members of a given group. The larger the group is, the more times a particular pattern will be used. In principle, the same pattern is used for mass contracting.

However, the above model constitutes a simplification and may become obsolete with the development of personalization techniques. If personalizing mechanisms are used to generate the contents of contracts,[27] it becomes possible to compile standard terms for each consumer individually on the basis of data contained in the entrepreneur's system.[28]

Personalization is based on the use of electronic tools that are specific reusable algorithms. Thus, the mass element appears in this case not in reference to a particular set of terms but to the mechanism of its creation. This applies to the consumer's data, the collection of clauses and the code used to compose pattern – thus, although the outcome differs, the mechanism of personalization is common and serves for the mass conclusion of contracts.

As a result, it is not the set of standard terms that is applied for mass contracting, but the mechanism of their creation.

2.3. SHAPING THE CONTENT OF CONTRACTS IN A UNIFORM WAY

Personalization can take different forms, manifesting in the manner of concluding the agreement (e.g. bidding, auction), elements related to the form of the offer, its content, time and means of communication or lack thereof. If personalization concerns elements not related to shaping the content of the relationship, which arise as a result of the conclusion of a personalized contract, it will not affect the classification of the contract. Similarly, if the personalization affects only elements individualising the parties or main obligations of the parties (e.g. determination

[27] On first-degree price discrimination: Acquisti, A., Taylor, C. and Wagman, L. (2016) The Economics of Privacy. *Journal of Economic Literature*, 52 (2), p. 466.

[28] Similar postulates have been already offered by *C. Busch* regarding information duties. Busch, C. (2016) The Future of Pre-contractual Information Duties: From Behavioural Insights to Big Data. In: Christian Twigg-Flesner (ed.). *Research Handbook on EU Consumer and Contract Law.* Cheltenham, UK, Northampton, MA, USA: Edward Elgar Publishing, pp. 221–241.

of the price), it will be assumed that personalization did not cover standard terms, as these can never include individualising elements. Defining an individual consumer or specifying the subject of the contract will always have the character of an individually negotiated provision.[29]

Uniform shaping of the contract template means that it will define the content of future contracts identically, in isolation from the specifics of a particular contractual relationship.[30] The aim of using personalizing mechanisms is, however, to introduce individualization. If profiling results in the creation of multi-person groups, a unified pattern can be used within a given group. As long as the personalization creates only the appearance of individualisation, it is reasonable to argue that personalized agreements have uniform content and that they standardize contractual relationships.

The problem arises if entrepreneurs start mixing and changing clauses depending on the occurrence of specific characteristics of the consumer. The number of possible combinations of provisions can vary – theoretically, every consumer might be treated differently. In this case, the thesis that personalized contracts lead to the uniform shaping of the content of contracts will be unjustifiable.

2.4. HYBRID CHARACTER OF THE PERSONALIZED AGREEMENT – CONCLUSIONS AND RECOMMENDATIONS

A certain duality of the personalized agreement is to be observed – they have characteristics of both individually negotiated contracts and standard contracts. The content of personalized agreements is shaped by the entrepreneur – the consumer has no real impact on the content of commitment because he cannot negotiate it. At the same time, however, the consumer's features and behaviour have a decisive impact on the content of the offer. The lack of traditional negotiations may be seen as an element indicating the adhesive character of the contract, but it can be argued that negotiations are becoming an anachronism – they are replaced by profiling tools, which are supposed to lead to the same effect as negotiations between the parties.

A personalized offer can be single-use, but it can also be prepared to be leveraged on numerous occasions, depending on the technology used

[29] Radwański, Z. (2003) *Zobowiązania: część ogólna*. 4th ed. Warszawa: C.H. Beck, p. 142.

[30] (2011) Court of Appeal in Katowice, V ACa 546/11, 29 November. [online] Available from: https://www.katowice.sa.gov.pl/container/orzeczenia/V_ACa_546-11.pdf [Accessed 11 December 2018].

by the entrepreneur. In the case of personalization through profiling, it is possible to observe unification within a given group due to the fact that personalization leads only to apparent individualization. The development of personalization mechanisms can result in further granularization of personalized contracts – each might be generated separately, for every single customer.

As a result, it is impossible to apply the norms of either of the regimes directly. Due to qualification doubts, as well as the lack of specific normative regulation of personalized agreements, it is necessary to search for the optimal solution, having in regard the aim of the legislator when regulating the relationship between the consumer and the business – that is, the need to diminish the undesired effect of contractual inequality between these parties.

Considering the need to protect the consumer, it would be advisable to allow the *per analogiam* application of norms regulating adhesive agreements, as this regime provides higher protection then rules on individually negotiated contracts or unilaterally imposed provisions. It sets strict rules on incorporation of standards terms (it shall be delivered to it prior to the conclusion of the contract and, if in an electronic form, it shall be made available to the other party prior to the conclusion of the contract in such a manner that the latter is able to store and retrieve the template in the regular course of actions[31]). It impedes positioning the quality of service or product below the average without drawing consumers attention to that particular provision.[32] Finally, it battles disproportionality within rights and obligations of the parties by implementing general, standardized protection.[33]

3. PERSONALIZATION PROCESS FROM THE PERSPECTIVE OF UNFAIR COMMERCIAL PRACTICES FRAMEWORK

The UCPD has been implemented into Polish law by the *Act on Competition and Consumer Protection* and the *Act on Counteracting Unfair Market Practices*

[31] Art. 384 § 1, 4 PCC.

[32] Zoll, F. (2012) Problem negatywnego uzgodnienia cech rzeczy sprzedanej – w oczekiwaniu na wspólne europejskie prawo sprzedaży. *Transformacje Prawa Prywatnego*, 2, pp. 167–174.

[33] Rules on exploitation (Art. 388 PCC), unfair terms and unexpected clauses regulation (Art. 3851-4 PCC), Luzak, J. (2017) You too will be judged: *erga omnes* effect of registered unfair contract terms in Poland. *Journal of European Consumer and Market Law*, 6 (3), pp. 120–124.

(ACUMP). The latter, in accordance with the implemented directive, provides a general definition of unfair market practice – a practice that is contrary to good morals, interpreted as opposing the requirements of professional diligence[34] and materially distorts or is likely to materially distort the market behaviour of the average consumer with regard to the product. Therefore, this regulation addresses the issue of the permissibility of the personalization method that leads to a certain result e.g. a personalized marketing technique or a personalized offer.

Though this definition seems broad and irrespective of technology applied, there are certain issues that make protecting consumers from the undue influence of entrepreneurs less effective in the personalized online environment.

It can be doubted whether an individual activity of an entrepreneur – e.g. addressing a consumer with an individually tailored offer – can be considered a market practice. This interpretation has been rejected. Market practice means, among other things, a statement or piece of information that could take form of a single action.[35] The UCPD does not contain any indication that the act or omission on the part of the professional must be recurrent or must concern more than one consumer.[36]

The weakness of the protection lies in the standardization of premises. The point of reference is an average consumer,[37] yet the personalization uses strategies that correspond with the individual addressee's characteristics. A person with a strong authority bias, heavily influenced by the fear of being excluded, who applied to a certain university, views an advertisement where a person dressed as a dentist presents study according to which 70 % of students from this university have already benefited from the newest teeth-whitening treatment. Personalization opens the possibility for adjusting a marketing technique to a set of particular incentives this person is likely to react to.[38] Such a combined message is highly persuasive in this specific case, and significantly less effective for

[34] Stefanicki, R. (2009) *Ustawa o przeciwdziałaniu nieuczciwym praktykom rynkowym. Komentarz*. Warszawa: LexisNexis Polska, LEX no 10064, Art. 4, point 1.

[35] *Polski Związek Firm Deweloperskich v. Prezes UOKiK* (2010) SOKiK (Court of Competition and Consumer Protection) 25 March, No XVII Ama 43/09, Dziennik Urzędowy UOKiK, 3, p. 104.

[36] *Nemzeti Fogyasztóvédelmi Hatóság v. UPC Magyarország Kft.* (2015) TSUE. No. C-388/13, § 42.

[37] As worded in Art. 2 point 8, Art. 4. 1., Art. 5. 1., Art. 6. 1., Art. 8. 1. ACUMP in accordance with motive 18, Art. 5.2.b., Art. 6.1 and 2, Art. 7.1 and 2, Art. 8 UCPD.

[38] Calo, R. (2014) Digital Market Manipulation. *The George Washington Law Review*, 82, pp. 996, 999, 1010.

other customers.[39] Therefore, the practice cannot be considered likely to materially distort the market behaviour of the average consumer. If the point of reference remains standardized, the protection mechanism will fail to cover such individualized practices.

Another issue is drawing a line between sophisticated, persuasive marketing techniques and unfair market practices. Personalization means processing data on a consumer, which allows for determining his weaknesses, complexes, fears and behavioural biases.[40] This allows entrepreneurs to put the consumer under pressure in a manner which strongly limits the consumer's ability to make an informed decision. In certain situations, mechanisms based on persuasion can exert an undue pressure on the person,[41] which opens the possibility of classifying such behaviour as an aggressive practice. Can personalization significantly impair the consumer's ability to make an autonomous decision – limiting his freedom of choice? Can entrepreneurial practices cause someone to make a contractual decision which they would not have made otherwise? Answering these questions depends primarily on the results of empirical research on consumer behaviour towards personalized content.[42] In practice, a deep *ad casu* analysis of the effectiveness of a particular personalization tool would be needed – requiring access to personalization mechanisms, data on users, the results of personalization, user feedback and information on factual customer responses and data how the fair personalization – matching the needs and situations, not abusing weaknesses – influences the consumer's tendency to make certain contractual decisions.

In addition, frequently, personalization means matching pressure to one's weaknesses. The consumer is not misled in regards to the characteristics of the product, nor coerced into concluding an agreement. The entrepreneur manipulates him by providing personalized content, without disclosing information on the personalization

[39] Wagner, G. and Eidenmüller H. (2019) Down by Algorithms? Siphoning Rents, Exploiting Biases, and Shaping Preferences: Regulating the Dark Side of Personalized Transactions. *The University of Chicago Law Review*, 86, p. 594.

[40] Ibid, pp. 593–594.

[41] Schulze, R. and Schulte-Nölke, H. (2003) Analysis of National Fairness Laws Aimed at Protecting Consumers in Relation to Commercial Practices (Report Commissioned by the European Commission, DG Sanco), p. 37. [online] Available from: https://lirias.kuleuven.be/bitstream/123456789/204413/1/unfair_practices_en.pdf [Accessed 12 December 2018].

[42] Ibid.

process itself. As a result, only the nudges that amount to undue influence and as such preclude free decision-making or contain misleading information may be considered unfair commercial practices according to the UCPD.[43] The more conscious the consumers are of the practice, the more substantial nudging could be allowed.

As a rule, the subject to control is a specific practice of the entrepreneur in isolation from his other actions not a set of coordinated practices a customer is faced with.[44] However, in the online environment, the behaviours of the entrepreneur can be combined, which increases their effectiveness.[45] Each practice assessed separately might not be influential enough to materially distort the consumer's behaviour, yet, if it is designed to correlate with others, the impact of the whole mechanism grows. An example can be the case of a person fighting obesity and a donut advertisement. Provided that the message about the new promotion of his favourite donuts reaches him at the time when he used to have snack break at work and mentions the nearby bakery, the temptation would be considerably stronger than if the advertisement was not personalized.

Hence, it would be recommended to adopt a broader approach when assessing the character of a practice in question – taking into account also other practices of the entrepreneur and assessing the influence of the practice bundle on a consumer. As well current point of reference being an average consumer, though sufficient in case of segmentation-based personalization, might not maintain its functionality in the era of personalization. However, changes in this regard might not be necessary as here the individual protection mechanisms of defects of consent come into play (especially institution of mistake, fraud and threat).

4. INITIATION OF THE PERSONALIZATION PROCESS

The third group of norms is aimed at regulating the acceptability of use of personalization mechanisms – constituting the legal requirements for

[43] Brownsword, R. (2018) The E-Commerce Directive, Consumer Transactions, and the Digital Single Market – Questions of Regulatory Fitness, Regulatory Disconnection and Rule Redirection. In: Stefan Grundmann (ed.). *European Contract Law in Digital Age.* Cambridge, Antwerp, Portland: Intersentia, p. 187.

[44] Nevertheless, when assessing whether the market practice is aggressive, all its features and circumstances of placing the product on the market should be considered, in particular time, place, type of a given practice or the intentional use by the entrepreneur of a compulsory location of the consumer or other circumstances which limit the consumer's ability to make an informed decision regarding the contract. See Art. 8.3 ACUMP.

[45] Brownsword, R. (2018) Op. cit., pp. 165–172; Calo, R. (2014) Op. cit., pp. 995–1017.

lawful personalization processes. It is commonly accepted that data protection laws apply to personalized pricing.[46] Though what justifies the application of the norms of the GDPR is the processing of personal data, up until now, the research focused on one aspect of personalization – price personalization. The same observations can be made in the case of personalization leading to other results. The use of personalization itself might make the entrepreneur subject to the GDPR, regardless of the effect of this process.

The first premise of the application of the GDPR is the processing of personal data. According to Art. 4 (2) of the GDPR, nearly all the activities which can be exercised over personal data fall within this scope. Therefore, any operation or set of operations which is performed on personal data during personalization or with the objective of personalization, including storing or analysing data, constitute the processing of personal data.

Personal data encompasses any information relating to an identified or identifiable natural person [Art. 4 (2) GDPR]. There are two main scenarios to consider – a registered consumer case and a non-registered consumer case. In the first, the profilee provides the data knowingly and voluntarily during the registration process. Subsequently, his activities are monitored and this data supplements the information within his profile. As a result, all the information that is gathered on such a profile is considered personal data. The qualification of data processed in the second situation is not that clear. A user that is not registered nor signed-in as a rule will not be identified in a traditional manner. Nevertheless, there are other ways of identifying him each time he accesses the web – e.g. a cookie-identifier. The actions he takes in the online environment can be tracked and saved on his unique profile. This method allows for singling out a particular person, therefore the gathered profile data is considered personal data despite the lack of information traditionally used for individualisation (e.g. name, login).[47] Doubts emerge in the case of information that is not *per se* connected to the user's identity and is used

[46] Steppe, R. (2017) Online price discrimination and personal data: A General Data Protection Regulation perspective. *Computer Law & Security Review*, 33, pp. 768–785; Zuiderveen Borgesius, F.J., Poort, J.P. (2017) Online Price Discrimination and EU Data Privacy Law. *Journal of Consumer Policy*, 40 (3), p. 356; Borocz, I. (2015) Op. cit., pp. 50–52.

[47] Zuiderveen Borgesius, F.J. and Poort, J.P. (2017) Op. cit., p. 357; Article 29. Working Party 2010 Opinion 2/2010 on Online behavioural advertising (WP 171) 22 June 2010; Judgement of 19 October 2016, Breyer, Case C-582/14, ECLI:EU:C:2016:779 regarding a dynamic IP address.

for segmentation purposes – e.g. the fact that the person uses an *Apple* device. At the moment in which this data is connected to the profile of a particular person, it becomes personal data, as it becomes related to an identified natural person.

Personal data should be processed in accordance with the requirements of the GDPR – that is, *inter alias*, fairly, lawfully and transparently.

In the case of personalization during the pre-contractual stage in the private sector, there might be three legal grounds for processing personal data: the data subject has given consent (Art. 6a GDPR), processing is necessary for the performance of a contract (Art. 6b GDPR) or there are legitimate interests of the controller involved (Art. 6f GDPR). The doctrine[48] rejects the two latter grounds. The premise that the data is necessary for the performance of a contract or because of legitimate interests of the entrepreneur is understood narrowly; neither the fact that the processing of this data may maximise the profits of the processor nor the circumstance that the company sees this data as useful while developing its marketing strategies falls within their scope.[49]

Can Art. 6b and 6f constitute grounds for personalization aiming at different results? In the case of personalization that brings about results predominantly beneficial for the business but not bound to the obligation of the entrepreneur (e.g. not sending offers to low-spenders or consumers who often exercise their right to withdraw), as a rule the processing of personalized data should not be seen by *Data Protection Authorities* as necessary, as there are other ways to maximize profits. In addition, the consumer's interests and rights (especially their right to privacy) override the company's interests in this scenario.[50]

Similarly, processing enables the professional to address individual characteristics of the consumer in a way that is beneficial for both (e.g. no cosmetics containing substance X are advertised to an individual who is allergic to this particular ingredient). However, the fact that such personalization also benefits the consumer is irrelevant[51] when assessing realization of the premises of Art. 6f. The interests of the consumer should

[48] Steppe, R. (2017) Prijsdiscriminatie in het digitale tijdperk: Beschouwingen over de nieuwe algemene verordening gegevensbescherming. In: Matthias E. Storme, Werner F. Helsen (eds.), *Innovatie en disruptie in het economisch recht.* Antwerpen: Intersentia, pp. 105–149; Zuiderveen Borgesius, F.J. and Poort, J.P. (2017) Op. cit., p. 360. Argumentation formulated in regard to price discrimination.

[49] Kuner, C. (2007) *European data protection law. Corporate Compliance and Regulation*. 2nd ed. Oxford: Oxford University Press, pp. 234–235.

[50] Zuiderveen Borgesius, F.J. and Poort, J.P. (2017) Op. cit., p. 360.

be taken into account but not as a positive premise allowing for personalization but as a negative one – if there are interests or fundamental rights and freedoms of the data subject which require protection of personal data that override legitimate interests pursued by the controller or by a third party, Art. 6f GDPR cannot constitute grounds for such processing. Art. 6f should not be then interpreted as: if there are interests or fundamental rights and freedoms of the data subject whose protection requires processing of personal data, the controller or the third party is authorized to process this data despite the lack of other legal grounds for processing (e.g. Art. 6d).

The most controversial situation appears when the processing of personal data is beneficial for the entrepreneur but also constitutes an optimal manner of fulfilling legal obligation, e.g. enables the entrepreneur to assess the risk of the other party evading the obligation (e.g. the person is included in the national debtors' register). Here, a legitimate interest of the administrator lies in compliance with the requirement of due diligence when selecting a contractor. The processing of personal data might be considered necessary to achieve the objective resulting from the aforementioned interest – processing data on users is the core instrument that allows for diminishing anonymity within the online environment and reducing transaction risks. However, accepting this argumentation leads to the following conclusion: personalization should be allowed in e-commerce in every case, as it is the best solution for reducing anonymity and enhancing trust online. Consequently, the consumer is practically stripped of the protection granted by GDPR. Therefore, in this scenario, the entrepreneur's interests (to apply the most suited tools to fulfil his legal obligation) should be considered overridden by the interests or fundamental rights and freedoms of the data subject (mainly right to privacy).

Consequently, the only ground for processing personal data for the personalization in the private sector should be the informed consent of the data subject. The data subject should be given clear and comprehensive information about purposes of processing before consenting to be its subject – e.g. before cookies are saved on his device. Furthermore, the purpose cannot be only vaguely or generally described (e.g. "improving

[51] Lubasz, D. and Chomiczewski, W. (2018) In: Dominik Lubasz (ed.). *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*. Warszawa: Wolters Kluwer, LEX no 10655, Art. 6 point 7.3.

user's experience" or "enhancing personalized experience of user"), but must be stated clearly and accurately[52] so that the data subject can understand the intended results of the personalization (e.g. "personalized pricing" or "inaccessibility of offers not corresponding with profile").

The personalization of offers might fall under the scope of Art. 22 of the GDPR, as it can elicit fully automated decisions with far-reaching effects.[53] This provision attributes a person the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or otherwise significantly affects him. Personalized pricing fulfils these premises – (i) an algorithm decides on a price for a particular customer, (ii) in a fully automated manner, (iii) using personal data to evaluate the consumer's willingness to pay. (iv) It affects his legal situation because the determination of a price gives the final shape to his contractual obligation.[54]

The observations made regarding price personalization remain valid for other types of personalization. (i) Personalization mechanisms are designed to result in a decision regarding an individual person, yet their content may differ substantially depending on the functionality of the system (segmentation effect only, choice of manner and time of contact, content or form of offer). (ii) The algorithms used for personalization automate certain processes; in the case of *Big Data* analysis of consumer data, human intervention is *per se* unnecessary, except for the instances in which the code is being revised or changed. (iii) The personalization mechanisms work on personal data. (iv) The use of personalization mechanisms, no matter the aim of their particular usage, has a legal effect on the person – it alters his legal situation.

Firstly, the intent of personalization towards the consumer triggers the GDPR general protection. Secondly, it complicates the verification of compliance of the process with the requirements of the UCPD, while enabling the entrepreneur to influence the behaviour of a consumer to an unprecedented degree. Thirdly, it alters the scope of the legitimate expectations of the consumer, as building trust towards an entrepreneur becomes the main goal of personalization. Finally, it may also alter

[52] Art. 5.1(b) GDPR.

[53] Zuiderveen Borgesius, F.J. and Poort, J.P. (2017) Op. cit., p. 361.

[54] Subsumption model presented by: Mendoza, I. and Bygrave, L. A. (2017). *The Right Not to Be Subject to Automated Decisions Based on Profiling*. [online] Available from: https://ssrn.com/abstract=2964855 [Accessed 12 December 2018].

the mechanism of decoding the content of a contract as the information processed within the entrepreneur's systems on the subjective aim of the consumer should be taken into account when assessing the performance of the obligation by the professional.

As a result in each case of personalization, the data subject should be given meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject (Art. 13.2f and 14.2f GDPR). However, the fulfilment of this requirement may be problematic. It can be argued that the specifics of personalization mechanisms constitute company secrets, and even if the company was willing to reveal this information, it might be difficult to explain the reasoning of self-learning tools.

4.1. WEAKNESSES OF THE CONSENT BASED PROTECTION IN GDPR

Despite the novelty of the solution proposed within the GDPR, there are certain factors that undermine the functionality of this protective model.

Consent-based protection against use of personalization mechanisms towards a person[55] constitutes a variation of the protection by information model.[56] It is believed that with access to the data, the data subject (being the consumer in most cases) is able to make an informed, rational decision even when dealing with a significantly stronger entity. Providing the consumer with easy access to information should be enough to balance information asymmetries and thus prevent this person from being abused or tricked into an unfavourable contract – it is assumed that this person, with all the information at hand, will not agree to exploitation.

However, this protection model has flaws that impair its functionality, especially in the online environment. From the economic analysis of law perspective, the major issues are the cognitive limitations of the addresses of information,[57] the costs of its processing and the significant disproportion between the costs of reading and understanding information and the benefits of gaining this knowledge.[58] A person aware of her cognitive

[55] In this model an informed consent constitutes lawful ground for data processing. Busch, C. (2019) Op. cit., pp. 310–311.

[56] Busch, C. (2016) Op. cit., pp. 222–224.

[57] Calo, R. (2014) Op. cit., pp. 1000–1001.

[58] Mikłaszewicz, P. (2008) Op. cit., pp. 62–63; Luzak, J. (2015) Online Disclosure Rules of the Consumer Rights Directive: Protecting Passive or Active Consumers?. *Journal of European Consumer and Market Law*, 4 (3), p. 82.

limitations is not willing to make an effort which will most likely fail to improve the situation or expand her knowledge. The average consumer has neither the expertise on the subject of the contract, nor the knowledge of the law to allow an accurate interpretation of all provisions in a standard contract. Internet tools enable the consumer to diminish the influence of these factors, as they automate the comparison of content and facilitate the search for important pieces of information. However, they do not compensate for the increasing amount of data that the consumer is exposed to as a consequence of every click online.[59]

The GDPR consent-based protection resulted in a multiplication of the information the consumer is presented with at the pre-contractual stage. From the legislators' perspective, an individual should be given detailed and specific information on the processing of his personal data before consenting to processing – that is, before he can familiarize himself with the content he is looking for. This means that most actions taken by the consumer online will trigger a consent request. Then more information appear – e.g. the pre-contractual information demanded by the consumer rights directive. This inevitably leads to information overload.[60]

This critical point of information overload comes surprisingly fast in the case of online transactions. Behavioural studies show that the above is due to the intensity of the exposure to data, the conviction of the personal irrelevancy of the information presented and that the information is already known (assumption of repeatability of the information within pop-ups of certain kind) and the abundance of distractions within this environment and outside of it (short attention span).[61]

Last but not least, some undesirable entrepreneur behaviour models are observed. The main problem is the "take-it-or-leave-it" approach. The consumer that does not agree to the processing of his personal data is automatically denied access to the website or has to pay for it. The Internet's implied characteristic is the coexistence of numerous sites offering the same content/services and competing for users. This predication loses its accuracy in the case of sales portals or sharing economy portals; these tend to merge

[59] Busch, C. (2019) Op. cit., pp. 330–331.

[60] Busch, C. (2019) Op. cit., p. 322.

[61] Południak-Gierz, K. (2017) From Information Asymmetry to Information Overload – Technological Society of Consumers. In: Patrícia Kaplánová (ed.). *Contemporary issues of societal development.* Novo mesto, pp. 31–47.

and concentrate the majority of online traffic within a certain market (e.g. *Airbnb*, *Uber*, *Amazon*, Polish *Allegro*). Therefore, the decision to avoid one portal causes a similar result to the overall resignation from access to a specific Internet market.

4.2. POSSIBLE ENHANCEMENTS OF GDPR'S CONSENT-BASED PROTECTION MODEL

Principles present in GDPR (core principles of legitimacy, proportionality and legality as well as limitation purpose) set an adequate benchmark for the data protection regulation. However, in case of personalization within consumer e-commerce, the fact that the legal ground of processing of data is the consent of the data subject might limit GDPR's practical impact. Nevertheless, the effectiveness of the current informed consent-based protection model of GDPR can be increased.

The first, albeit temporary, approach aims at limiting the amount of information the data subject is provided with before the commencement of personalization. It requires empirical research on the reasons consumers fear and reject personalization. According to recent studies, the most problematic issue concerns price discrimination,[62] yet the matter requires further investigation. The solution might be to expressly inform the consumer only about the typical most unwanted aspects of personalization and provide a way to access extra information.

Another option, though rather practical then legal, would be to let the current regulation operate but encourage the members of the Internet society to "name and shame"[63] – that is, to investigate which entities processing data are not in line with the requirements of the GDPR, exercise especially user-unfriendly profiling or implement personalization not in order to adjust the offer to the needs and characteristics of the consumers, but to exploit false convictions and trick them into less favourable contracts.[64]

---

[62] Zuiderveen Borgesius, F.J. and Poort, J.P. (2017) Op. cit.; Borocz, I. (2015) Op. cit., p. 37.

[63] This model is based on the assumption that Internet societies have significant self--regulatory potential. Poullet, Y. (2002) How To Regulate Internet: New Paradigms For Internet Governance Self-Regulation: Value And Limits. In: Claire Monville (ed.). *Variations sur le droit de la société de l'information*. Bruxelles: Bruylant, pp. 84–91. [online] Available from: http://www.crid.be/pdf/public/4656.pdf [Accessed 2 May 2019]; Schultz, T. (2008) Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interfaces. *The European Journal of International Law*, 19 (4), pp. 829–837.

[64] On misperceptions: Bar-Gill, O. (2019) Algorithmic Price Discrimination When Demand Is A Function Of Both Preferences And (Mis)Perceptions. *University of Chicago Law Review*, 86 (2), pp. 228–232; Calo, R. (2014) Op. cit., pp. 1003–1017.

It is also worth considering imposing default standards on entities using personalization.[65] Forbidding or limiting the use of *Big Data* for personalization (e.g. banning price discrimination) might be equally harmful to consumer interests[66] so this would require in-depth research on the functioning of personalization mechanisms. Another issue is that if norms are set in legislative procedure they might quickly become outdated, as the development speed of technological and marketing techniques makes it difficult to set technologically insensitive norms. Some solutions might be to link the standards to other values (entrepreneurs should not ask for consent to use data in a way that is against contractual fairness, but simply refrain from doing so), to attribute the responsibility for data processing to the visible entities and to implement privacy-enhancing technology (e.g. a browser's default settings should not allow for identifying its user). Nevertheless, general clauses based protection is not optimal in the case of B2C relations.

The newest proposition is based on the idea of the personalization of laws regarding personalization.[67] The matter was investigated in regard to personalized pricing. The use of personalized price caps was proposed, which could diminish the effect of misperception on consumers' willingness-to-pay.[68] Another option was to personalize information duties based on the use of personalization – the information should precisely name the gains and losses of personalization used by the trader. In the case of personalized pricing, that would be information on the true value of the product towards a particular consumer.[69] The main weakness of the solution is the lack of incentive for the entrepreneur to eliminate the misperception-based component of the willingness-to-pay.[70] Secondly, the personalization of law, though alluring, poses a serious threat of uncontrollable free discretion in deciding on the legal rights and obligations of market participants, diminishing legal certainty.[71]

---

[65] Busch, C. (2019) Op. cit., pp. 323–324.

[66] Bar-Gill, O. (2019) Op. cit., pp. 223, 242.

[67] Ibid.

[68] Bar-Gill, O. (2019) Op. cit., pp. 223, 243–244.

[69] Porat, A. and Strahilevitz, L. J. (2014) Personalizing Default Rules and Disclosure with Big Data. *Michigan Law Review*, 112, pp. 1417–1421; Bar-Gill, O. (2019) Op. cit., p. 244.

[70] Bar-Gill, O. (2019) Op.cit., p. 244.

[71] Południak-Gierz, K. (2017) Dangers and benefits of personalisation in Contract Law: big data approach. *Queen Mary Law Journal*, Special Conference Issue: Autumn, pp. 25–36.

5. MODERN EU PROTECTIVE MECHANISMS VERSUS TRADITIONAL NATIONAL INSTITUTIONS – EFFICIENCY EVALUATION

The use of personalization algorithms in shaping offers does not pass unnoticed by legal systems, even in instances when personalization itself in not expressly dealt with in legal provisions. The reaction towards personalization can be observed on different levels: when assessing lawfulness of data processing within entrepreneur's tools, setting the point of reference for a fair process of personalization so that it does not become an unfair market practice and at the stage of interpretation of personalized contract. Theoretically, presented legal framework covers the most obvious issues related to the use of personalization mechanism during shaping an offer. However, the efficiency of these sets of rules differ.

Polish contract law – mostly rules on standard contracts – combats the undesired results of personalization by influencing the content of a contract concluded with the use of personalization mechanisms. These mechanisms are not designed to protect entities from disloyal use of personalization mechanisms but they reduce the contractual imbalance caused by limited autonomy of the weaker party (usually the consumer). It happens regardless of methodology used to force, trick or convince to conclude the agreement of such wording. As a result, they maintain their functionality also in case of personalized agreements.

Provisions of ACUMP as well as GDPR aim at granting *ex-ante* protection. The mechanism used in ACUMP (prevention of infringement caused by the improper conduct of the entrepreneur) is being supplemented with an information protection mechanism (consent requirement). The tendency to stretch protection towards the pre-contractual stage in EU law demonstrates the preventive approach of the legislator. However these instruments have certain weaknesses that might reduce their effectiveness.

In case of protection granted by provisions on unfair market practices the main issue is standardization of the point of reference. It impedes taking into account subjective peculiarities of a particular case that limit autonomy of this consumer – and the power of personalization is bestowed precisely in addressing these elements. Also, it might not be a singular practice that limits the autonomy of a person but the frequency and correlation between the practices. These features are not adequately addressed by the current

regulation and therefore, the effectiveness of protection granted within ACUMP in case of personalization mechanism is limited.

In comparison, the newly introduced protective mechanism of GDPR, designed as an answer to big data technology, is founded upon old protective assumptions. As a result, this protection model is burdened with the flaws of the old protection-by-information regime. In conclusion, applicable *ex post* national protective regulations remain vital for the protection of consumers concluding personalized agreements, as the protection systems offered by the ACUMP and GDPR seem leaky and not adequate in the era of personalized consumer contracts.

LIST OF REFERENCES

[1] Acquisti, A., Taylor, C. and Wagman, L. (2016) The Economics of Privacy. *Journal of Economic Literature*, 52 (2).

[2] Act on Competition and Consumer Protection (Dz.U.2018.798 j.t.).

[3] Act on Counteracting Unfair Market Practices (Dz.U.2017.2070 j.t.).

[4] Bar-Gill, O. (2019) Algorithmic Price Discrimination When Demand Is A Function Of Both Preferences And (Mis)Perceptions. *University of Chicago Law Review*, 86 (2).

[5] Bednarek, M. (2005) *Wzorce umów w prawie polskim.* Warszawa: Monografie Prawnicze.

[6] Bednarek, M. (2013) Wzorce umów. In: Zbigniew Radwański (ed.). *System Prawa Prywatnego*. Vol. 5, Ewa Łętowska (ed.). *Prawo zobowiązań – część ogólna.* 2nd ed. Legalis.

[7] Borocz, I. (2015) Clash of Interests – Is Behaviour-Based Price Discrimination in Line with the GDPR. *Studia Iuridica Auctoritate Universitatis Pecs Publicata*, 153 (37).

[8] Brownsword, R. (2018) The E-Commerce Directive, Consumer Transactions, and the Digital Single Market – Questions of Regulatory Fitness, Regulatory Disconnection and Rule Redirection. In: Stefan Grundmann (ed.). *European Contract Law in Digital Age*. Cambridge, Antwerp, Portland: Intersentia.

[9] Busch, C. (2016) The Future of Pre-contractual Information Duties: From Behavioural Insights to Big Data. In: Twigg-Flesner C. (ed.). *Research Handbook on EU Consumer and Contract Law*. Cheltenham, UK, Northampton, MA, USA: Edward Elgar Publishing.

[10] Busch, C. (2019) Implementing Personalized Law: Personalized Disclosures in Consumer Law and Data Privacy Law. *The University of Chicago Law Review*, 86 (2).

[11] Calo, R. (2014) Digital Market Manipulation. *The George Washington Law Review*, 82.

[12] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993, p. 29–34).

[13] Directive 2005/29/EC of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council. *Official Journal of the European Union* (2005/L 149/22).

[14] Duhigg, C. (2009) What Does Your Credit-Card Company Know About You? Submitted to: *The New York Times Magazine*. [online] Available from: http://www.nytimes.com/2009/05/17/magazine/17credit-t.html [Accessed 12 December 2018].

[15] Furner, Ch. P., Serino, C. M. and Smatt, C. Making it personal: How personalization affects trust over time. [online] Available from: http://ieeexplore.ieee.org/document/1385576/ [Accessed 1 May 2019].

[16] Hellwege, P. (2018) Right of Withdrawal in Distance and Off-Premises Contracts. In: Nils Jansen, Reinhard Zimmermann (eds.). *Commentaries on European contract laws*. Oxford: Oxford University Press.

[17] Hondius, E. (1995) The Reception of Directive on Unfair Terms in Consumer Contracts by Member States. *European Review of Private Law*, 3.

[18] Judgement of 19 October 2016, Breyer, Case C-582/14, ECLI:EU:C:2016:779.

[19] Judgement of Constitutional Tribunal (8.12.2003), K 3/02, OTK-A 2003/9/99.

[20] Judgement of Court of Appeal in Katowice (29.11.2011) V ACa 546/11. [online] Available from: https://www.katowice.sa.gov.pl/container/orzeczenia/V_ACa_546-11.pdf [Accessed 11 December 2018].

[21] Judgement of Court of Appeal in Warsaw (1.11.2016) VI ACa 1285/15. [online] Available from: http://orzeczenia.waw.sa.gov.pl/details/$N/154500000003003_VI_ACa_001285_2015_Uz_2016-11-09_002 [Accessed 11 December 2018].

[22] Judgement of Polish Supreme Court (20.07.2017) I CSK 704/16, Legalis no 1668805.

[23] Judgement of Polish Supreme Court (26.03.2010) I CSK 444/09 Legalis no 362191.

[24] Judgement of Polish Supreme Court (7.07.2005) V CK 855/04, PUG 2005/10.

[25] Judgement of Polish Supreme Court (1.03.2017) IV CSK 285/16, LEX no 2308321.

[26] Judgement of Polish Supreme Court (5.09.1991) III CZP 75/91, OSNC 1992/5/67.

[27] Komiak, Sh. and Benbasat, I. (2006) The Effects of Personalization and Familiarity on Trust and Adoption of Recommendation Agents. *MIS Quarterly*, 30 (4).

[28] Kuner, C. (2007*) European data protection law. Corporate Compliance and Regulation.* 2nd ed. Oxford: Oxford University Press.

[29] Łętowska, E. (1974) Problematyka ogólnych warunków i wzorów umów w świetle poglądów doktryny obcej. *Studia Prawnicze*, 3.

[30] Łętowska, E. (2002) *Prawo umów konsumenckich*. 2nd ed. Warszawa: C.H. Beck.

[31] Łętowska, E. (2004) *Nieuczciwe klauzule w prawie umów konsumenckich*. Warszawa: C. H. Beck.

[32] Lubasz, D. and Chomiczewski, W. (2018) In: Dominik Lubasz (ed.). *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*. Warszawa: Wolters Kluwer, LEX no 10655.

[33] Luzak, J. (2015) Online Disclosure Rules of the Consumer Rights Directive: Protecting Passive or Active Consumers?. *Journal of European Consumer and Market Law*, 4 (3).

[34] Luzak, J. (2017) You too will be judged: erga omnes effect of registered unfair contract terms in Poland. *Journal of European Consumer and Market Law*, 6 (3).

[35] Mendoza, I. and Bygrave, L. A. (2017) *The Right Not to Be Subject to Automated Decisions Based on Profiling*. [online] Available from: https://ssrn.com/abstract=2964855 [Accessed 12 December 2018].

[36] Mikłaszewicz, P. (2008) *Obowiązki informacyjne w umowach z udziałem konsumentów na tle prawa Unii Europejskiej*. Warszawa, Kraków: Wolters Kluwer Polska.

[37] Mularski, K. and Radwański, Z. (2019) Zagadnienia ogólne czynności prawnych. In: Zbigniew Radwański (ed.). *System prawa prywatnego*, 2, Zbigniew Radwański, Andrzej Olejniczak (eds.). *Prawo cywilne – część ogólna.* 3rd ed. Warszawa: C.H. Beck.

[38] *Nemzeti Fogyasztóvédelmi Hatóság v. UPC Magyarország Kft.* (2015) TSUE. No. C-388/13.

[39] Polish Civil Code (Dz.U.2018.1025).

[40] *Polski Związek Firm Deweloperskich v. Prezes UOKiK.* (2010) SOKiK (Court of Competition and Consumer Protection) 25 March, No XVII Ama 43/09, Dziennik Urzędowy UOKiK, 3.

[41] Południak-Gierz, K. (2017) Dangers and benefits of personalisation in Contract Law: big data approach. *Queen Mary Law Journal*, Special Conference Issue: Autumn.

[42] Południak-Gierz, K. (2017) From Information Asymmetry to Information Overload – Technological Society of Consumers. In: Patrícia Kaplánová (ed.). *Contemporary issues of societal development.* Novo mesto.

[43] Porat, A. and Strahilevitz, L. J. (2014) Personalizing Default Rules and Disclosure with Big Data. *Michigan Law Review*, 112 (8).

[44] Poullet, Y. (2002) How To Regulate Internet: New Paradigms For Internet Governance Self-Regulation: Value And Limits. In: Claire Monville (ed.). *Variations sur le droit de la société de l'information*. Bruxelles: Bruylant.

[45] Pyrzyńska, A. (2019) In: Maciej Gutowski (ed.). *Kodeks cywilny. Tom II. Komentarz. Art. 353–626*. 2nd ed. Legalis.

[46] Pyziak-Szafnicka, M. (1994) Kilka uwag na temat ochrony przed narzucaniem nieuczciwych warunków umowy. *Przegląd Prawa Handlowego*, 9.

[47] Radwański, Z. (2003) *Zobowiązania: część ogólna.* 4th ed. Warszawa: C.H. Beck.

[48] Radwański, Z. and Olejniczak, A. (2018) *Zobowiązania: część ogólna*. 13th ed. Warszawa: C. H. Beck.

[49] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union* (L 119, 4.5.2016).

[50] Rejdak, M. (2005) Definicja terminu „wzorzec umowy konsumenckiej". *Ruch Prawniczy, Ekonomiczny i Socjologiczny*, LXVII (3).

[51] Rzetecka-Gil, A. (2011) *Kodeks cywilny. Komentarz. Zobowiązania – część ogólna*. LEX no 8853.

[52] Schultz, T. (2008) Carving up the Internet: Jurisdiction, Legal Orders, and the Private/ Public International Law Interfaces. *The European Journal of International Law*, 19 (4).

[53] Schulze, R. and Schulte-Nölke, H. (2003) Analysis of National Fairness Laws Aimed at Protecting Consumers in Relation to Commercial Practices (Report Commissioned by the European Commission, DG Sanco), 37. [online] Available from: https://lirias. kuleuven.be/bitstream/123456789/204413/1/unfair_practices_en.pdf [Accessed 12 December 2018].

[54] Schulze, R. and Zoll, F. (2018) *European Contract Law*. 2nd ed. München: C. H. Beck; Oxford: Hart; Baden-Baden: Nomos.

[55] Stefanicki, R. (2009) *Ustawa o przeciwdziałaniu nieuczciwym praktykom rynkowym. Komentarz*. Warszawa: LexisNexis Polska.

[56] Steppe, R. (2017) Online price discrimination and personal data: A General Data Protection Regulation perspective. *Computer Law & Security Review*, 33.

[57] Steppe, R. (2017) Prijsdiscriminatie in het digitale tijdperk: Beschouwingen over de nieuwe algemene verordening gegevensbescherming. In: Matthias E. Storme, Werner F. Helsen (eds.). *Innovatie en disruptie in het economisch recht.* Antwerpen: Intersentia.

[58] Trzaskowski, R. (2018) In: Jacek Gudowski (ed.). *Kodeks cywilny. Komentarz. Tom III. Zobowiązania. Część ogólna.* Warszawa: Wolters Kluwer, LEX no 10698.

[59] Twigg-Flesner C. (2010) In: Hans-W. Micklitz, Jules Stuyck and Evelyne Terryn (eds.). *Cases, materials and Text on Consumer Law*. Oxford, Portland, Oregon: Hart Publishing.

[60] Wagner, G. and Eidenmüller H. (2019) Down by Algorithms? Siphoning Rents, Exploiting Biases, and Shaping Preferences: Regulating the Dark Side of Personalized Transactions. *The University of Chicago Law Review*, 86 (2).

[61] Zachariasiewicz, M. A. (1995) Niektóre problemy prawne związane z korzystaniem z nienormatywnych wzorców umownych. *Rejent*, 9.

[62] Zoll, F. (1997) Potrzeba i kierunek nowelizacji kodeksowego ujęcia problematyki wzorców umownych. *Biuletyn Rady Legislacyjnej*, 1.

[63] Zoll, F. (2012) Problem negatywnego uzgodnienia cech rzeczy sprzedanej – w oczekiwaniu na wspólne europejskie prawo sprzedaży. *Transformacje Prawa Prywatnego*, 2.

[64] Zoll, F. (2018) *Rękojmia. Odpowiedzialność sprzedawcy*. Warszawa: Wydawnictwo C. H. Beck.

[65] Zuiderveen Borgesius, F.J. and Poort, J.P. (2017) Online Price Discrimination and EU Data Privacy Law. *Journal of Consumer Policy*, 40 (3).

DOI 10.5817/MUJLT2019-2-3

JURIDICAL STATUS OF SO-CALLED SMART CONTRACTS AGAINST THE BACKGROUND OF THE POLISH LEGAL FRAMEWORK*

by

BOGNA KACZOROWSKA**

Among substantial advancements challenging contemporary contract law special attention is given to autonomous, cryptographic solutions based on decentralised infrastructure provided by blockchain technology, intended to execute transactions automatically, designated as smart contracts. The need for comprehensive research on legal implications of practical implementation of this technological innovation is triggered particularly by the prognostications declaring it a valid alternative to hitherto contract law framework that is expected to be ultimately replaced by algorithmic mechanisms underpinning smart contracts.

A relevant assessment of the impact smart contracts are presumed to have on the contract law domain requires a thorough analysis of their juridical status. The specificity of the category of smart contracts raises doubts whether they comply with the definition criteria inherent to contract law terminology. Additionally, it is of material importance to determine the function smart contracts can perform in the sphere of contractual practice and to confront it with the role and axiology of contract law.

The article aims at analysing the peculiarities of smart contracts from the perspective of the Polish private law system with account being also taken of current development tendencies concerning the concept of contract.

---

* The article constitutes an extended version of the paper delivered at *16th International Conference Cyberspace* held in Brno, 30 November – 1 December 2018.

** bogna.Kaczorowska@uwr.edu.pl, Department of Civil Law and Private International Law, Institute of Civil Law, Faculty of Law, Administration and Economics, University of Wrocław, Poland.

KEY WORDS

Algorithmisation, Blockchain-based "Smart Contracts", Concept of Contract, Contract Law, Contractual Obligations, Polish Private Law

1. INTRODUCTION

The current phase of development in the sphere of digital technologies brings multifarious implications which private law framework needs to be confronted with.[1] Intricate questions being raised for consideration in the context of unprecedented progress mainly in digitisation and automation processes induce to verify whether the essential private law institutions remain appropriate and functional.[2] This refers in particular to the domain of contract law[3] deemed notably exposed to novel tendencies regarding innovative patterns of arranging and conducting economic exchange.[4] Among substantial advancements challenging contemporary contract law special attention is given to autonomous cryptographic solutions based on decentralised infrastructure provided by blockchain technology, intended to execute and enforce transactions automatically, designated as smart contracts.[5] The need for comprehensive research on legal ramifications resulting from practical implementation of this technological innovation is triggered particularly by the prognostications declaring it a valid alternative to hitherto contract law framework that is expected to be ultimately replaced by algorithmic mechanisms underpinning smart contracts.[6]

A relevant assessment of the impact smart contracts are presumed to have on contract law requires a thorough analysis of their juridical status. The specificity of the category of smart contracts raises doubts whether they

[1] Cf. Machnikowski, P. (2015b) Prawo zobowiązań w 2025 roku. Nowe technologie, nowe wyzwania. In: A. Olejniczak et al. (eds.). *Współczesne problemy prawa zobowiązań*. Warszawa: Lex a Wolters Kluwer Business, pp. 379 *et seq.*; Kurosz, K. (2017) Zawieranie umów przez sztuczną inteligencję (systemy autonomiczne) a wady oświadczeń woli – wprowadzenie do problemu. In: W. Robaczyński (ed.). *Czynić postęp w prawie. Księga jubileuszowa dedykowana Profesor Birucie Lewaszkiewicz-Petrykowskiej*. Łódź: Wydawnictwo Uniwersytetu Łódzkiego, pp. 73 *et seq.*; Sellwood, M. (2017) The Road to Autonomy. *San Diego Law Review*, 54 (4), pp. 830 *et seq.*; Grundmann, S. and Hacker, P. (2017) Digital Technology as a Challenge to European Contract Law: From the Existing to the Future Architecture. *European Review of Contract Law*, 13 (3), pp. 255–293.

[2] Cf. i.a.: Kocot, W.J. (2017) Kontrakty kreatywne – nowy rozdział w cyberewolucji prawa umów. In: P. Kostański, P. Podrecki and T. Targosz (eds.). *Experientia docet. Księga jubileuszowa ofiarowana Pani Profesor Elżbiecie Traple*. Warszawa: Wolters Kluwer, pp. 946 *et seq.*; Schulze, R. and Staudenmayer, D. (2016) Digital Revolution – Challenges for Contract Law. In: R. Schulze and D. Staudenmayer (eds.). *Digital Revolution: Challenges for Contract Law in Practice*. Baden-Baden: Nomos, pp. 19 *et seq.*; Geis, G.S. (2008) Automating Contract Law. *New York University Law Review*, 83 (2), pp. 450–500.

comply with the definition criteria inherent to contract law terminology. Additionally, it is of material importance to determine the function smart contracts can perform in the sphere of contractual practice and to confront it with the role and axiology of contract law considering also current development tendencies concerning the concept of contract.

Without pretending to explore the question conclusively, the analysis will cover selected issues regarding the properties of smart contracts in the light of Polish private law with a view toward delineating debatable aspects that shall affect qualification of this technological innovation in legal terms.

2. DEFINITIONAL ASSUMPTIONS AND TERMINOLOGICAL QUERY ABOUT SMART CONTRACTS

In respect of smart contracts' technological peculiarities to be juxtaposed with private law institutions, it is argued that a distinctive hindrance to comprehensive analysis thereof consists in terminological inappropriateness and misapplication of conceptual framework

[3] It should be noted that due to the structure of Polish private law conforming with pandectistic system in which a central position is attributed to a general category of juridical acts, contract law is not formally recognised as a separate area. Nevertheless, on account of unquestionable relevance of contracts in the practice of legal interactions, one is not precluded from analysing the complex body of private law norms regarding different aspects of contracts and contractual obligations (despite their dispersal amongst provisions included in the general part of civil law and the law of obligations) as an integral whole to be referred to as contract law. Cf. Machnikowski, P. (2010) *Prawne instrumenty ochrony zaufania przy zawieraniu umowy*. Wrocław: Wydawnictwo Uniwersytetu Wrocławskiego, pp. 12–13; Machnikowski, P., Balcarczyk, J. and Drela, M. (2017) *Contract Law in Poland*. Alphen aan den Rijn: Kluwer Law International, pp. 25, 29, 42; Łolik, M. (2014) *Współczesne prawo kontraktów – wybrane zagadnienia*. Warszawa: Wydawnictwo C.H. Beck, p. 1; Romanowski, M. (2013) Position of the Law of Obligations in Polish Law in the Context of a Reform of the European Law of Obligations. In: R. Schulze and F. Zoll (eds.). *The Law of Obligations in Europe: A New Wave of Codifications*. Munich: Sellier European Law Publishers, pp. 67–69; Brzozowski, A. (2013) Pojęcie umowy w prawie polskim, funkcje umów. Źródła prawa regulującego umowy. In: *System prawa prywatnego*. 5: E. Łętowska (ed.). *Prawo zobowiązań – część ogólna*. Warszawa: Wydawnictwo C.H. Beck, p. 421. On the evolution of Polish contract law, see also: Konopacka, M. (2017) Kamienie milowe w rozwoju historycznym polskiego prawa umów. *Gdańskie Studia Prawnicze*, 38 (2), pp. 309–320. It shall be emphasised that the current Polish contract law is largely based on no longer in force legal solutions adopted in the Decree of the President of the Republic of Poland of 27 October 1933 – Code of Obligations (rozporządzenie Prezydenta Rzeczypospolitej – Kodeks zobowiązań, Journal of Laws No. 82, item 598, as amended, hereinafter: the Code of Obligations), commonly perceived as "the first genuinely European civil law codification" and "the most prominent achievement of the interwar European private law doctrine" (see i.a.: Dajczak, W. (2014) Kodeks zobowiązań jako lekcja metody prawnoporównawczej. *Kwartalnik Prawa Prywatnego*, 4, pp. 829, 852–853; Giaro, T. (2013) Some Prejudices about the Legal Tradition of Eastern Europe. In: B. Sitek, J.J. Szczerbowski and A.W. Bauknecht (eds.). *Comparative Law in Eastern and Central Europe*. Newcastle upon Tyne: Cambridge Scholars Publishing, pp. 42–43).

[4] Cf. i.a.: Łolik, M. (2014) Op. cit., p. 3.

appertaining to contract law.[7] The category of smart contracts is defined[8] essentially[9] by reference to a type of computer programmes operating autonomously on distributed, decentralised database secured cryptographically, denominated as blockchain, enabling automatic and irrevocable performance and execution of transactions, once the predefined conditions are met.[10] Purportedly, blockchain technology underlying smart contracts provides a mechanism of recording any transaction performed on the network and distributing a copy of it among single nodes involved upon prior consensus in verification ("validation") procedure, without the need for recourse to trusted institutional intermediaries.[11] One should, however, take account of avowed diversity of smart contracts and

[5] Cf. Caria, R. de. (2018) The Legal Meaning of Smart Contracts. *European Review of Private Law*, 26 (6), pp. 731–751; Allen, J.G. (2018) Wrapped and Stacked: 'Smart Contracts' and the Interaction of Natural and Formal Language. *European Review of Contract Law*, 14 (4), pp. 307–343; Werbach, K. (2018) Trust, but Verify: Why the Blockchain Needs the Law. *Berkeley Technology Law Journal*, 33 (2), pp. 493, 504 *et seq.*; Millard, C. (2018) Blockchain and Law: Incompatible Codes? *Computer Law & Security Review*, 34 (4), pp. 843–846; Szostek, D. (2018) *Blockchain a prawo*. Warszawa: Wydawnictwo C.H. Beck, pp. 27 *et seq.*, 113 *et seq.*; Szczerbowski, J.J. (2018a) *Lex cryptographia. Znaczenie prawne umów i jednostek rozliczeniowych opartych na technologii blockchain*. Warszawa: Wydawnictwo Naukowe PWN, pp. 11 *et seq.*; Bacina, M. (2018) When Two Worlds Collide: Smart Contracts and the Australian Legal System. *Journal of Internet Law*, 21 (8), pp. 1, 16 *et seq.*; Reyes, C.L. (2018) Cryptolaw for Distributed Ledger Technologies: A Jurisprudential Framework. *Jurimetrics: The Journal of Law, Science & Technology*, 58 (3), pp. 283–302; Goldenfein, J. and Leiter, A. (2018) Legal Engineering on the Blockchain: 'Smart Contracts' as Legal Conduct. *Law and Critique*, 29 (2), pp. 141 *et seq.*; Idelberger, F. (2018) Connected Contracts Reloaded – Smart Contracts as Contractual Networks. In: S. Grundmann (ed.). *European Contract Law in the Digital Age*. Cambridge–Antwerp–Portland: Intersentia, pp. 205 *et seq.*; Hsiao, J.I.-H. (2017) Smart Contract on the Blockchain – Paradigm Shift for Contract Law?. *US-China Law Review*, 14 (10), pp. 685–694; Giancaspro, M. (2017) Is a 'Smart Contract' Really a Smart Idea?: Insights from a Legal Perspective. *Computer Law & Security Review*, 33 (6), pp. 825–835; Malby, S. (2017) Strengthening the Rule of Law through Technology. *Commonwealth Law Bulletin*, 43 (3–4), pp. 314, 316–317; Wheeler, S. (2017) Visions of Contract. *Journal of Law and Society*, 44 (S1), pp. S76, S90–S91; Raskin, M. (2017) The Law and Legality of Smart Contracts. *Georgetown Law Technology Review*, 1 (2), pp. 306 *et seq.* Institutional initiatives towards exploring prospects for widespread use of blockchain-based applications (including smart contracts) in the field of digitised transactions, comprising also analytical work on an adequate regulatory surroundings, have been undertaken in Poland within the framework of governmental strategy. On the activities devoted to blockchain technology under operational programme "Od papierowej do cyfrowej Polski" ("From Paper to Digital Poland", "Paperless&Cashless Poland") coordinated and supervised by the *Ministry of Digital Affairs* as a part of the governmental policy "Plan na rzecz odpowiedzialnego rozwoju" ("Action plan for responsible development of Poland") adopted upon the resolution No. 14/2016 of the Council of Ministers of 16 February 2016 cf. also i.a.: Hulicki, M. and Lustofin, P. (2017) Wykorzystanie koncepcji blockchain w realizacji zobowiązań umownych. *Człowiek w Cyberprzestrzeni*, 1, pp. 42–43; Szostek, D. (2018) Op. cit., pp. 1, 4–5. In order to critically identify the fields in which implementation of blockchain technology brings real benefits when compared with other technical solutions, in December 2018 the *Ministry of Digital Affairs* has established the *Working Group on Distributed Ledgers and Blockchain* whose activity falls within the scope of the *Distributed Ledgers Stream* created upon the decision of the *Chairman of the Council of Ministers Committee for Digital Affairs* of 10 October 2018. See: Ministerstwo Cyfryzacji. (2019) *Grupa robocza ds. rejestrów rozproszonych i blockchain*. [online] Available from: https://www.gov.pl/web/cyfryzacja/grupa-robocza-ds-rejestrow-rozproszonych-i-blockchain1 [Accessed 7 August 2019].

multiplicity of blockchains' structures as well as manifold configurations in which particular smart contracts can act upon respective blockchains.[12] Accordingly, due to conspicuous heterogeneity of smart contracts forms it is necessary to emphasise that actually only some of them can be ultimately examined in terms of congruence with legal constructs and, where appropriate, equated with contracts in juridical sense.[13] In this context, the very denomination granted to smart contracts requires a critical analysis. Above all, anticipating further study and without losing sight of the complexity of contract definition in different legal traditions,[14] it should be stated that in case of the designation under consideration the reference to the concept of contract appears to be rather a hyperbole.[15] It seems symptomatic that smart contracts tend to be characterised in terms

[6] Cf. Savelyev, A. (2017) Contract Law 2.0: 'Smart' Contracts as the Beginning of the End of Classic Contract Law. *Information & Communications Technology Law*, 26 (2), pp. 116–134. In this context, including polemical remarks, see also: Durovic, M. and Janssen, A. (2018) The Formation of Blockchain-Based Smart Contracts in the Light of Contract Law. *European Review of Private Law*, 26 (6), pp. 754 *et seq.*; Szczerbowski, J.J. (2018a) Op. cit., pp. 12 *et seq.*, 54–55; Cannarsa, M. (2018) Interpretation of Contracts and Smart Contracts: Smart Interpretation or Interpretation of Smart Contracts?. *European Review of Private Law*, 26 (6), pp. 775 *et seq.*; Sklaroff, J.M. (2017) Smart Contracts and the Cost of Inflexibility. *University of Pennsylvania Law Review*, 166 (1), pp. 265 *et seq.*

[7] Mik, E. (2017) Smart Contracts: Terminology, Technical Limitations and Real World Complexity. *Law, Innovation and Technology*, 9 (2), pp. 270, 272 *et seq.*; Mik, E. (2018) Electronic Platforms: Openness, Transparency & Privacy Issues. *European Review of Private Law*, 26 (6), pp. 855, 856, 867 *et seq.*; Szostek, D. (2018) Op. cit., p. 114 *et seq.*; Durovic, M. and Janssen, A. (2018) Op. cit., pp. 755 *et seq.*

[8] One shall consider both doctrinal attempts to conceptualise smart contracts and increasing number of enactments covering the concept of smart contracts. For an overview of recently adopted legal definitions of smart contracts, see i.a.: Pardolesi, R. and Davola, A. (2019) "Smart contract": lusinghe ed equivoci dell'innovazione purchesia. In: F. Capriglione (ed.). *Liber Amicorum Guido Alpa*. Milano: Cedam, pp. 297–316; Rohr, J. (2019) Smart Contracts in Traditional Contract Law, Or: The Law of the Vending Machine. *Cleveland State Law Review*, 67 (1), pp. 71 *et seq.*; Temte, M.N. (2019) Blockchain Challenges Traditional Contract Law: Just How Smart Are Smart Contracts?. *Wyoming Law Review*, 19 (1), pp. 88 *et seq.*; Caria, R. de. (2018) Op. cit., pp. 735–737 *et seq.*; DiMatteo, L.A. and Poncibò, C. (2018) Quandary of Smart Contracts and Remedies: The Role of Contract Law and Self-Help Remedies. *European Review of Private Law*, 26 (6), p. 806; Szostek, D. (2018) Op. cit., pp. 119–120; Szczerbowski, J.J. (2018a) Op. cit., p. 18; Ridder, C.A. de, Tunstall, M.K. and Prescott, N. (2017) Recognition of Smart Contracts in the United States. *Intellectual Property & Technology Law Journal*, 29 (11), pp. 17–19.

[9] It shall be pointed out that there is an apparent lack of unanimity in defining smart contracts. Nonetheless, one can find the definition referring to a type of smart contracts executed on blockchain authoritative to some extent, as they prove to have the highest economic impact (cf. Szczerbowski, J.J. (2018a) Op. cit., pp. 15, 31–36; Szostek, D. (2018) Op. cit., pp. 120 *et seq.*; Durovic, M. and Janssen, A. (2018) Op. cit., pp. 754, 757 *et seq.*; Mik, E. (2017) Op. cit., p. 274; Caria, R. de. (2018) Op. cit., pp. 733 *et seq.*; Governatori, G. et al. (2018) On Legal Contracts, Imperative and Declarative Smart Contracts, and Blockchain System. *Artificial Intelligence and Law*, 26 (4), pp. 378, 385 *et seq.*; Giancaspro, M. (2017) Op. cit., pp. 826, 827; Levy, K.E.C. (2017) Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and the Social Workings of Law. *Engaging Science, Technology, and Society*, 3, pp. 2–3). See also: Geiregat, S. (2018) Cryptocurrencies Are (Smart) Contracts. *Computer Law & Security Review*, 34 (5), p. 1148; Werbach, K. (2018) Op. cit., pp. 505, 523; Allen, J.G. (2018) Op. cit., p. 309.

of imitation of conventional ones.[16] Moreover, regardless of the quality of a specific neosemantism attributed to the examined concept, substantial controversies surround the intimation that allegedly the category of smart contracts demonstrates capability resembling human intelligence or exceptional operability and trustworthiness.[17] This argument is reflected in an ongoing discussion associated with the search for an exact Polish language equivalent for the term in question.[18]

3. CONCEPTUALISATION OF CONTRACT UNDER POLISH LAW: AN OUTLINE

For the purpose of the analysis a synthetic insight into the concept of contract under Polish law is needed with the aim of providing a relevant point of reference. It should be indicated that there is no legal definition of contract in contemporary Polish private law system.[19] According to the widely accepted doctrinal position, a contract shall be defined

[10] Cf. Carron, B. and Botteron, V. (2019) How Smart Can a Contract Be?. In: D. Kraus, T. Obrist and O. Hari (eds.). *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law*. Cheltenham–Northampton: Edward Elgar Publishing, pp. 105 *et seq.*; Polański, P. (2019) Inwigilacja, dostępność, blockchain i sztuczna inteligencja: pytania o kierunki rozwoju prawa nowych technologii w erze rewolucji internetowej. *Monitor Prawniczy*, 2, p. 112; Woebbeking, M.K. (2019) The Impact of Smart Contracts on Traditional Concepts of Contract Law. *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 10 (1), pp. 107–108; Szczerbowski, J.J. (2018a) Op. cit., pp. 14 *et seq.*, 36 *et seq.*; Szczerbowski, J.J. (2018b) Transaction Costs of Blockchain Smart Contracts. *Law and Forensic Science*, 16 (2), pp. 1–2; Cannarsa, M. (2018) Op. cit., pp. 774–775, 776; Werbach, K. (2018) Op. cit., pp. 489 *et seq.*, 504 *et seq.*; Druck, J.A. (2018) "Smart Contracts" Are Neither Smart Nor Contracts: Discuss. *Banking & Financial Services Policy Report*, 37 (10), pp. 5 *et seq.*; Bacina, M. (2018) Op. cit., pp. 1, 16 *et seq.*; Giancaspro, M. (2017) Op. cit., p. 826; Kocot, W.J. (2017) Op. cit., pp. 950 *et seq.*; Hulicki, M. and Lustofin, P. (2017) Op. cit., pp. 38, 43 *et seq.*; Klinger, B. and Szczepański, J. (2017) Blockchain – historia, cechy i główne obszary zastosowań. *Człowiek w Cyberprzestrzeni*, 1, pp. 14, 16–17; Scholz, L.H. (2017) Algorythmic Contracts. *Stanford Technology Law Review*, 20 (2), pp. 146 *et seq.*; Gambino, A. (2017) Dignità umana e mercato digitale. *Diritto Mercato Tecnologia*, pp. 12–13; Cieplak, J. and Leefatt, S. (2017) Smart Contracts: A Smart Way to Automate Performance. *Georgetown Law Technology Review*, 1 (2), pp. 417 *et seq.*

[11] Cf. Scholz, L.H. (2017) Op. cit., pp. 146 *et seq.*; Szczerbowski, J.J. (2018a) Op. cit., pp. 36 *et seq.*; Mik, E. (2017) Op. cit., pp. 275 *et seq.* See also, including polemical remarks on blockchain as a "mechanism of trust": Werbach, K. (2018) Op. cit., pp. 490 *et seq.*

[12] See Mik, E. (2017) Op. cit., pp. 271 *et seq.*; Mik, E. (2018) Op. cit., pp. 856 *et seq.* Cf. also Hulicki, M. and Lustofin, P. (2017) Op. cit., pp. 39–40; Szczerbowski, J.J. (2018a) Op. cit., pp. 15, 36; Werbach, K. (2018) Op. cit., pp. 489, 498–499. On distinct categories of smart contracts serving either as tools in contracting process or as "artificial agents", see: Durovic, M. and Janssen, A. (2018) Op. cit., pp. 759–761, 770.

[13] Cf. Carron, B. and Botteron, V. (2019) Op. cit., p. 108 *et seq.*; Szczerbowski, J.J. (2018a) Op. cit., pp. 15–17, 35, 46 *et seq.*, 121–122; Szostek, D. (2018) Op. cit., pp. 121 *et seq.*; Kasprzyk, K. (2018) The Concept of Smart Contracts from the Legal Perspective. *Review of Comparative Law*, 34 (3), pp. 115–116; Governatori, G. et al. (2018) Op. cit., pp. 2 *et seq.*; Allen, J.G. (2018) Op. cit., pp. 311 *et seq.*; Cannarsa, M. (2018) Op. cit., pp. 775 *et seq.*; Werbach, K. and Cornell, N. (2017) Contracts Ex Machina. *Duke Law Journal*, 67 (2), pp. 338 *et seq.*, 368 *et seq.*

as a juridical act[20] involving (at least) two parties and requiring unanimous declarations of intent.[21] Worthy of note is that a definition of similar wording has been proposed within the framework of the recodification process in the previous draft of the book one of the new Polish civil code published in 2008 by the *Civil Law Codification Commission* at the *Ministry of Justice*,[22] eventually rejected upon its thorough revision in 2015.[23] Consistently, a historically conditioned approach based on consensus as a crucial element of contract remains of significant importance, along with the assumption according to which a contract shall be considered a socially relevant act.[24] As determined by current approach, a contract serves as an institution intended to enable autonomous private law entities to regulate legal relations by virtue of their own decisions, however, under

---

[14] Cf. Durovic, M. and Janssen, A. (2018) Op. cit., pp. 761 *et seq.* On the category of contract and its functions in a comparative view, including references to historical determinants, cf. i.a.: Elizalde, F. de. (2018) The Sources and Effects of Contractual Terms: Towards Approximation of Common Law and Civil Law. In: F. de Elizalde (ed.). *Uniform Rules for European Contract Law?: A Critical Assessment*. Oxford: Hart Publishing, pp. 163–188; Zweigert, K. and Kötz, H. (2011) *Introduction to Comparative Law*. transl. T. Weir. Oxford: Clarendon Press, pp. 324 *et seq.*; Graziadei, M. (2007) *Variations on the Concept of Contract in a European Perspective*. In: R. Schulze (ed.). *New Features in Contract Law*. Munich: Sellier European Law Publishers, pp. 311 *et seq.* For more on the methodological demand to address comparative argument in examining private law institutions, alongside historical and dogmatic analyses thereof, see: Longchamps de Bérier, F. (2016) Z uwag do metodologii nauki prawa prywatnego: argumenty historyczny, dogmatyczny i prawnoporównawczy na przykładzie darowizny na wypadek śmierci oraz zapisu windykacyjnego. In: A. Wudarski (ed.). *Polska komparatystyka prawa. Prawo obce w doktrynie prawa polskiego*. Warszawa: Stowarzyszenie Notariuszy Rzeczypospolitej Polskiej, pp. 285–329.

[15] On the criticism raised in this regard, cf.: Szczerbowski, J.J. (2018a) Op. cit., pp. 16–17; Durovic, M. and Janssen, A. (2018) Op. cit., pp. 755, 757 *et seq.* See also i.a.: Goldenfein, J. and Leiter, A. (2018) Op. Cit., pp. 141 *et seq.*; Cannarsa, M. (2018) Op. cit., pp. 775, 776 *et seq.*; Sklaroff, J.M. (2017) Op. cit., p. 276.

[16] Cf. Szczerbowski, J.J. (2018a) Op. cit., p. 17. On smart contracts as "analogue" of legal agreements, see also: Cannarsa, M. (2018) Op. cit., p. 777.

[17] Cf. Szczerbowski, J.J. (2018a) Op. cit., p. 16; Druck, J.A. (2018) Op. cit., pp. 5 *et seq.* See also: Durovic, M. and Janssen, A. (2018) Op. cit., p. 755; Levy, K.E.C. (2017) Op. cit., pp. 2 *et seq.*; Mik, E. (2017) Op. cit., p. 287; Kolber, A.J. (2018) Not-So-Smart Blockchain Contracts and Artificial Responsibility. *Stanford Technology Law Review*, 21 (2), pp. 198–234; Werbach, K. (2018) Op. cit., pp. 515–516, 518, 527; Werbach, K. and Cornell, N. (2017) Op. cit., p. 369.

[18] See: Szczerbowski, J.J. (2018a) Op. cit., pp. 14–17; Szostek, D. (2018) Op. cit., pp. 120 *et seq.*; Klinger, B. and Szczepański, J. (2017) Op. cit., p. 17; Kocot, W.J. (2017) Op. cit., pp. 950 *et seq.*

[19] Cf. Brzozowski, A. (2013) Op. cit., pp. 420–421; Strugała, R. (2013b) *Standardowe klauzule umowne: adaptacyjne, salwatoryjne, merger, interpretacyjne oraz pactum de forma*. Warszawa: Wydawnictwo C.H. Beck, p. 15. By contrast, prerequisites required to be met for establishing the existence of a contract were provided for in art. 50 of the Code of Obligations which read that a contract is formed by a unanimous declaration of intent made by two parties one of which commits to render a performance and the other accepts this commitment (§ 1) and that the subject matter of a contract may be also creation, modification or termination of a legal relation without commitment to render performance (§ 2). On this issue, see i.a.: Pecyna, M. (2013) *Merger clause jako zastrzeżenie wyłączności dokumentu, klauzula integralności umowy, reguła wykładni umowy*. Warszawa: Lex a Wolters Kluwer Business, p. 179.

authority and control of law.[25] A key role is attributed to the freedom of contract principle,[26] declaring that the parties entering into a contract may arrange the legal relation at their own discretion, on the condition that its content or purpose are not contrary to the nature of the relation, a normative act or principles of social coexistence.[27] Within the above limits contracting parties are regarded competent[28] to create specific rules binding between them (*lex contractus*), which influence the content of obligation.[29] Theoretical construct of contractual freedom is based, to a material extent,

---

[20] Juridical act is considered an essential instrument that serves to determine one's legal situation in the sphere of private law, within the framework of autonomy of will *sensu largo*. In the absence of legal definition, the concept of juridical act adopted in the doctrine refers to actions of entities in civil law, consisting at the very least in expressing a declaration of intent, aimed at producing legal effects which are recognised by material law as being intended by the parties. See: Radwański, Z. and Mularski, K. (2019b) Zagadnienia ogólne czynności prawnych. In: A. Olejniczak and Z. Radwański (eds.). *System prawa prywatnego*. 2: *Prawo cywilne – część ogólna*. Warszawa: Wydawnictwo C.H. Beck, pp. 13 *et seq.*; Grykiel, J. (2018). In: M. Gutowski (ed.). *Kodeks cywilny*. 1: *Komentarz. Art. 1–352*. Warszawa: Wydawnictwo C.H. Beck, pp. 507–509; Janas, A. (2018). In: M. Habdas and M. Fras (eds.). *Kodeks cywilny. Komentarz*. 1: *Część ogólna (art. 1–125)*. Warszawa: Wolters Kluwer, pp. 461 *et seq.* It is argued that the research on juridical acts draws on the achievements of theory of law regarding so-called conventional acts, although respective precepts contained in the Civil Code have been determined by the legal tradition and deeply ingrained conceptual framework as well as objectives pursued by the codification (cf. Sobolewski, P. (2017). In: K. Osajda (ed.). *Kodeks cywilny. Komentarz*. 1: *Część ogólna. Przepisy wprowadzające kc. Prawo o notariacie (art. 78–95 i 96–99)*. Warszawa: Wydawnictwo C.H. Beck, pp. 488–490, 547; see also: Machnikowski, P. (2017a). In: E. Gniewek and P. Machnikowski (eds.). *Kodeks cywilny. Komentarz*. Warszawa: Wydawnictwo C.H. Beck, pp. 124, 139). On the characterisation of conventional acts, see i.a.: Radwański, Z. and Mularski, K. (2019b) Op. cit., pp. 11 *et seq.*; Czepita, S. (2017) On the Concept of a Conventional Act and Its Types. *Ruch Prawniczy, Ekonomiczny i Socjologiczny*, 79 (1), pp. 85–102. For more on the theory of juridical acts elaborated by the pandectists, see i.a.: Giaro, T. (2018) Kształtowanie i ochrona praw prywatnych. In.: W. Dajczak, T. Giaro, F. Longchamps de Bérier. *Prawo rzymskie. U podstaw prawa prywatnego*. Warszawa: Wydawnictwo Naukowe PWN, pp. 128 *et seq.*

[21] Radwański, Z. and Olejniczak, A. (2018) *Zobowiązania – część ogólna*. Warszawa: Wydawnictwo C.H. Beck, pp. 122–124; Bierć, A. (2018) *Zarys prawa prywatnego. Część ogólna*. Warszawa: Wolters Kluwer, p. 710; Zagrobelny, K. (2018a) Umowy jako źródło zobowiązań. In: E. Gniewek and P. Machnikowski (eds.). *Zarys prawa cywilnego*. Warszawa: Wydawnictwo C.H. Beck, p. 247; Machnikowski, P., Balcarczyk, J. and Drela, M. (2017) Op. cit., pp. 29, 32, 68; Pecyna, M. (2013) Op. cit., p. 179. Under the Code of Obligations, the concept of contract denoted a unanimous expression of intent of two parties aimed at producing legal effects. For more on this issue, see: Longchamps de Bérier, R. (1938) *Zobowiązania*, Lwów: Księgarnia Wydaw. Gubrynowicz i Syn, p. 142; Samolewicz, S. (1937) *Zarys polskiego prawa zobowiązań*. Lwów: Skł. gł. Księgarnia T.S.L., p. 13.

[22] See: Komisja Kodyfikacyjna Prawa Cywilnego działająca przy Ministrze Sprawiedliwości (2009) *Księga pierwsza Kodeksu cywilnego. Projekt z uzasadnieniem*. Warszawa: Wydawnictwo C.H. Beck, pp. 59 *et seq.* For more on the issue of Polish private law recodification, see also: Kaczorowska, M. (2009) Rekodyfikacja prawa cywilnego w Polsce wobec rozwoju europejskiego prawa prywatnego. Rozważania na tle projektu księgi pierwszej Kodeksu cywilnego. *Ruch Prawniczy, Ekonomiczny i Socjologiczny*, 3, pp. 19–29; Machnikowski, P. (2014) Poland. In: J. Hurdík, P. Lavický et al. (eds.). *Private Law Reform*. Brno: Masaryk University, pp. 197–212; Gnela, B. and Michałowska, K. (academic supervision) (2014) *Directions of Private Law Development: Comments on the Draft of Book One of the Civil Code*. Warszawa: Difin.

upon regulatory (normative) character of a contract creating an obligation.[30] In this regard, contract constitutes a norm-setting act,[31] as reflected in the mechanism covering the effects it gives rise to.[32] The underlying rule is declared to be of cardinal importance for the whole framework of the civil law system.[33] Accordingly, a contract entails not only the effects expressed therein but also those that follow from a normative act, principles of social coexistence and established customs.[34] Thus, in terms of determining the content of obligation, encompassing the rights and duties of the parties, the content of contract ascertained adequately within the process of its

[23] See: Machnikowski, P. (2017b) In: P. Machnikowski (ed.). *Kodeks cywilny. Księga pierwsza. Część ogólna. Projekt Komisji Kodyfikacyjnej Prawa Cywilnego przyjęty w 2015 r. z komentarzem członków Zespołu Problemowego KKPC*. Warszawa: Wydawnictwo C.H. Beck, pp. XIII–XVI, 71 *et seq*.

[24] Radwański, Z. and Olejniczak, A. (2018) Op. cit., p. 123. Cf. also: Bierć, A. (2018) Op. cit., p. 710; Machnikowski, P., Balcarczyk, J. and Drela, M. (2017) Op. cit., p. 68; Zagrobelny, K. (2018a) Op. cit., p. 247; Brzozowski, A. (2013) Op. cit., p. 421.

[25] Cf. Radwański, Z. and Mularski, K. (2019b) Op. cit., pp. 9 *et seq.*; Radwański, Z. and Olejniczak, A. (2018) Op. cit., p. 123; Machnikowski, P. (2013b) Swoboda umów. In: *System prawa prywatnego*. 5, pp. 462–463; Machnikowski, P., Balcarczyk, J. and Drela, M. (2017) Op. cit., p. 87.

[26] The normative expression of contractual freedom principle is art. 353^1 of the Act of 23 April 1964 – Civil Code (ustawa – Kodeks cywilny, Journal of Laws of 2019 item 1145, as amended, hereinafter: the Civil Code).

[27] Machnikowski, P., Balcarczyk, J. and Drela, M. (2017) Op. cit., pp. 34, 87; Machnikowski, P. (2013b) Op. cit., pp. 462 *et seq.*; Machnikowski, P. (2013c) Treść umowy. In: *System prawa prywatnego*. 5, pp. 510 *et seq.* For more on the principle of freedom of contracts and its limits resulting from public policy, normative act and good morals, under art. 55 of the Code of Obligations, see i.a.: Longchamps de Bérier, R. (1938) Op. cit., pp. 147–150.

[28] For more on the category of competence considered adequate to define the freedom of contract, see: Radwański, Z. and Olejniczak, A. (2018) Op. cit., p. 132; Machnikowski, P. (2013b) Op. cit., pp. 463 *et seq.*, 478 *et seq.*; Zagrobelny, K. (2018a) Op. cit., pp. 269–270; Strugała, R. (2013b) Op. cit., p. 66; Pecyna, M. (2013) Op. cit., p. 179.

[29] Machnikowski, P. (2013b) Op. cit., pp. 478 *et seq.*; Machnikowski, P. (2013c) Op. cit., p. 504; Łolik, M. (2014) Op. cit., p. 29.

[30] Machnikowski, P. (2013b) Op. cit., pp. 478 *et seq.*

[31] Machnikowski, P. (2013b) Op. cit., pp. 478–481; Strugała, R. (2013b) Op. cit., pp. 21–22, 64.

[32] For more on this issue, see: Machnikowski, P. (2013b) Op. cit., pp. 478 *et seq.*; Machnikowski, P., Balcarczyk, J. and Drela, M. (2017) Op. cit., p. 87.

[33] Cf. Grykiel J. (2018) Op. cit., pp. 506 *et seq.*

[34] See: art. 56 of the Civil Code. For more on this issue, cf.: Machnikowski, P. (2013b) Op. cit., pp. 478 *et seq.*; Machnikowski, P., Balcarczyk, J. and Drela, M. (2017) Op. cit., pp. 87–88. On the parallel mechanism adopted under art. 60 of the Code of Obligations as to supplementing the content of contract in line with a normative act, usage and equity, see: Longchamps de Bérier, R. (1938) Op. cit., pp. 154–155.

interpretation[35] constitutes but one among a number of factors to be considered.[36]

On account of a contract being perceived in essence as the parties' self--commitment, the *pacta sunt servanda* principle applies. It requires that the contract be performed in accordance with its content.[37] Exemptions from this principle are allowed in certain cases on grounds of a statutory provision or the parties' common intent.[38] Worthy of particular note is the attempt to harmonise the *pacta sunt servanda* principle with the *rebus sic stantibus* clause regarding the influence of a change of circumstances on obligations.[39] One shall, however, draw attention to an argued need to reconsider the term *pactum* (agreement) represented in the above principle on account of currently identified symptoms of the so-called decodification process in the domain of private law.[40] An important factor

[35] Cf. Janas, A. (2018) Op. cit., p. 463; Machnikowski, P. (2017a) Op. cit., p. 152; Łolik, M. (2014) Op. cit., pp. 29, 47; Rott-Pietrzyk, E. (2013) *Interpretacja umów w prawie modelowym i wspólnym europejskim prawie sprzedaży (CESL)*. Warszawa: Wydawnictwo C.H. Beck, pp. 67–71. See also: Kaczorowska, B. (2018a) *Wykładnia umów obligacyjnych w świetle współczesnych tendencji rozwoju prawa prywatnego*. Wrocław: Wydawnictwo i Drukarnia Świętego Krzyża, *passim*.

[36] For more on this issue, see: Machnikowski, P. (2013b) Op. cit., pp. 478–481; Machnikowski, P. (2013c) Op. cit., pp. 504 *et seq.*; Grykiel, J. (2018) Op. cit., pp. 508, 514; Rott-Pietrzyk, E. (2013) Op. cit., p. 71.

[37] Cf. Brzozowski, A. (2013) Op. cit., p. 421; Machnikowski, P. (2013a) Struktura zobowiązania. In: *System prawa prywatnego*. 5, p. 163; Zagrobelny, K. (2018b) Wykonanie zobowiązania. In: E. Gniewek and P. Machnikowski (eds.). *Zarys prawa cywilnego…*, p. 367. On the application of the *pacta sunt servanda* principle under the Code of Obligations, see: Longchamps de Bérier, R. (1938) Op. cit., p. 317.

[38] Cf. Brzozowski, A. (2013) Op. cit., p. 421.

[39] Cf. i.a.: Zagrobelny, K. (2018b) Op. cit., p. 367; Brzozowski, A. (2018) Wpływ zmiany okoliczności na zobowiązania. In: *System prawa prywatnego*. 6: A. Olejniczak (ed.). *Prawo zobowiązań – część ogólna*, Warszawa: Wydawnictwo C.H. Beck, pp. 1307 *et seq.*; Brzozowski, A. (2014) *Wpływ zmiany okoliczności na zobowiązania. Klauzula rebus sic stantibus*. Warszawa: Wydawnictwo C.H. Beck, pp. 3 *et seq.*; Machnikowski, P., Balcarczyk, J. and Drela, M. (2017) Op. cit., pp. 126, 127; Gorczyński, G. (2015) Klauzula *rebus sic stantibus* w XXI wieku. In: A. Olejniczak et al. (eds.). *Współczesne problemy prawa zobowiązań…*, pp. 186 *et seq.* See also, in the context of commercial contracts: Włodyka, S. and Spyra, M. (2017) Ogólna charakterystyka umów handlowych. In: M. Stec (ed.). *System prawa handlowego*. 5: *Prawo umów handlowych*, Warszawa: Wydawnictwo C.H. Beck, pp. 22, 23. On recognition of the *rebus sic stantibus* clause under art. 269 of the Code of Obligations, see also: Longchamps de Bérier, R. (1938) Op. cit., pp. 404 *et seq.*; Giaro, T. (2013) Op. cit., pp. 43–44. For more on the issue regarding promise-keeping juxtaposed with the consequences of a significant change of circumstances in historical perspective and in contemporary private law systems, cf.: Dajczak, W. (2018) Zobowiązania. In: W. Dajczak, T. Giaro, F. Longchamps de Bérier. *Prawo rzymskie…*, pp. 523–524.

[40] Dajczak, W. (2017) Amerykańska zapowiedź „śmierci umowy" na tle tradycji romanistycznej. In: F. Longchamps de Bérier (ed.). *Dekodyfikacja prawa prywatnego. Szkice do portretu*. Warszawa: Wydawnictwo Sejmowe, pp. 89 *et seq.*, 100–101. Cf. Longchamps de Bérier, F. (2019) Decodification of Contract Law. In: C. Su, F. Longchamps de Bérier and P. Grzebyk (eds.). *Theory and Practice of Codification: The Chinese and Polish Perspectives*. Beijing: Social Sciences Academic Press, pp. 137–149. For more on the phenomenon of private law decodification, see also i.a.: Rudnicki, J. (2018) *Dekodyfikacja prawa cywilnego w Polsce*. Bielsko-Biała: Wydawnictwo Od.Nowa.

to be reckoned with under this approach shall be the crisis of the liberal theory of contract as an expression of the parties' autonomy of will, as well as the 19th century paradigm of civil law codification designed as a comprehensive system with a view to ensuring the certainty of law.[41] Consequently, mainly in case of a considerable asymmetry between the contracting parties' positions, particular significance is attached to legitimate, justifiable expectations of the creditor. Therefore, in the light of the assumed redefinition of the concept of *pactum* in the foregoing context, when determining the due performance the priority is envisaged to be given to "what could have been justifiably expected by the creditor at the contracting stage" instead of "what has been planned substantively".[42] Pursuant to this view, what shall be anticipated is a systemic change to law of contractual obligations expressed by surpassing in a far-reaching manner the content of the parties' declarations of intent as well as statutory provisions in order to retrieve the social and economic sense of contract.[43]

Against this particular background delineated above, taking into account the multidimensional ambience in which, essentially, any research devoted to the very nature of contract and contractual obligation shall be placed, a critical analysis outlining some aspects of the smart contracts' juridical import will be undertaken.

4. CRITICAL ANALYSIS OF SMART CONTRACTS' JURIDICAL RELEVANCE: AN OUTLINE

As argued in doctrine, the principal classification of blockchain-based smart contracts encompasses the following categories: cryptocurrencies which constitute chronologically the first implementation of blockchain technology aimed at creating an uncomplicated system of cryptographic units transfer, on the one hand, and so-called complete smart contracts

[41] Dajczak, W. (2017) Op. cit., pp. 90, 101.

[42] Dajczak, W. (2017) Op. cit., pp. 100–101. Cf. also: Longchamps de Bérier, F. (2019) Op. cit., p. 147.

[43] Dajczak, W. (2017) Op. cit., p. 101. Cf. also: Dajczak, W. (2012) *The Nature of the Contract in Reasoning of Civilian Jurists*. Poznań: Wydawnictwo Naukowe UAM, pp. 175–176. What constitutes a relevant research issue in this respect is the comparison between civil law system and common law framework on the basis of the criterion of adaptability to the aforementioned decodification consequences (Dajczak, W. (2017) Op. cit., pp. 101–102). Correspondingly, a theoretical approach and contract drafting techniques characteristic respectively for civil law and common law are subject to a comparative analysis in the light of the phenomenon of automation of legal relations, with the emphasis on coding contracts (see: Cannarsa, M. (2018) Op. cit., pp. 776, 781–782).

utilising multifunctional programming languages, on the other hand.[44] Due to the properties of programming languages complete smart contracts are deemed capable of expressing content of any relation and therefore necessitate being explored in more detail from the viewpoint of contract law.[45] In this regard the scrutiny of smart contracts' juridical relevance shall be preceded by drawing a distinction between dissimilar types of them. It is emphasised that one shall differentiate a smart contract itself embodying the binding expression of an agreement – as the only form of record (smart contract entirely written in code), from a smart contract implementing automatically a separate agreement expressed in natural language, and thus serving as evidence for the existence and the content of a conventional agreement (as a tool or carrier of a record reflecting a prior traditional contract frequently being a framework agreement or a conditional contract in nature)[46]. The former category, referred to as pure complete smart contracts,[47] both instantiated and executed in a direct manner on the blockchain, warrants in particular closer attention. However, mainly due to complications connected substantially with translation of natural language contract into smart contract code, material legal problems have to be addressed also in regard to the latter category.

In formal terms, there is no impediment to express a legally relevant arrangement in a computer code by means of blockchain technology. As a general rule, freedom of declaration of intent form is enshrined under the Civil Code.[48] Accordingly, subject to statutory exceptions the intention

---

[44] Cf. Szczerbowski, J.J. (2018a) Op. cit., pp. 13–14, 46 *et seq.*, 60 *et seq.* See also: Geiregat, S. (2018) Op. cit., pp. 1144–1149; Szostek, D. (2018) Op. cit., pp. 51 *et seq.*, 113 *et seq.*

[45] Cf. Szczerbowski, J.J. (2018a) Op. cit., pp. 49 *et seq.*

[46] Carron, B. and Botteron, V. (2019) Op. cit., pp. 111 *et seq.*; Governatori, G. et al. (2018) Op. cit., p. 378; Szostek, D. (2018) Op. cit., pp. 121–122, 123–124; Cannarsa, M. (2018) Op. cit., pp. 776–777; Durovic, M. and Janssen, A. (2018) Op. cit., pp. 756, 759 *et seq.* Another, threefold distinction embraces respectively: so-called pure complete smart contracts, both formed and executed directly on a blockchain; hybrid complete smart contracts, formed on the blockchain but executed outside it, including those requiring an external input managed by a third system; smart contracts constituting components of traditional contracts, including smart contracts templates intended to associate natural language pertaining to contractual transactions with smart contract code (for more, see: Szczerbowski, J.J. (2018a) Op. cit., pp. 50–53, 121–122). On smart contract templates cf.: Hulicki, M. and Lustofin, P. (2017) Op. cit., pp. 44. 46; Werbach, K. (2018) Op. cit., pp. 542–543. On the interrelation between programming code and natural language in the sphere of smart contracts, including direct coding and contract translation, cf.: Mik, E. (2017) Op. cit., pp. 287 *et seq.*; DiMatteo, L.A. and Poncibò, C. (2018) Op. cit., pp. 807 *et seq.* See also i.a.: Allen, J.G. (2018) Op. cit., pp. 312 *et seq.*, 319; Scholz, L.H. (2017) Op. cit., pp. 146–147; Cieplak, J. and Leefatt, S. (2017) Op. cit., pp. 417–418.

[47] Szczerbowski, J.J. (2018a) Op. cit., pp. 50–51, 121, 132.

[48] See: art. 60 of the Civil Code.

of a person performing a juridical act may be expressed by any behaviour which manifests that person's intention sufficiently, including the intention being manifested in electronic format, it is hence possible to select any form of sign or means of communication as well as configuration thereof.[49] In this regard, principally, smart contracts shall be granted legal relevance, as a specific expression of the parties' intent to cause legal effect consisting in creation, modification or termination of a civil law relation.[50] However, dual requirement must be taken into account when determining the completion of a declaration of intent as defined by Polish law. Any declaration of intent needs to be externalised so that it proves to be discernible, and manifested in a sufficient manner, that is in such a mode as to render it intelligible for the addressee. The latter refers not only to the type of signs used by the party performing a juridical act but also to the language, required to be at least decodable by the addressee, as well as to the way in which the respective wording is phrased.[51] What constitutes an essential condition on this point is that the content of a declaration be unambiguously identifiable by use of interpretation methods, otherwise, in failure to establish any reasonable meaning of a given conduct, there are no grounds to recognise it as the completion of a declaration of intent.[52]

In the above context, a particular question arises over the specificity of machine-readable format of the arrangement encoded in a smart contract. It is argued that the apprehension of the smart contract's content poses considerable difficulties, mainly due to the artificial programming languages intricacies,[53] with a risk of abuse by one party of the incomplete understanding by the other.[54] Conceivably, it concerns both pure complete smart contracts formed and enforced entirely in the code and those originated as contractual documents drafted in natural language to be

[49] For more on this issue, see: Grykiel, J. (2018) Op. cit., p. 593; Górska, K. (2018) Czynności prawne na tle innych zdarzeń cywilnoprawnych. In: E. Gniewek and P. Machnikowski (eds.). *Zarys prawa cywilnego…*, pp. 169 *et seq.*; Zagrobelny, K. (2018) Op. cit.., p. 277; Machnikowski, P., Balcarczyk, J. and Drela, M. (2017) Op. cit., pp. 29, 57; Machnikowski, P. (2017a) Op. cit., p. 140. Cf. *The Civil Code. Kodeks cywilny* (2019). E. Kucharska (transl.). Warszawa: Wydawnictwo C.H. Beck, pp. 38–39.

[50] Cf. Szczerbowski, J.J. (2018a) Op. cit., pp. 35, 98–90, 101, 183.

[51] Cf. Grykiel, J. (2018) Op. cit., pp. 593–594; Janas, A. (2018) Op. cit., p. 531.

[52] Cf. Janas, A. (2018) Op. cit., p. 531; Sobolewski, P. (2018) Op. cit., pp. 547–548.

[53] It should be noted that in legal analyses of smart contracts attention is drawn to declarative programming languages as a possible alternative to imperative programming languages, currently dominant as far as smart contract coding is concerned. Declarative languages are expected to prove more readily understandable and facilitate drafting smart contract content. For more on this issue, see: Governatori, G. et al. (2018) Op. cit., pp. 378, 387 *et seq.*; Szostek, D. (2018) Op. cit., pp. 125–126.

translated consecutively into code.[55] Additional determinant affecting smart contracts comprehensibility is the sequence of code conversions required in order to render the programme executable. The initial source code – while to some extent retaining intelligibility owing to its resemblance to natural language – is then subject to conversion into assembler code which, in turn, necessitates to be compiled into machine-executable bytecode.[56] Consequently, there is a growing possibility of divergence between the parties' common intent and the smart contract programme executed automatically.[57]

What shall be viewed as a highly problematic issue in that regard is the interpretation of smart contracts' content. This is mostly due to the particularity of interpretation based on the operation of source code compiler.[58] In the light of the above considerations, the question as to possible replacement of contractual interpretation in the juridical sense by machine-driven interpretation pertaining to smart contracts as well as the very legal relevance of the latter, requires critical assessment.[59] Whilst, on the one hand, it is argued that the existing contract law interpretative rules do not apply to machine-based interpretation of smart contracts,[60] on the other there are calls for judicial activity supporting rational implementation of the Civil Code provisions regarding contractual interpretation in the domain of smart contracts.[61] In line with a widely accepted approach, interpretation process encompasses a set of operations

---

[54] An additional factor emphasised in this regard is that programming languages used to create smart contracts, as well as their compilers, continue to evolve rapidly which renders them prone to errors (see: Szczerbowski, J.J. (2018a) Op. cit., pp. 122, 133–134, 184). For more on the consequences of the unintelligibility of programming languages used to code smart contracts, cf. also: Carron, B. and Botteron, V. (2019) Op. cit., p. 129; Cannarsa, M. (2018) Op. cit., p. 784; Giancaspro, M. (2017) Op. cit., pp. 831 *et seq.*

[55] For more on this issue, see: Cannarsa, M. (2018) Op. cit., pp. 777 *et seq.*; Giancaspro, M. (2017) Op. cit., pp. 831 *et seq.*; Mik, E. (2017) Op. cit., pp. 287 *et seq.*

[56] Cf. Szczerbowski, J.J. (2018a) Op. cit., pp. 133–135, 184. See also: Allen, J.G. (2018) Op. cit., pp. 331, 336; Governatori, G. et al. (2018) Op. cit., pp. 387, 395, 405–406.

[57] Szczerbowski, J.J. (2018a) Op. cit., p. 135. Cf. also: Cannarsa, M. (2018) Op. cit., pp. 781, 784.

[58] For more on this issue, see: Governatori, G. et al. (2018) Op. cit., pp. 393 *et seq.*; Szczerbowski, J.J. (2018a) Op. cit., pp. 13–14, 133 *et seq.* Cf. also: Giancaspro, M. (2017) Op. cit., pp. 831, 832–833.

[59] For more on the comparative study of the issue of contractual interpretation in the light of deterministic nature of computer languages, including mainly differences between common law and civil law approaches to contract drafting techniques and interpretation of contracts, see: Cannarsa, M. (2018) Op. cit., pp. 779–780, 782, 883.

[60] Savelyev, A. (2017) Op. cit., p. 125.

[61] Cf. Szczerbowski, J.J. (2018a) Op. cit., p. 133. On the need for ascertaining a way for courts to interpret automated contracts, see: Cannarsa, M. (2018) Op. cit., p. 785. Cf. also: DiMatteo, L.A. and Poncibò, C. (2018) Op. cit., pp. 808, 809.

leading subsequently towards establishing whether a given expression (arrangement of signs) manifested by the party performs the regulatory function and therefore constitutes a declaration of intent, and afterwards identifying its legally relevant meaning.[62] The general interpretative rules applicable to contracts in Polish private law are structured according to so--called combined (subjective-objective) method which is axiologically conditioned.[63] The methodology of interpretation process aims at considering respectively, to the extent appropriate, the real intention of the subject performing the declaration of intent (which refers also to the common intent of the contracting parties) and the reliance of third parties as well as the certainty of legal transactions.[64] Thus, a declaration of intent shall be interpreted so as is required, in view of the circumstances in which it was made, by principles of social coexistence and established customs, whereas in contracts, one should examine the common intention of the parties and the aim of the contract rather than rely on its literal wording.[65] Several characteristics of the process of smart contracts coding need to be analysed on this point. Essentially, the necessity to predetermine in advance, in a precise and comprehensive manner every condition to be met in order to automatically perform a predefined action, raises doubts as to consistency with the contract law framework, including the contractual interpretation model. The use of programming languages which serve to code smart contract terms results in considerable inflexibility that is found incompatible with both the inherent peculiarities and axiology of contract law and contract drafting practice.[66] Yet, private law general clauses[67] and open-textured standards (such as good faith, reasonableness or due diligence) are of vital importance for contractual interactions.[68] The reference to the general clause of "principles of social coexistence"[69] in the interpretative regime serves as a criterion according to which among a number of possible interpretation results one shall prefer the meaning of the contractual clause that proves to the highest degree in conformity

[62] Cf. i.a.: Grykiel, J. (2018) Op. cit., pp. 641–642; Machnikowski, P. (2017a) Op. cit., p. 151.

[63] See i.a.: Radwański, Z. and Mularski, K. (2019a) Wykładnia oświadczeń woli. In: A. Olejniczak and Z. Radwański (eds.). *System prawa prywatnego*. 2, pp. 85 *et seq.*; Grykiel, J. (2018) Op. cit., p. 647; Machnikowski, P. (2017a) Op. cit., pp. 152–153; Machnikowski, P., Balcarczyk, J. and Drela, M. (2017) Op. cit., pp. 101–102; Rott-Pietrzyk, E. (2013) Op. cit., pp. 23 *et seq.*, 67 *et seq.* Cf. also: Kaczorowska, B. (2018a) Op. cit., pp. 289 *et seq.*

[64] Cf. Radwański, Z. and Mularski, K. (2019a) Op. cit., pp. 85–86; Machnikowski, P. (2017a) Op. cit., p. 152; Grykiel, J. (2018) Op. cit., pp. 647–648; Bierć, A. (2018) Op. cit., pp. 763–766.

[65] See: art. 65 of the Civil Code. For more on this issue, cf. i.a.: Machnikowski, P., Balcarczyk, J. and Drela, M. (2017) Op. cit., pp. 98 *et seq.*; Rott-Pietrzyk, E. (2013) Op. cit., pp. 67 *et seq.*

with binding moral norms.[70] Such objectivised interpretation involving the standard of accordance with moral norms is viewed in relation to the requirement of due diligence and so-called reasonableness test, assuming not only rationality of judgements but also a demand for honest and fair conduct.[71] By contrast, it results exceedingly difficult to give effect to the above interpretative criteria within the operation of the smart contract source code compiler as the abstract concepts referred to in the aforementioned general clauses prove ineligible to be represented as an algorithm, and therefore untranslatable into a computer processable

---

[66] Cf. i.a.: Sklaroff, J.M. (2017) Op. cit., pp. 267, 277 *et seq.*, 291 *et seq.*; DiMatteo, L.A. and Poncibò, C. (2018) Op. cit., pp. 813–814; Druck, J.A. (2018) Op. cit., pp. 7–9; Levy, K.E.C. (2017) Op. cit., p. 10; Mik, E. (2017) Op. cit., pp. 292 *et seq.*; Hsiao, J.I.-H. (2017) Op. cit., pp. 690–691. See also: Szczerbowski, J.J. (2018a) Op. cit., p. 18; Werbach, K. and Cornell, N. (2017) Op. cit., p. 367. It should be noted that attention is drawn to resemblance between the mechanism pertaining to smart contract coding and the practice of inserting entire agreement clauses (merger clauses) in contracts in writing (on this issue cf.: Cannarsa, M. (2018) Op. cit., pp. 782–783). For more on the effectiveness of merger clauses from Polish contract law perspective, see i.a.: Machnikowski, P. (2015a) Merger Clause in Contracts under Polish Law. In: B. Gessel-Kalinowska vel Kalisz (ed.). *The Challenges and the Future of Commercial and Investment Arbitration: Liber Amicorum Professor Jerzy Rajski*. Warsaw: Lewiatan Court of Arbitration, pp. 182–190; Strugała, R. (2013a) Merger Clauses in Contracts Governed by Polish Law. *Wroclaw Review of Law, Administration and Economics*, 3 (1), pp. 14–27; Pecyna, M. (2013) Op. cit., *passim*. For more on arguments provided to demonstrate compatibility of "smart contracting" with English law rules regarding contract formation, see: Durovic, M. and Janssen, A. (2018) Op. cit., pp. 761 *et seq.*

[67] General clauses perform multiple functions in the field of contract law, one of which is the interpretative function. For more on this issue, cf. i.a.: Rott-Pietrzyk, E. (2010) Klauzule generalne a wykonanie zobowiązania (z uwzględnieniem koncepcji systemu klauzul generalnych w projekcie kc). In: E. Gniewek, K. Górska and P. Machnikowski (eds.). *Zaciąganie i wykonywanie zobowiązań. Materiały III Ogólnopolskiego Zjazdu Cywilistów (Wrocław, 25–27.9.2008 r.)*. Warszawa: Wydawnictwo C.H. Beck, pp. 327–342; Machnikowski, P., Balcarczyk, J. and Drela, M. (2017) Op. cit., p. 100; Wilejczyk, M. (2014) *Zagadnienia etyczne części ogólnej prawa prywatnego*. Warszawa: Wydawnictwo C.H. Beck, pp. 65 *et seq.*; Piaskowy, A. (2012) Klauzule generalne w projekcie nowego kodeksu cywilnego. *Transformacje Prawa Prywatnego*, 3, pp. 49–67.

[68] Cf. i.a.: Carron, B. and Botteron, V. (2019) Op. cit., p. 115; Woebbeking, M.K. (2019) Op. cit., p. 109; DiMatteo, L.A. and Poncibò, C. (2018) Op. cit., pp. 809–810, 813; Giancaspro, M. (2017) Op. cit., pp. 831, 833; Mik, E. (2017) Op. cit., p. 294. See also: Machnikowski, P., Balcarczyk, J. and Drela, M. (2017) Op. cit., pp. 25–26.

[69] Formerly, under art. 107 of the Code of Obligations the major interpretative criterion was the concept of good faith in an objective sense. Along with the rule of interpretation in conformity with usages of fair dealing it was perceived as an instrument to ensure a higher ethical standard of contractual transactions (cf. Longchamps de Bérier, R. (1938) Op. cit., pp. 138 *et seq.*). On the relevance of the categories of good faith and usages of fair dealing in key conceptual framework pertaining to the Code of Obligations, see: Mańko, R. (2016) Towards a Typology of Dimensions of the Continuity and Discontinuity of Law: The Perspective of Polish Private Law after the 1989 Transformation. *Wroclaw Review of Law, Administration and Economics*, 6 (2), p. 114.

[70] Radwański, Z. and Mularski, K. (2019a) Op. cit., pp. 98–100; Machnikowski, P. (2017a) Op. cit., p. 153; Machnikowski, P. (2010) Op. cit., p. 124. See also: Machnikowski, P., Balcarczyk, J. and Drela, M. (2017) Op. cit.., p. 100; Bierć, A. (2018) Op. cit., pp. 770, 771, 774; Wilejczyk, M. (2014) Op. cit., pp. 226–227. For more on criticism towards adoption of a general clause based on moral judgements as an interpretative criterion in the recodification process, cf.: Machnikowski, P. (2017b) Op. cit., p. 85.

code.[72] Furthermore, the criterion of contextual interpretation is of substantial importance.[73] So-called situational context required to be taken into account by the interpreter encompasses external recognisable circumstances accompanying the performance of a declaration of intent.[74] The aforementioned elements become increasingly relevant in consideration of the foregoing tendency towards adopting more flexible approach to perception of the *pacta sunt servanda* principle, under which the judge shall be expected to give wider attention to extra-contract elements when reconstructing the relevant sense of the agreement.[75] In this regard, what shall be emphasised is the weightiness of context-dependent open-textured terms guaranteeing semantic flexibility characteristic of conventional contracts drafted in natural language.[76] On the contrary, the possibility to reach compliance with open-textured standards in the sphere of smart contracts is generally eliminated as far as any contractual term ambiguity or purposeful vagueness are viewed as inefficiencies smart contract mechanism is called to remove.[77] As another point of view, however, the line of reasoning aimed at demonstrating purported unambiguous

[71] Cf. i.a.: Radwański, Z. and Mularski, K. (2019a) Op. cit., pp. 96 *et seq.*; Bierć, A. (2018) Op. cit., pp. 770–771; Wilejczyk, M. (2014) Op. cit., pp. 223–226; Rott-Pietrzyk, E. (2013) Op. cit., pp. 68–69. For more on the interpretative criterion of reasonable understanding of a party's declaration proposed in the revised draft of the book one of the new Polish civil code of 2015, see: Machnikowski, P. (2017b) Op. cit., pp. 83–85.

[72] Cf. Mik, E. (2017) Op. cit., p. 294. See also: Carron, B. and Botteron, V. (2019) Op. cit., pp. 115 *et seq.*; Parola, L., Merati, P. and Gavotti, G. (2018) Blockchain e smart contract: questioni giuridiche aperte. *I Contratti,* 6, p. 686; Cannarsa, M. (2018) Op. cit., p. 785; Allen, J.G. (2018) Op. cit., pp. 336–338; Werbach, K. (2018) Op. cit., p. 527; Szczerbowski, J.J. (2018) Op. cit., p. 102; Bacina, M. (2018) Op. cit., p. 19; Giancaspro, M. (2017) Op. cit., p. 833; Sklaroff, J.M. (2017) Op. cit., p. 294. A separate issue to be considered is the means to interface the operation of smart contracts with the occurrences taking place outside the blockchain (for more on this aspect, see i.a.: Mik, E. (2017) Op. cit., pp. 278, 294–298; Durovic, M. and Janssen, A. (2018) Op. cit., p. 760; Szczerbowski, J.J. (2018a) Op. cit., pp. 130–132; 183–184; Werbach, K. (2018) Op. cit., pp. 545–548; Allen, J.G. (2018) Op. cit., pp. 337–338).

[73] It is argued that acontextual interpretation of contracts shall be excluded (cf. Rott-Pietrzyk, E. (2013) Op. cit., pp. 49, 71).

[74] For more on this issue, see i.a.: Machnikowski, P. (2017a) Op. cit., p. 155; Machnikowski, P., Balcarczyk, J. and Drela, M. (2017) Op. cit., pp. 99–100; Grykiel, J. (2018) Op. cit., pp. 655–656.

[75] Dajczak, W. (2017) Op. cit., p. 101.

[76] Cf. Governatori, G. et al. (2018) Op. cit., pp. 381, 396; Sklaroff, J.M. (2017) Op. cit., pp. 281 *et seq.*; Werbach, K. (2018) Op. cit., p. 527; Mik, E. (2017) Op. cit., p. 292. On this issue, with particular consideration of the relevance of inferences drawn from the context that shall affect the interpretation of smart contract code, see also: Allen, J.G. (2018) Op. cit., pp. 339–340. For more on the role of contract law intervention in the sphere of contracts which prove by their very nature incomplete, as the parties are unable to anticipate every future contingency when drafting a contract, cf.: Rodrigues, U.R. (2019) Law and the Blockchain. *Iowa Law Review*, 104 (2), pp. 681 *et seq.*

[77] See i.a.: Woebbeking, M.K. (2019) Op. cit., p. 109; Allen, J.G. (2018) Op. cit., pp. 336–338; DiMatteo, L.A. and Poncibò, C. (2018) Op. cit., pp. 812, 818; Sklaroff, J.M. (2017) Op. cit., pp. 263 *et seq.*; Mik, E. (2017) Op. cit., pp. 292–293. Cf. also: Savelyev, A. (2017) Op. cit., p. 125.

nature of a smart contract coded in programming languages is contested since it is persuaded that instead of eliminating ambiguity smart contracts only disguise it, as the technical process of determining the semantics of any computer programme actually proves to be socially contingent.[78] Moreover, the anonymity constituting a key feature of the mechanism underpinning smart contracts excludes the recourse to the interpretative criterion of commercial context when establishing the meaning of particular terms, hence substantially preventing their adequate implementation.[79] Accordingly, automated (machine-driven) interpretation of algorithmised smart contract terms does not permit to achieve an appropriate objective contract law pursues to reach in order to establish the content of the contracting parties' rights and obligations. What is more, as argued in critical research, in contrast to alleged smart contracts' self-sufficiency in the sphere of interpretation, the prospect for surmounting the interpretative difficulties intrinsic to conventional contracts shall be denied.[80] It seems therefore reasonable to exclude the eventuality of contractual interpretation being reduced to automated smart contract mechanism.[81]

Given the above properties of smart contracts "self-interpretation" and the constraints ensuing from the use of programming languages, arguably in like manner the operation designed to establish the content of obligation stemming from the arrangement instantiated in smart contract results discomposed. Yet, as reported previously, the juridical scheme of determining the legal effects a contract is supposed to produce requires its content to be properly established in the interpretation process but also involves regard to general clauses, in this case performing the normative function.[82] Consequently, the application of normatively required determinants regarding the due manner of the performance of contractual

[78] Grimmelmann, J. (2019) All Smart Contracts Are Ambiguous. *University of Pennsylvania Journal of Law and Innovation* (forthcoming). [online] Available from: https://ssrn.com/abstract=3315703 [Accessed 28 January 2019], pp. 2, 9 *et seq.* Cf. also: DiMatteo, L.A. and Poncibò, C. (2018) Op. cit., p. 811.

[79] Sklaroff, J.M. (2017) Op. cit., pp. 262, 291, 295 *et seq*. Cf. Szostek, D. (2018) Op. cit., p. 122. On the negative consequences of the parties' anonymity, see also: Werbach, K. (2018) Op. cit., p. 528; Bacina, M. (2018) Op. cit., p. 21.

[80] See: DiMatteo, L.A. and Poncibò, C. (2018) Op. cit., p. 811.

[81] Cf. also: Bobrowicz, P. (2017) Psychologiczny kontekst oraz domniemania interpretacyjne i normy prawne w wykładni oświadczeń woli. *Prawo i Więź*, 3, pp. 59–60.

[82] Cf. Radwański, Z. and Olejniczak, A. (2017) *Prawo cywilne – część ogólna*. Warszawa: Wydawnictwo C.H. Beck, p. 293; Wilejczyk, M. (2014) Op. cit., pp. 231 *et seq.*; Rott-Pietrzyk, E. (2010) Op. cit., pp. 327 *et seq.*, 333–334, 337–338.

obligation is to be excluded in the field of smart contracts. Thus, the obligation shall be performed in accordance with its content and in a manner consistent with its socio-economic purpose as well as with principles of social coexistence and if established customs exist in this respect, also consistent with these customs.[83] It is argued that "auto--executability" perceived as a smart contracts' distinctive feature corresponds to performance in a technological sense, and not in a contract law sense.[84] Another issue necessitating further critical appraisal is the consequence of smart contract automated enforcement resulting virtually in – apparently misconceived – "absolutisation" of the *pacta sunt servanda* principle and, hence, purported elimination of the contract law remedies aimed at protecting the creditor.[85] In substance, because of ineluctability of autonomous, algorithm-based implementation of the antecedently programmed action, the possibility that a smart contract be breached is supposed to be entirely excluded.[86] It is thus maintained that the mechanism of smart contracts itself ensures unquestionable performance, rendering the variety of institutionalised remedies and securities unnecessary and pointless.[87] Moreover, immutability of code claimed as an essential quality of blockchain-based smart contracts precludes – in principle – their adaptation in case of change of circumstances.[88] The aforesaid characteristics attributed to smart contracts stand in contrast to the juridical output developed in the sphere of contractual obligations. Indeed, it is argued that contract law is defined

[83] See: art. 354 of the Civil Code. For more on this issue, cf.: Machnikowski, P., Balcarczyk, J. and Drela, M. (2017) Op. cit., p. 88. It shall be noted that formerly art. 189 of the Code of Obligations adopted a general principle that the obligation be performed in accordance with its content, in a manner consistent with the requirements of good faith and with usages of fair dealing (cf. Longchamps de Bérier, R. (1938) Op. cit., pp. 317–319).

[84] See: Polański, P. (2019) Op. cit., p. 112.

[85] Savelyev, A. (2017) Op. cit., p. 130. For more on this issue, including polemical remarks, see i.a.: Cannarsa, M. (2018) Op. cit., p. 781; DiMatteo, L.A. and Poncibò, C. (2018) Op. cit., pp. 805–824; Werbach, K. and Cornell, N. (2017) Op. cit., pp. 318 *et seq.*; Raskin, M. (2017) Op. cit., pp. 310–311. Cf. also: Kaczorowska, B. (2018b) Zarys problematyki „prawa umów *in statu renascendi*". In: A. Dańko-Roesler et al. (eds.). *Ius est ars boni et aequi. Księga pamiątkowa dedykowana Profesorowi Józefowi Frąckowiakowi*. Wrocław: Stowarzyszenie Notariuszy Rzeczypospolitej Polskiej, p. 404.

[86] Savelyev, A. (2017) Op. cit., pp. 127, 130. On this issue see also: Caria, R. de. (2018) Op. cit., p. 740; DiMatteo, L.A. and Poncibò, C. (2018) Op. cit., p. 818; Werbach, K. and Cornell, N. (2017) Op. cit., p. 318.

[87] Savelyev, A. (2017) Op. cit., p. 130.

[88] Savelyev, A. (2017) Op. cit., pp. 127–130. On this issue, cf. also: Carron, B. and Botteron, V. (2019) Op. cit., pp. 120–121; Woebbeking, M.K. (2019) Op. cit., p. 110.

first and foremost by its remedial function and *ex post* intervention.[89] What deserves particular emphasis in this respect is the universality of Roman law experience with regard to creditor's remedies in the event of non-performance of obligation.[90] On the contrary, the algorithm-driven operation of code involves *ex ante* determination of the whole course of transaction, which is expected to lead towards smart contracts' self-sufficiency, calling into question the *ex post* adjudication model.[91] This tends to imply a reversal of elementary functions ascribed to the law of contractual obligations.[92] Further, it should be underlined that the requirement to honour contractual promises reflected in the *pacta sunt servanda* principle never operated as a principle being absolute in character.[93] As mentioned previously, one of the vital exceptions to the *pacta sunt servanda* rule is the *rebus sic stantibus* clause recognised under Polish law. In these terms, the pursuit of efficiency and certainty of transactions to be achieved through unarguable execution of pre-defined terms encoded into a smart contract contradicts the need for flexibility which is met by the law of contractual obligations.

5. CONCLUSION

In the light of the above remarks, it shall be assumed that there are grounds to consider some aspects of so-called smart contracts in terms of private law constructs, however, with a number of reservations. Most of these follow from the incompatibility between the properties of the mechanism underlying smart contracts and the intrinsic value system pertaining to contract law. The main smart contracts' inadequacy appears to amount to substantial dehumanisation of transactional process.[94]

---

[89] See: Werbach, K. (2018) Op. cit., p. 544; Werbach, K. and Cornell, N. (2017) Op. cit., pp. 318 *et seq.* Cf. DiMatteo, L.A. and Poncibò, C. (2018) Op. cit., pp. 813 *et seq.*

[90] For more on this issue see Dajczak, W. (2018) Op. cit., pp. 507–508.

[91] DiMatteo, L.A. and Poncibò, C. (2018) Op. cit., pp. 815 *et seq.*; Werbach, K. and Cornell, N. (2017) Op. cit., pp. 318 *et seq.*, 364.

[92] Werbach, K. and Cornell, N. (2017) Op. cit., p. 377. Cf. DiMatteo, L.A. and Poncibò, C. (2018) Op. cit., p. 813.

[93] Zimmermann, R. (1996) *The Law of Obligations: Roman Foundations of the Civilian Tradition*. *Oxford:* Oxford University Press, p. 578.

[94] Cf. i.a.: Mik, E. (2017) Op. cit., p. 270; Gambino, A. (2017) Op. cit., pp. 13–14. On postulates regarding the introduction of human intervention in the model of smart contract operation, see i.a.: Allen, J.G. (2018) Op. cit., pp. 339–338, 341–342. On arguments claiming yet human impact on the smart contracts coding process, cf. i.a.: Grimmelmann, J. (2019) Op. cit., pp. 11 *et seq.*, 21–23.

Particular interdependencies individualised *supra* from the perspective of Polish law can be identified to an extent in regard to other legal systems, mainly those belonging to the continental legal tradition,[95] given certain similarities among contract law frameworks in several aspects addressed within the scheme of the undertaken analysis. This is largely due to reception of essential Roman law principles relating to contractual obligations.[96] Accordingly, what could be substantially viewed in a generalised manner as points of concern, are mainly the inconsistencies between the specificity of smart contracts and the methodology of contractual interpretation, the manner of determining the content of contractual obligation as well as the criteria of its due performance. Nonetheless, as already outlined, it is argued that a comparative overview of interpretative models and contract drafting techniques provides insight into why a higher degree of compatibility can be discerned between smart contracts model and common law framework than when confronted with the civil law one.[97] Such an observation becomes all the more relevant as the influence of Anglo-American contract drafting style on both transnational and continental contractual practice is increasingly noticeable.[98]

Innovative solutions arising from smart contracts infrastructure are only of limited application.[99] The arguments that automated smart contracts will not constitute an alternative to traditional contracts, as they do not prove

[95] By way of example, on detailed analysis undertaken recently as regards characteristics of smart contracts in the light of Swiss law of obligations, see: Carron, B. and Botteron, V. (2019) Op. cit. pp. 101–143; as regards German law context, cf. i.a.: Woebbeking, M.K. (2019) Op. cit., pp. 106–113; as regards some aspects of the French contract law framework, cf. i.a.: Cannarsa, M. (2018) Op. cit., pp. 779–780. Particular attention shall be drawn to Italian law because of the introduction of a definition of smart contracts at the legislative level (see i.a.: Pardolesi, R. and Davola, A. (2019) Op. cit., pp. 297–316; Donna, L. Di (2019) Diritto e tecnologia. Il contratto ai tempi dell'intelligenza artificiale e la giustizia predittiva. In: F. Capriglione (ed.). *Liber Amicorum…*, pp. 319 *et seq.*; Parola, L., Merati, P. and Gavotti, G. (2018) Op. cit., pp. 681–688).

[96] Longchamps de Bérier, R. (1938) Op. cit., p. 3.

[97] Cannarsa, M. (2018) Op. cit., pp. 776, 781–182. According to this view, what determines the above congruity is the apparent correspondence between the specificity of coding process characteristic for smart contracts and predominantly objective approach towards interpretation of contracts under common law which, in turn, is reflected in contracting parties' tendency towards drafting extensive contracts including any possible contingency so that it is possible to exclude unforeseeable judicial decisions. On current models of contractual interpretation from comparative legal perspective and interrelation between interpretative regimes and standards of contract drafting, see also i.a.: Kaczorowska, B. (2018a) Op. cit., pp. 263–264, 316 *et seq.*, 468–473.

[98] For more on this issue, see i.a.: Machnikowski, P., Balcarczyk, J. and Drela, M. (2017) Op. cit., pp. 42–43; Łolik, M. (2014) Op. cit., pp. 3–4; Strugała, R. (2013a) Op. cit., pp. 14–16; Strugała, R. (2013b) Op. cit., pp. 2–4, 7–11, 345–347.

[99] Cf. DiMatteo, L.A. and Poncibò, C. (2018) Op. cit., pp. 813, 819–820, 823.

capable of safeguarding the parties' interests across all types of legal relations,[100] must be concurred with. It seems unquestionable that their implementation in practice shall not result in replacement of the existing legal framework nor annulment of contract law as such. What can be found suggestive is the call for a deeper analysis on the instances requiring the blockchain-based algorithmic constructs to be "combined" with human--interpreted legal institutions, based on an arguable assumption regarding the predisposition to coexist for both the smart contracts mechanism and contracts in a juridical sense.[101] However, any eventual form of such interaction, assuming but ancillary role of technological innovations, shall warrant respect for principles of the objective moral order reflected in the private law system as well as compliance with key functions contract law is expected to perform.[102] It appears appropriate to note that the debate on smart contracts from the legal perspective and the attempt to explore their impact on contractual practice contribute to accentuating the functionality and operability of the main contract law precepts.[103]

LIST OF REFERENCES

[1] Act of 23 April 1964 – Civil Code (ustawa – Kodeks cywilny, Journal of Laws of 2019 item 1145, as amended).

[2] Allen, J.G. (2018) Wrapped and Stacked: 'Smart Contracts' and the Interaction of Natural and Formal Language. *European Review of Contract Law*, 14 (4).

[3] Bacina, M. (2018) When Two Worlds Collide: Smart Contracts and the Australian Legal System. *Journal of Internet Law*, 21 (8).

[4] Bierć, A. (2018) *Zarys prawa prywatnego. Część ogólna*. Warszawa: Wolters Kluwer.

[5] Bobrowicz, P. (2017) Psychologiczny kontekst oraz domniemania interpretacyjne i normy prawne w wykładni oświadczeń woli. *Prawo i Więź*, 3.

[100] See: Szczerbowski, J.J. (2018a) Op. cit., p. 123. Cf. also: Szostek, D. (2019) Regulacje prawne drugiej dekady XXI wieku – dokąd zmierzamy? Czy zastąpi nas inżynieria prawa?. *Monitor Prawniczy*, 2, pp. 115, 118–119; Allen, J.G. (2018) Op. cit., p. 320; DiMatteo, L.A. and Poncibò, C. (2018) Op. cit., pp. 814, 823.

[101] Cf. Werbach, K. (2018) Op. cit., pp. 534 *et seq*., 544 *et seq*. See also: Mik, E. (2018) Op. cit., pp. 855, 866, 870. On suggested implementation of hybrid "code-and-contract" combinations, assuming smart contracts being accompanied by traditional contracts, cf. Durovic, M. and Janssen, A. (2018) Op. cit., pp. 767–768, 770–771.

[102] For more on main functions attributed to modern law of obligations, including the protective function, see i.a.: Radwański, Z. and Olejniczak, A. (2018) Op. cit., pp. 1–2.

[103] Cf. also: Werbach, K. and Cornell, N. (2017) Op. cit. , pp. 353 *et seq*., 374 *et seq.*

[6] Brzozowski, A. (2013) Pojęcie umowy w prawie polskim, funkcje umów. Źródła prawa regulującego umowy. In: *System prawa prywatnego*. 5: E. Łętowska (ed.). *Prawo zobowiązań – część ogólna*. Warszawa: Wydawnictwo C.H. Beck.

[7] Brzozowski, A. (2014) *Wpływ zmiany okoliczności na zobowiązania. Klauzula rebus sic stantibus*. Warszawa: Wydawnictwo C.H. Beck.

[8] Brzozowski, A. (2018) Wpływ zmiany okoliczności na zobowiązania. In: *System prawa prywatnego*. 6: A. Olejniczak (ed.). *Prawo zobowiązań – część ogólna.* Warszawa: Wydawnictwo C.H. Beck.

[9] Cannarsa, M. (2018) Interpretation of Contracts and Smart Contracts: Smart Interpretation or Interpretation of Smart Contracts?. *European Review of Private Law*, 26 (6).

[10] Caria, R. de. (2018) The Legal Meaning of Smart Contracts. *European Review of Private Law*, 26 (6).

[11] Carron, B. and Botteron, V. (2019) How Smart Can a Contract Be?. In: D. Kraus, T. Obrist and O. Hari (eds.). *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law*. Cheltenham–Northampton: Edward Elgar Publishing.

[12] Cieplak, J. and Leefatt, S. (2017) Smart Contracts: A Smart Way to Automate Performance. *Georgetown Law Technology Review*, 1 (2).

[13] Czepita, S. (2017) On the Concept of a Conventional Act and Its Types. *Ruch Prawniczy, Ekonomiczny i Socjologiczny*, 79 (1).

[14] Dajczak, W. (2012) *The Nature of the Contract in Reasoning of Civilian Jurists*. Poznań: Wydawnictwo Naukowe UAM.

[15] Dajczak, W. (2014) Kodeks zobowiązań jako lekcja metody prawnoporównawczej. *Kwartalnik Prawa Prywatnego*, 4.

[16] Dajczak, W. (2017) Amerykańska zapowiedź „śmierci umowy" na tle tradycji romanistycznej. In: F. Longchamps de Bérier (ed.). *Dekodyfikacja prawa prywatnego. Szkice do portretu*. Warszawa: Wydawnictwo Sejmowe.

[17] Dajczak, W. (2018) Zobowiązania. In: W. Dajczak, T. Giaro, F. Longchamps de Bérier. *Prawo rzymskie. U podstaw prawa prywatnego*. Warszawa: Wydawnictwo Naukowe PWN.

[18] Decree of the President of the Republic of Poland of 27 October 1933 – Code of Obligations (rozporządzenie Prezydenta Rzeczypospolitej – Kodeks zobowiązań, Journal of Laws No. 82, item 598, as amended).

[19] DiMatteo, L.A. and Poncibò, C. (2018) Quandary of Smart Contracts and Remedies: The Role of Contract Law and Self-Help Remedies. *European Review of Private Law*, 26 (6).

[20] Donna, L. Di. (2019) Diritto e tecnologia. Il contratto ai tempi dell'intelligenza artificiale e la giustizia predittiva. In: F. Capriglione (ed.). *Liber Amicorum Guido Alpa*. Milano: Cedam.

[21] Druck, J.A. (2018) "Smart Contracts" Are Neither Smart Nor Contracts: Discuss. *Banking & Financial Services Policy Report*, 37 (10).

[22] Durovic, M. and Janssen, A. (2018) The Formation of Blockchain-Based Smart Contracts in the Light of Contract Law. *European Review of Private Law*, 26 (6).

[23] Elizalde, F. de. (2018) The Sources and Effects of Contractual Terms: Towards Approximation of Common Law and Civil Law. In: F. de Elizalde (ed.). *Uniform Rules for European Contract Law?: A Critical Assessment*. Oxford: Hart Publishing.

[24] Gambino, A. (2017) Dignità umana e mercato digitale. *Diritto Mercato Tecnologia*.

[25] Geiregat, S. (2018) Cryptocurrencies Are (Smart) Contracts. *Computer Law & Security Review*, 34 (5).

[26] Geis, G.S. (2008) Automating Contract Law. *New York University Law Review*, 83 (2).

[27] Giancaspro, M. (2017) Is a 'Smart Contract' Really a Smart Idea?: Insights from a Legal Perspective. *Computer Law & Security Review*, 33 (6).

[28] Giaro, T. (2018) Kształtowanie i ochrona praw prywatnych. In: W. Dajczak, T. Giaro, F. Longchamps de Bérier. *Prawo rzymskie. U podstaw prawa prywatnego*. Warszawa: Wydawnictwo Naukowe PWN.

[29] Giaro, T. (2013) Some Prejudices about the Legal Tradition of Eastern Europe. In: B. Sitek, J.J. Szczerbowski and A.W. Bauknecht (eds.). *Comparative Law in Eastern and Central Europe*. Newcastle upon Tyne: Cambridge Scholars Publishing.

[30] Gnela, B. and Michałowska, K. (academic supervision). (2014) *Directions of Private Law Development: Comments on the Draft of Book One of the Civil Code*. Warszawa: Difin.

[31] Goldenfein, J. and Leiter, A. (2018) Legal Engineering on the Blockchain: 'Smart Contracts' as Legal Conduct. *Law and Critique*, 29 (2).

[32] Gorczyński, G. (2015) Klauzula *rebus sic stantibus* w XXI wieku. In: A. Olejniczak et al. (eds.). *Współczesne problemy prawa zobowiązań*. Warszawa: Lex a Wolters Kluwer Business.

[33] Governatori, G. et al. (2018) On Legal Contracts, Imperative and Declarative Smart Contracts, and Blockchain System. *Artificial Intelligence and Law*, 26 (4).

[34] Górska, K. (2018) Czynności prawne na tle innych zdarzeń cywilnoprawnych. In: E. Gniewek and P. Machnikowski (eds.). *Zarys prawa cywilnego*. Warszawa: Wydawnictwo C.H. Beck.

[35] Graziadei, M. (2007) *Variations on the Concept of Contract in a European Perspective*. In: R. Schulze (ed.). *New Features in Contract Law*. Munich: Sellier European Law Publishers.

[36] Grimmelmann, J. (2019) All Smart Contracts Are Ambiguous. *University of Pennsylvania Journal of Law and Innovation* (forthcoming). [online] Available from: https://ssrn.com/abstract=3315703 [Accessed 28 January 2019].

[37] Grundmann, S. and Hacker, P. (2017) Digital Technology as a Challenge to European Contract Law: From the Existing to the Future Architecture. *European Review of Contract Law*, 13 (3).

[38] Grykiel, J. (2018). In: M. Gutowski (ed.). *Kodeks cywilny*. 1: *Komentarz. Art. 1–352*. Warszawa: Wydawnictwo C.H. Beck.

[39] Hsiao, J.I.-H. (2017) Smart Contract on the Blockchain – Paradigm Shift for Contract Law?. *US-China Law Review*, 14 (10).

[40] Hulicki, M. and Lustofin, P. (2017) Wykorzystanie koncepcji blockchain w realizacji zobowiązań umownych. *Człowiek w Cyberprzestrzeni*, 1.

[41] Idelberger, F. (2018) Connected Contracts Reloaded – Smart Contracts as Contractual Networks. In: S. Grundmann (ed.). *European Contract Law in the Digital Age*. Cambridge–Antwerp–Portland: Intersentia.

[42] Janas, A. (2018). In: M. Habdas and M. Fras (eds.). *Kodeks cywilny. Komentarz*. 1: *Część ogólna (art. 1–125)*. Warszawa: Wolters Kluwer.

[43] Kaczorowska, B. (2018a) *Wykładnia umów obligacyjnych w świetle współczesnych tendencji rozwoju prawa prywatnego*. Wrocław: Wydawnictwo i Drukarnia Świętego Krzyża.

[44] Kaczorowska, B. (2018b) Zarys problematyki „prawa umów *in statu renascendi*". In: A. Dańko-Roesler et al. (eds.). *Ius est ars boni et aequi. Księga pamiątkowa dedykowana Profesorowi Józefowi Frąckowiakowi*. Wrocław: Stowarzyszenie Notariuszy Rzeczypospolitej Polskiej.

[45] Kaczorowska, M. (2009) Rekodyfikacja prawa cywilnego w Polsce wobec rozwoju europejskiego prawa prywatnego. Rozważania na tle projektu księgi pierwszej Kodeksu cywilnego. *Ruch Prawniczy, Ekonomiczny i Socjologiczny*, 3.

[46] Kasprzyk, K. (2018) The Concept of Smart Contracts from the Legal Perspective. *Review of Comparative Law*, 34 (3).

[47] Klinger, B. and Szczepański, J. (2017) Blockchain – historia, cechy i główne obszary zastosowań. *Człowiek w Cyberprzestrzeni*, 1.

[48] Kocot, W.J. (2017) Kontrakty kreatywne – nowy rozdział w cyberewolucji prawa umów. In: P. Kostański, P. Podrecki and T. Targosz (eds.). *Experientia docet. Księga jubileuszowa ofiarowana Pani Profesor Elżbiecie Traple*. Warszawa: Wolters Kluwer.

[49] Kolber, A.J. (2018) Not-So-Smart Blockchain Contracts and Artificial Responsibility. *Stanford Technology Law Review*, 21 (2).

[50] Komisja Kodyfikacyjna Prawa Cywilnego działająca przy Ministrze Sprawiedliwości. (2009) *Księga pierwsza Kodeksu cywilnego. Projekt z uzasadnieniem*. Warszawa: Wydawnictwo C.H. Beck.

[51] Konopacka, M. (2017) Kamienie milowe w rozwoju historycznym polskiego prawa umów. *Gdańskie Studia Prawnicze*, 38 (2).

[52] Kurosz, K. (2017) Zawieranie umów przez sztuczną inteligencję (systemy autonomiczne) a wady oświadczeń woli – wprowadzenie do problemu. In: W. Robaczyński (ed.). *Czynić postęp w prawie. Księga jubileuszowa dedykowana Profesor Birucie Lewaszkiewicz-Petrykowskiej.* Łódź: Wydawnictwo Uniwersytetu Łódzkiego.

[53] Levy, K.E.C. (2017) Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law. *Engaging Science, Technology, and Society*, 3.

[54] Longchamps de Bérier, F. (2016) Z uwag do metodologii nauki prawa prywatnego: argumenty historyczny, dogmatyczny i prawnoporównawczy na przykładzie darowizny na wypadek śmierci oraz zapisu windykacyjnego. In: A. Wudarski (ed.). *Polska komparatystyka prawa. Prawo obce w doktrynie prawa polskiego*. Warszawa: Stowarzyszenie Notariuszy Rzeczypospolitej Polskiej.

[55] Longchamps de Bérier, F. (2019) Decodification of Contract Law. In: C. Su, F. Longchamps de Bérier and P. Grzebyk (eds.). *Theory and Practice of Codification: The Chinese and Polish Perspectives*. Beijing: Social Sciences Academic Press.

[56] Longchamps de Bérier, R. (1938) *Zobowiązania.* Lwów: Księgarnia Wydaw. Gubrynowicz i Syn.

[57] Łolik, M. (2014) *Współczesne prawo kontraktów – wybrane zagadnienia*. Warszawa: Wydawnictwo C.H. Beck.

[58] Machnikowski, P. (2010) *Prawne instrumenty ochrony zaufania przy zawieraniu umowy*. Wrocław: Wydawnictwo Uniwersytetu Wrocławskiego.

[59] Machnikowski, P. (2013a) Struktura zobowiązania. In: *System prawa prywatnego*. 5: E. Łętowska (ed.). *Prawo zobowiązań – część ogólna*. Warszawa: Wydawnictwo C.H. Beck.

[60] Machnikowski, P. (2013b) Swoboda umów. In: *System prawa prywatnego*. 5: E. Łętowska (ed.). *Prawo zobowiązań – część ogólna*. Warszawa: Wydawnictwo C.H. Beck.

[61] Machnikowski, P. (2013c) Treść umowy. In: *System prawa prywatnego*. 5: E. Łętowska (ed.). *Prawo zobowiązań – część ogólna*. Warszawa: Wydawnictwo C.H. Beck.

[62] Machnikowski, P. (2014) Poland. In: J. Hurdík, P. Lavický et al. (eds.). *Private Law Reform*. Brno: Masaryk University.

[63] Machnikowski, P. (2015a) Merger Clause in Contracts under Polish Law. In: B. Gessel--Kalinowska vel Kalisz (ed.). *The Challenges and the Future of Commercial and Investment Arbitration: Liber Amicorum Professor Jerzy Rajski*. Warsaw: Lewiatan Court of Arbitration.

[64] Machnikowski, P. (2015b) Prawo zobowiązań w 2025 roku. Nowe technologie, nowe wyzwania. In: A. Olejniczak et al. (eds.). *Współczesne problemy prawa zobowiązań*. Warszawa: Lex a Wolters Kluwer Business.

[65] Machnikowski, P. (2017a). In: E. Gniewek and P. Machnikowski (eds.). *Kodeks cywilny. Komentarz*. Warszawa: Wydawnictwo C.H. Beck.

[66] Machnikowski, P. (2017b). In: P. Machnikowski (ed.). *Kodeks cywilny. Księga pierwsza. Część ogólna. Projekt Komisji Kodyfikacyjnej Prawa Cywilnego przyjęty w 2015 r. z komentarzem członków Zespołu Problemowego KKPC*. Warszawa: Wydawnictwo C.H. Beck.

[67] Machnikowski, P., Balcarczyk, J. and Drela, M. (2017) *Contract Law in Poland*. Alphen aan den Rijn: Kluwer Law International.

[68] Malby, S. (2017) Strengthening the Rule of Law through Technology. *Commonwealth Law Bulletin*, 43 (3–4).

[69] Mańko, R. (2016) Towards a Typology of Dimensions of the Continuity and Discontinuity of Law: The Perspective of Polish Private Law after the 1989 Transformation. *Wroclaw Review of Law, Administration and Economics*, 6 (2).

[70] Mik, E. (2017) Smart Contracts: Terminology, Technical Limitations and Real World Complexity. *Law, Innovation and Technology*, 9 (2).

[71] Mik, E. (2018) Electronic Platforms: Openness, Transparency & Privacy Issues. E*uropean Review of Private Law*, 26 (6).

[72] Millard, C. (2018) Blockchain and Law: Incompatible Codes? *Computer Law & Security Review*, 34 (4).

[73] Ministerstwo Cyfryzacji. (2019) *Grupa robocza ds. rejestrów rozproszonych i blockchain.* [online] Available from: https://www.gov.pl/web/cyfryzacja/grupa-robocza-ds-rejestrow-rozproszonych-i-blockchain1 [Accessed 7 August 2019].

[74] Pardolesi, R. and Davola, A. (2019) "Smart contract": lusinghe ed equivoci dell'innovazione purchesia. In: F. Capriglione (ed.). *Liber Amicorum Guido Alpa*. Milano: Cedam.

[75] Parola, L., Merati, P. and Gavotti, G. (2018) Blockchain e smart contract: questioni giuridiche aperte. *I Contratti*, 6.

[76] Pecyna, M. (2013) *Merger clause jako zastrzeżenie wyłączności dokumentu, klauzula integralności umowy, reguła wykładni umowy*. Warszawa: Lex a Wolters Kluwer Business.

[77] Piaskowy, A. (2012) Klauzule generalne w projekcie nowego kodeksu cywilnego. *Transformacje Prawa Prywatnego*, 3.

[78] Polański, P. (2019) Inwigilacja, dostępność, blockchain i sztuczna inteligencja: pytania o kierunki rozwoju prawa nowych technologii w erze rewolucji internetowej. *Monitor Prawniczy*, 2.

[79] Radwański, Z. and Mularski, K. (2019a) Wykładnia oświadczeń woli. In: A. Olejniczak and Z. Radwański (eds.). *System prawa prywatnego*. 2: *Prawo cywilne – część ogólna*. Warszawa: Wydawnictwo C.H. Beck.

[80] Radwański, Z. and Mularski, K. (2019b) Zagadnienia ogólne czynności prawnych. In: A. Olejniczak and Z. Radwański (eds.). *System prawa prywatnego*. 2: *Prawo cywilne – część ogólna*. Warszawa: Wydawnictwo C.H. Beck.

[81] Radwański, Z. and Olejniczak, A. (2017) *Prawo cywilne – część ogólna*. Warszawa: Wydawnictwo C.H. Beck.

[82] Radwański, Z. and Olejniczak, A. (2018) *Zobowiązania – część ogólna*. Warszawa: Wydawnictwo C.H. Beck.

[83] Raskin, M. (2017) The Law and Legality of Smart Contracts. *Georgetown Law Technology Review*, 1 (2).

[84] Reyes, C.L. (2018) Cryptolaw for Distributed Ledger Technologies: A Jurisprudential Framework. *Jurimetrics: The Journal of Law, Science & Technology*, 58 (3).

[85] Ridder, C.A. de, Tunstall, M.K. and Prescott, N. (2017) Recognition of Smart Contracts in the United States. *Intellectual Property & Technology Law Journal*, 29 (11).

[86] Rodrigues, U.R. (2019) Law and the Blockchain. *Iowa Law Review*, 1014 (2).

[87] Rohr, J. (2019) Smart Contracts in Traditional Contract Law, Or: The Law of the Vending Machine. *Cleveland State Law Review*, 67 (1).

[88] Romanowski, M. (2013) Position of the Law of Obligations in Polish Law in the Context of a Reform of the European Law of Obligations. In: R. Schulze and F. Zoll (eds.).

The Law of Obligations in Europe: A New Wave of Codifications. Munich: Sellier European Law Publishers.

[89] Rott-Pietrzyk, E. (2010) Klauzule generalne a wykonanie zobowiązania (z uwzględnieniem koncepcji systemu klauzul generalnych w projekcie kc). In: E. Gniewek, K. Górska and P. Machnikowski (eds.). *Zaciąganie i wykonywanie zobowiązań. Materiały III Ogólnopolskiego Zjazdu Cywilistów (Wrocław, 25–27.9.2008 r.)*. Warszawa: Wydawnictwo C.H. Beck.

[90] Rott-Pietrzyk, E. (2013) *Interpretacja umów w prawie modelowym i wspólnym europejskim prawie sprzedaży (CESL)*. Warszawa: Wydawnictwo C.H. Beck.

[91] Rudnicki, J. (2018) *Dekodyfikacja prawa cywilnego w Polsce*. Bielsko-Biała: Wydawnictwo Od.Nowa.

[92] Samolewicz, S. (1937) *Zarys polskiego prawa zobowiązań*. Lwów: Skł. gł. Księgarnia T.S.L.

[93] Savelyev, A. (2017) Contract Law 2.0: 'Smart' Contracts as the Beginning of the End of Classic Contract Law. *Information & Communications Technology Law*, 26 (2).

[94] Scholz, L.H. (2017) Algorythmic Contracts. *Stanford Technology Law Review*, 20 (2).

[95] Schulze, R. and Staudenmayer, D. (2016) Digital Revolution – Challenges for Contract Law. In: R. Schulze and D. Staudenmayer (eds.). *Digital Revolution: Challenges for Contract Law in Practice*. Baden-Baden: Nomos.

[96] Sellwood, M. (2017) The Road to Autonomy. *San Diego Law Review*, 54 (4).

[97] Sklaroff, J.M. (2017) Smart Contracts and the Cost of Inflexibility. *University of Pennsylvania Law Review*, 166 (1).

[98] Sobolewski, P. (2017). In: K. Osajda (ed.). *Kodeks cywilny. Komentarz*. 1: *Część ogólna. Przepisy wprowadzające kc. Prawo o notariacie (art. 78–95 i 96–99)*. Warszawa: Wydawnictwo C.H. Beck.

[99] Strugała, R. (2013a) Merger Clauses in Contracts Governed by Polish Law. *Wroclaw Review of Law, Administration and Economics*, 3 (1).

[100] Strugała, R. (2013b) *Standardowe klauzule umowne: adaptacyjne, salwatoryjne, merger, interpretacyjne oraz pactum de forma*. Warszawa: Wydawnictwo C.H. Beck.

[101] Szczerbowski, J.J. (2018a) *Lex cryptographia. Znaczenie prawne umów i jednostek rozliczeniowych opartych na technologii blockchain*. Warszawa: Wydawnictwo Naukowe PWN.

[102] Szczerbowski, J.J. (2018b) Transaction Costs of Blockchain Smart Contracts. *Law and Forensic Science*, 16 (2).

[103] Szostek, D. (2018) *Blockchain a prawo*. Warszawa: Wydawnictwo C.H. Beck.

[104] Szostek, D. (2019) Regulacje prawne drugiej dekady XXI wieku – dokąd zmierzamy? Czy zastąpi nas inżynieria prawa?. *Monitor Prawniczy*, 2.

[105] Temte, M.N. (2019) Blockchain Challenges Traditional Contract Law: Just How Smart Are Smart Contracts?. *Wyoming Law Review*, 19 (1).

[106] *The Civil Code. Kodeks cywilny* (2019). E. Kucharska (transl.). Warszawa: Wydawnictwo C.H. Beck.

[107] Werbach, K. (2018) Trust, but Verify: Why the Blockchain Needs the Law. *Berkeley Technology Law Journal*, 33 (2).

[108] Werbach, K. and Cornell, N. (2017) Contracts Ex Machina. *Duke Law Journal*, 67 (2).

[109] Wheeler, S. (2017) Visions of Contract. *Journal of Law and Society*, 44 (S1).

[110] Wilejczyk, M. (2014) *Zagadnienia etyczne części ogólnej prawa prywatnego*. Warszawa: Wydawnictwo C.H. Beck.

[111] Włodyka, S. and Spyra, M. (2017) Ogólna charakterystyka umów handlowych. In: M. Stec (ed.). *System prawa handlowego*. 5: *Prawo umów handlowych*, Warszawa: Wydawnictwo C.H. Beck.

[112] Woebbeking, M.K. (2019) The Impact of Smart Contracts on Traditional Concepts of Contract Law. *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 10 (1).

[113] Zagrobelny, K. (2018a) Umowy jako źródło zobowiązań. In: E. Gniewek and P. Machnikowski (eds.). *Zarys prawa cywilnego*. Warszawa: Wydawnictwo C.H. Beck.

[114] Zagrobelny, K. (2018b) Wykonanie zobowiązania, In: E. Gniewek and P. Machnikowski (eds.). *Zarys prawa cywilnego*. Warszawa: Wydawnictwo C.H. Beck.

[115] Zimmermann, R. (1996) *The Law of Obligations: Roman Foundations of the Civilian Tradition*. Oxford: Oxford University Press.

[116] Zweigert, K. and Kötz, H. (2011) *Introduction to Comparative Law*. transl. T. Weir. Oxford: Clarendon Press.

DOI 10.5817/MUJLT2019-2-4

REGULATORY APPROACHES TO FACEBOOK AND OTHER SOCIAL MEDIA PLATFORMS: TOWARDS PLATFORMS DESIGN ACCOUNTABILITY*

by

JÁN MAZÚR**, MÁRIA T. PATAKYOVÁ***

The paper represents a contribution to the ongoing discussion on regulating social media platforms (SMP) and especially Facebook, mostly fueled by a recent series of scandals such as Cambridge Analytica, which highlighted the recognized problem of Facebook's lack of accountability. In response to the scandal, which coincided with long-expected wide-scale implementation of the EU's GDPR, Facebook introduced a series of measures on its platform, such as improved traceability of advertisers, or greater power over one's own data. Besides, Facebook was put under scrutiny of competition law authorities, mainly the German Bundeskartellamt. Taking into consideration all the regulatory approaches, the question remains whether sufficiently effective design for holding the SMPs accountable has been established or not. In the paper, we first outline the accountability issues SMPs currently face, namely the data handling and privacy issue, the platforms' impact on political processes, or related monopolistic positioning. We ascertain that common denominator of these issues is the platforms' design, which is created to achieve business objectives, while imposing substantial negative externalities on the society. Alongside, we review the platforms' reactions, i.e. the self-regulatory measures adopted by the platforms in 2017–2018. We also specifically focus on the evaluation of the competition law

* This contribution is the result of the project implementation APVV-16-0553 *Metamorphoses and innovations of the corporations´ concept under conditions of globalisation (Premeny a inovácie konceptu kapitálových spoločností v podmienkach globalizácie)*.

** jan.mazur@flaw.uniba.sk, Assistant Professor, Department of Financial Law, Faculty of Law, Comenius University in Bratislava, Slovak Republic.

*** maria.patakyova2@flaw.uniba.sk, Assistant Professor, Institute of European Law, Faculty of Law, Comenius University in Bratislava, Slovak Republic.

as one instrument of regulating certain aspects of the platforms, especially in light of the recent German Bundeskartellamt decision on Facebook. We claim that most of the measures and current instruments, although improving the lack of accountability, fall short of addressing the core issue of Facebook's status – absence of scrutiny over the platform's design.

KEY WORDS

Abuse of Dominant Position, Accountability, Competition Law, Data Protection, Facebook, Platform's Design, Self-regulation, Social Media Platforms

1. INTRODUCTION

Facebook and other social media platforms (SMP) ventured far from being generally understood as actors for the common good.[1] There were numerous cases of abuses of the platforms, by third parties or platforms themselves, accidental or deliberate. Notorious influencing of elections in USA, or France, based on fake profiles and bots, creation and amplification of fake content, led to massive investigation and political uproar.[2] Such events are a reason for great concern, particularly to established democracies as they appear to be more susceptible to fake news techniques.[3] The mishandling of users' data by *Facebook*, especially in relation to third parties such as *Cambridge Analytica*, is alarming.[4] SMPs also became means of promotion of religious and racial hatred against

[1] Tufekci, Z. (2018) How social media took us from Tahrir Square to Donald Trump. *MIT Technology Review*. [online] Available from: http://www.technologyreview.com/s/611806/how-social-media-took-us-from-tahrir-square-to-donald-trump/ [Accessed 15 March 2019].

[2] Guess, A., Nagler, J. and Tucker, J. (2019) Less than you think: Prevalence and predictors of fake news dissemination on Facebook. *Science Advances,* 5 (1). [online] doi: 10.1126/sciadv.aau4586 [Accessed 15 March 2019]; Ferrara, E. (2017) Disinformation and social bot operations in the run up to the 2017 French presidential election. *First Monday,* 22 (8). [online] doi: 10.5210/fm.v22i8.8005 [Accessed 15 March 2019]; Allcott, H. and Gentzkow, M. (2017) Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives,* 31 (2), pp. 211–236. [online] doi: 10.1257/jep.31.2.211 [Accessed 15 March 2019]; Hansen, I. and Lim, D. J. (2018) Doxing democracy: influencing elections via cyber voter interference. *Contemporary Politics,* 25 (2), pp. 150–171. [online] doi: 10.1080/13569775.2018.1493629 [Accessed 15 March 2019]; see the *US Senate Judiciary Committee's* report in Senate Judiciary Committee. (2017) *Extremist content and Russian disinformation online: Working with tech to find solutions.* [online] Available from: www.judiciary.senate.gov/meetings/extremist-content-and-russian-disinformation-online-working-with-tech-to-find-solutions [Accessed 15 March 2019].

[3] Farrell, H. J. and Schneier, B. (2018) Common-Knowledge Attacks on Democracy. *SSRN Electronic Journal*. [online] doi: 10.2139/ssrn.3273111 [Accessed 15 March 2019].

[4] Isaak, J. and Hanna, M. J. (2018) User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer,* 51 (8), pp. 56–59. [online] doi: 10.1109/mc.2018.3191268 [Accessed 15 March 2019]; Bartlett, J. (2018) Big data is watching you – and it wants your vote. *The Spectator,* 24 March. [online] Available from: https://www.spectator.co.uk/2018/03/big-data-is-watching-you-and-it-wants-your-vote/ [Accessed 15 March 2019].

certain communities (e.g. the case of *Rohingya*, mob murders in India).[5] To sum it up, the platforms have become political market places with wide social implications, which necessarily leads to the question of accountability of the platforms.[6]

The paper focuses on the issue of accountability while it examines the regulatory approaches towards the platforms. In particular, the paper asks, first, what are the factors suggesting the lack of accountability of SMPs; second, whether SMPs may be efficiently regulated by currently available regulatory mechanisms, in particular by competition law after the *Bundeskartellalmt Facebook* decision; and third, what the underlying problems of regulating SMPs are.

In the first part, we review accountability deficits, selected according to their gravity and representativeness in the media, and reflect on the current regulatory regimes. We also briefly review self-regulatory measures applied by the platforms. In the second part of the paper, we specifically focus on the recent development in the competition law in relation to SMPs. Finally, we discuss prospective regulatory measures.

2. ACCOUNTABILITY DEFICITS OF SMPS

One of the core issues of platforms lies in the legal understanding of platforms: what are SMPs from legal point of view? SMPs have long been recognized as internet service providers (ISP), who are generally not responsible for the content published on their services by the users.[7] Unlike ISPs, traditional media are responsible and liable for the published content, as they are gatekeepers for third party content, and they produce content on their own. Understanding SMPs as traditional media requires making them responsible for the users' content, which is not feasible and could be arguably disproportionate as to the objectives of such measure.[8] But while SMPs do not produce content, their algorithms curate the content on behalf

---

[5] Goel, V. et al. (2018) How WhatsApp Leads Mobs to Murder in India. *The New York Times,* 18 July. [online] Available from: http://www.nytimes.com/interactive/2018/07/18/technology/whatsapp-india-killings.html [Accessed 15 March 2019]; Müller, K. and Schwarz, C. (2017) Fanning the Flames of Hate: Social Media and Hate Crime. *SSRN Electronic Journal*. [online] doi: 10.2139/ssrn.3082972 [Accessed 15 March 2019].

[6] Ceron, A. (2018) *Social Media and Political Accountability Bridging the Gap between Citizens and Politicians.* Cham, Switzerland: Palgrave Macmillan, p. 205.

[7] Jeweler, M. G. (2008) The Communications Decency Act of 1996: Why § 230 is Outdated and Publisher Liability for Defamation Should be Reinstated Against Internet Service Providers. *Pittsburgh Journal of Technology Law and Policy*, 8. [online] doi: 10.5195/tlp.2008.40 [Accessed 15 March 2019].

of users, for instance in prioritization and personalization. Such curation is not unlike curation in traditional media, although done automatically and with high degree of personalization.[9]

Understanding SMPs as a form of traditional media does not capture the nature of SMPs to their full extent. From a socio-political perspective, SMPs seem to effectively serve as online public fora. Some recent court decisions underline the political nature and importance of such public fora for free speech. For instance, in recent *Knight First Amendment Institute v. Trump (2018)*, the court held that the President's *Twitter* account effectively serves as a public forum and that

> *"the blocking of the plaintiffs based on their political speech constitutes viewpoint discrimination that violates the First Amendment"*.[10]

Commenting and disagreeing with online statuses and tweets constitutes protected speech with protected access.[11] A similar decision was reached by the *US District Court* in Virginia, upheld by the *4th US Circuit Court of Appeals* in 2019, when the court held that a *Facebook* page is deliberately designed to be a "public forum", which if used by the politicians, represents a constitutionally protected space. If a politician designates such space as a place or channel of communication for use by the public, notwithstanding that it is placed on a privately-operated platform, it is *"more than sufficient to create a forum for speech"*.[12]

---

[8] Although the platforms have long moderated the content and their users, in many instances they did so based on unclear and changing private rules, which cannot be influenced by the users, and with limited recourse. SMPs create a unique type of cyberspaces with continuous monitoring of economically, socially and politically relevant behavior, which brings in well-recognized identity dilemma; anonymity breeds abuses of free speech, cyberbullying, and trolling, yet disclosure brings profiling and privacy risks.

[9] Lazer, D. (2015) The rise of the social algorithm. *Science,* 348 (6239), pp. 1090–1091. [online] doi: 10.1126/science.aab1422 [Accessed 15 March 2019].

[10] Calvert, C. (2018) Federal judge rules Trump's Twitter account is a public forum. *The Conversation,* 24 May. [online] Available from: http://theconversation.com/federal-judge-rules-trumps-twitter-account-is-a-public-forum-97159 [Accessed 15 March 2019].

[11] The ruling (2nd instance decision pending) has numerous implications. First, it implies that the existence of myriads of public fora, i.e. the walls, feeds and posts of individual politicians and publicly active persons, who are ascribed responsibility for maintaining the integrity of these fora. The content responsibility of platforms remains limited. Second, a question of restricting other people from access to the public fora based on different grounds, such as they are banned from SMPs on different grounds, based on private regulation arises. Third, it does not deal specifically with cross-jurisdictional issues and related options of recourse. The decision does not represent a regulation of SMPs but rather public figures and public bodies active on SMPs.

[12] *Brian C. Davison v. Loudon County Board of Supervisors et al.* (2017) 1:16cv932 (JCC/IDD).

2.1. INCREASE OF SELF-REGULATORY EFFORTS

Once SMPs are understood as media or as public fora, admittedly, they should maintain a degree of control of what is written thereon. Although for a long time SMPs were hesitant as to the regulation of users' content, it has become clear that some users' behavior is considered undesirable by the general public, or as *Facebook* puts it, there is "bad content" produced by "bad actors".[13] While it may be clear in most instances what represents a bad content and who the bad actor is, there should certainly be a wider policy discussion on this, involving public sector, given the importance of these fora for the public discourse. As a part of the efforts to regulate bad content, *Facebook* started to publish regular reports on its conduct. However, SMPs need well-staffed teams of content moderators – native speakers – in order to understand local contexts, irony, sarcasm, in prevention of harassing reports.[14]

The debate over content moderation also leads to the question of independent review of SMPs' decisions. *Facebook* itself proposed setting up of an independent oversight group to review content moderation appeals and adjudicate them.[15] The logic of such intervention, as *Facebook* claims, is to prevent the concentration of too much decision-making within *Facebook* teams and to achieve platform's accountability, oversight and assurance

> *"that decisions are made in the best interest of the online community and not for commercial reasons."*[16]

The oversight group should be a platform's analog to the *US Supreme Court*, with the ability to create case law and to adapt the decision making to local

---

[13] *Facebook* claims to take down more of "bad" content than ever, also proactively (Q3 2018 15,4M). Take down of fake accounts (± 750-800M/Q) – mostly used as spamming accounts (still about 3–4 % of active users are fake accounts). Facebook Newsroom. (2018) *How Are We Doing at Enforcing Our Community Standards?.* [press release] 15 November. Available from: http://newsroom.fb.com/news/2018/11/enforcing-our-community-standards-2/ [Accessed 15 March 2019].

[14] As was publicized widely, there appears to be very limited time dedication of these content moderators as these positions seem to be highly understaffed and underpaid. See: Newton, C. (2019) The secret lives of Facebook moderators in America. *The Verge*, 25 February. [online] Available from: https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona [Accessed 15 March 2019].

[15] Zuckerberg, M. (2018) *A Blueprint for Content Governance and Enforcement.*[press release] 15 November. Available from: https://www.facebook.com/notes/mark-zuckerberg/a-blue print-for-content-governance-and-enforcement/10156443129621634/ [Accessed 15 March 2019].

[16] Ibid.

freedom of speech norms and laws. Still there are multiple unanswered questions regarding the oversight group.[17]

On top of individual abuses of platform design, SMPs have been abused by various more or less organized cyber actors, including state and non--state actors. These abuses are grave and have a potential of influencing democratic processes by polarizing societies, strengthening distrust and shifting political discourse. Some platforms, such as *Facebook*, attempted to address some of these threats. *Facebook* started to work with government and law enforcement agencies (*FBI*, *Department of Homeland Security*, etc.), cybersecurity researchers and other tech companies. It claims to coordinate and exchange real-time updates on emerging threats and disinformation campaigns with agencies and think tanks.[18] Also, *Facebook* launched cross--sectoral elections war rooms, 1st time in September 2018, where subject--matter experts from across the company gather to address potential problems and respond in real time.

The bad actors *Facebook* mentions exploit the platforms' design oriented on pursuing the platforms' business interests, including such features as tendency of sensational news and spam to spread easily (e.g. clickbaits, viral spam, fake news). In recent self-regulatory action, *Facebook* started to change algorithms to mitigate the negative effects of these sensational news and spam.[19] Similarly, *WhatsApp* changed its design to limit the number of people one can forward a message to tackle spreading of fake and dangerous news.[20] The fundamental logic of these actions is to disrupt economic incentives of bad actors on SMPs through design changes of the service. *Facebook* claims that its algorithms will distribute needlessly provocative posts less and less, preventing them from seeing a spike in engagement. Such action is mostly related to the so-called borderline

[17] For instance, it is unclear how the selection of members of the group would go about, how the independence would be secured, what rules the group would follow, or how the group would select the cases from thousands of applicants.

[18] Facebook Newsroom. (2018) *Fighting Election Interference in Real Time.* [press release] 18 October. Available from: https://newsroom.fb.com/news/2018/10/war-room/ [Accessed 15 March 2019].

[19] Zuckerberg, M. (2018) *A Blueprint for Content Governance and Enforcement.* [press release] 15 November. Available from: https://www.facebook.com/notes/mark-zuckerberg/a-blue print-for-content-governance-and-enforcement/10156443129621634/ [Accessed 15 March 2019].

[20] Wagner, K. (2018) WhatsApp will drastically limit forwarding to stop the spread fake news, following violence in India and Myanmar. *Recode*, 19 July. Available from: https://www.recode.net/2018/7/19/17594156/whatsapp-limit-forwarding-fake-news-violence-india-myanmar [Accessed 15 March 2019].

content, which is not necessarily prohibited by the *Facebook* "Community Rules" but are nevertheless abusive, misguiding or otherwise problematic.

Some shortcomings of SMPs are related to information asymmetries; a theory goes that as people do not know who spreads certain news, they cannot evaluate the trustworthiness of the originator of the message. This in turn leads to a situation when people share controversial news without realizing that not all the news originators in the cyberspace are equally trustworthy or openly claim their interests. Providing people with more information on the page owners should therefore increase the probability that some users would double-check the trustworthiness before reposting certain messages. For instance, *Facebook* started to provide additional previously undisclosed information on *Facebook* pages, such as changes to the page name, in order to assess their credibility, genuineness and motives.[21] Similarly, *Facebook* introduced a tool that provided, in some countries, related, fact-checked sources next to disputed ones.[22] Some SMPs also introduced political advertisers verification in order to increase political ads transparency, in the wake of the *US Honest Ads Act*.[23] There is a tendency to strengthen the identity verification of influential actors and accounts.[24]

2.2. NEED FOR OTHER TYPES OF REGULATION

All the self-regulatory efforts mentioned in the previous section are laudable, however, we believe that they do not address the problem properly. First, many of these efforts are self-initiated. Although SMPs have been under public pressure recently, there is hardly a legal basis for *Facebook* to tackle the information asymmetry, or for *WhatsApp* to mitigate the spread of fake news. There is a risk of detriment to the core values of any SMP in the future, which leaves these public fora and public

[21] Cox, J. (2018) Facebook Is Testing a Feature to Tell You If That DM Came from Russia. *VICE*, 10 July. [online] Available from: https://motherboard.vice.com/en_us/article/ne5wgw/facebook-testing-feature-direct-message-from-russia? [Accessed 15 March 2019].

[22] Silverman, C. (2017) Facebook Is Getting Rid Of Its Fact-Checking Label And Replacing It With This. *BuzzFeed News*, 20 December. [online] Available from: https://www.buzzfeednews.com/article/craigsilverman/facebook-is-getting-rid-of-its-fact-checking-label-and#.vq128VVB1 [Accessed 15 March 2019].

[23] Zuckerberg, M. (2018) *Note.* [press release] 6 April. Available from: https://www.facebook.com/zuck/posts/10104784125525891 [Accessed 15 March 2019].

[24] Stewart, E. (2018) Zuckerberg and Facebook are in trouble. Here's what the government might do about it. *Vox*, 10 April. [online] Available from: https://www.vox.com/policy-and-politics/2018/4/10/17208322/facebook-mark-zuckerberg-congress-testimony-regulation [Accessed 15 March 2019].

discourse vulnerable to abuses by the platforms themselves. This brings us to second issue – the platforms' design. Any oversight group would not address the core problem of the platform's design; the community will have to adopt the standards and norms as provided by SMPs, and not originate them. The oversight group would be merely an interpreter of rules, and perhaps a limited creator of norms, in terms of case law. Therefore, the implementation of oversight group would have only limited impact on the core problem of the platforms' design.

3. COMPETITION LAW AS A PANACEA?

Although the self-regulation should not be underestimated, it follows from the above that there should be a regulator separated from the SMPs. Self--regulation may serve as the first layer of regulation, similarly as a supervisory body of a corporation serves as an internal mechanism of control. However, existence of such supervisory body does not mean that there should not be external controllers, such as auditors, tax authorities, competition authorities, etc. Thus, what external regulatory mechanisms relevant for the issues described above can we identify?

3.1. THE THREE REGULATORY MECHANISMS

From among the prospective regulatory mechanisms we discuss three applicable mechanisms on SMPs, all targeting various aspects of the platforms.[25] The first one is the regulation through personal data protection. SMPs own considerable amount of data whereas much of it may fall within the definition of personal data pursuant to Article 4(1) of GDPR.[26] Given the large applicability of GDPR, possibility to impose high fines and pan-European character of the regulation, GDPR is of vital importance for regulation of SMPs. However, GDPR is of no use if a consent of data subjects is given[27], or if data processed by SMPs are no longer personal data. The latter is often the case when big data are at stake, i.e.

---

[25] See, for instance: Kerber, W. (2016) Digital markets, data, and privacy: competition law, consumer law and data protection. *Journal of Intellectual Property Law & Practice,* 11 (11), pp. 856–866; Botta, M. and Wiedemann, K. (2018) EU Competition Law Enforcement vis-à--vis Exploitative Conducts in the Data Economy Exploring the Terra Incognita. *Max Planck Institute for Innovation and Competition Research Paper,* 18-08, p. 23 *et seq.* [online] Available from: https://ssrn.com/abstract=3184119 [Accessed 4 March 2019].

[26] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union* (2016/L-119/1) 4 May.

> *"the collection and processing of large quantities of data through sophisticated methods (e.g. advanced processing through algorithms)."*[28]

The second regulatory mechanism is related to consumer protection, which is part of legal orders of all EU Member States. Consumers are defined as persons who do not act within their professional capacity, hence are more vulnerable in contractual relations. Their lack of professional knowledge is compensated by cogent legal norms which impose duties on businesses as the other parties of contractual relationships.[29] One of the aims of these cogent legal norms is to protect consumers from unfair contractual terms. In certain areas of law, protection from unfair contractual terms is given to non-consumers as well.[30] Although these special areas of law are rarely applicable to the SMPs, consumer protection law falls within the scope of our analysis, since users of SMPs are, as a rule, consumers. If a contractual term causes a severe inequity between a consumer and a business to the detriment of a consumer, such *unfair* contractual term may be invalid even though the consumer has agreed to it.[31] Therefore, such unfair terms may cover undisclosed harvesting of consumer's data, vague use of data, non-user-friendly terms and conditions.[32] Although part of these issues may be solved by personal data protection law, consumer protection may go, at least in theory, further, as it is not limited to acquiring and handling of personal data. However,

---

[27] Article 7 GDPR. To the notion of consent, see, for example: Botta, M. and Wiedemann, K. (2018) EU Competition Law Enforcement vis-vis-à-visà-vis Exploitative Conducts in the Data Economy Exploring the Terra Incognita. *Max Planck Institute for Innovation and Competition Research Paper*. 18-08, p. 23 *et seq*. [online] Available from: https://ssrn.com/abstract=3184119 [Accessed 4 March 2019]; Hintze, M. (2018) Viewing the GDPR through a De-Identification Lens: A Tool for Compliance, Clarification, and Consistency. *International Data Protection Law*, 8 (1), pp. 86–101.

[28] Davilla, M. (2017) Is Big Data a Different Kind of Animal? The Treatment of Big Data Under the EU Competition Rules. *Journal of European Competition Law & Practice*, 8 (6), p. 370. For another definition of big data, see: Stucke, M. E. and Alan, G. P. (2016) *Big Data and Competition Policy*. 1st ed. Oxford: Oxford University Press, p. 15 *et seq*.

[29] This follows, for instance, from Recitals 17, 34, 39 etc. of Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council. *Official Journal of the European Union* (2011/L-304/64) 22 November.

[30] See, for instance, sections 369a *et seq*. of Commercial Code: *Obchodný zákonník 2019*. SI 1991/513. Slovak Republic. In Slovak; Act on Unfair Conditions in Commercial Relations with Food as the Object: *Zákon o neprimeraných podmienkach v obchodných vzťahoch, ktorých predmetom sú potraviny 2013*. SI 2012/369. Slovak Republic. In Slovak.

[31] Section 53 of Civil Code: *Občiansky zákonník 2019*. SI 1964/40. Slovak Republic. In Slovak.

[32] Kerber, W. (2016) Digital markets, data, and privacy: competition law, consumer law and data protection. *Journal of Intellectual Property Law & Practice*, 11 (11), pp. 861–863.

the enforcement mechanism of consumer law seems to be weaker than the enforcement of GDPR.[33]

The last regulatory mechanism which is lively discussed among scholars is competition law. Together with *ex ante* control of mergers, which may prevent creation of too strong undertakings, competition law may tackle abuses of dominant position as well as agreements restricting competition. The supranational enforcement mechanism and the detergence effect of substantial fines which may be imposed by competition authorities make scholars wonder whether this might be the most suitable regulatory mechanisms for SMPs. We will discuss the adequacy of such thoughts in more detail.

3.2. ABUSE OF DOMINANT POSITION OF SMPS

In general, legal theory distinguishes between exclusionary abusive practices and exploitative abusive practices. The former aims to preventing the development of competition by a dominant undertaking, the latter is mainly concerned with charging of unfair prices by a dominant undertaking.[34]

Regarding exclusionary practices, it is questionable whether the position of certain SMPs, mainly *Facebook*, *qua* persons with access to great amount of data, puts them in position of owners of an essential facility.[35] If this was the case, competitors of *Facebook* could ask *Facebook* to give access to its data by arguing that otherwise they would be excluded from competition. However, this would hardly work in practice.[36] Moreover, it would mean that even more persons would have access to data and could use them in similar manner as *Facebook* can. In other words, even if the competition

---

[33] To this end, see, for instance, Patakyová, M. and Mazúr, J. (2018) Facebook – Global Issue without (Existing) Solution? In: Tomas Kliestik (ed.). *Globalization and Its Socio-Economic Consequences 18th International Scientific Conference, Proceedings, (Part V. – Digital Single Market).* Rajecké Teplice, 10–11 October. Žilina: University of Žilina.

[34] Whish, R. and Bailey, D. (2012) *Competition Law.* 7th ed. Oxford University Press, p. 201; Jones, A. and Sufrin, B. (2016) *EU Competition Law. Text, Cases and Materials.* 6th ed. Oxford: Oxford University Press, p. 352.

[35] Botta, M. and Wiedemann, K. (2018) EU Competition Law Enforcement vis-à-vis Exploitative Conducts in the Data Economy Exploring the Terra Incognita. *SSRN Electronic Journal,* p. 46 *et seq*. doi: 10.2139/ssrn.3184119 [Accessed 15 March 2019].

[36] Davilla, M. (2017) Is Big Data a Different Kind of Animal? The Treatment of Big Data Under the EU Competition Rules. *Journal of European Competition Law & Practice,* 8 (6), p. 380. [online] doi: 10.1093/jeclap/lpx039 [Accessed 15 March 2019]; Colangelo, G. and Maggiolino, M. (2018) Data Accumulation and the Privacy-Antitrust Interface: Insights from the Facebook Case for the EU and the U.S. *SSRN Electronic Journal*, p. 43. [online] doi: 10.2139/ssrn.3125490. Available from: https://ssrn.com/abstract=3125490 [Accessed 2 March 2019].

was better off, the privacy concerns would be aggravated.[37] This is certainly not what a regulation should stand for. Arguably, the regulation should aim to control the power currently possessed by certain SMPs, namely *Facebook*, as opposite to spreading the power to virtually all SMPs. Therefore, exploitative practices seem to be better suited for issues related to SMPs.

At the very beginning of any discussion related to exploitative practices it is worth mentioning that competition authorities usually put their hands off this type of abuse, and they have good reasons to do so. Exploitative practices are related to excessive prices for products/services. The idea is that, since an undertaking holds dominant position, it may charge unfair prices for its customers (consumers) and, therefore, exploit them. It is often very difficult to establish the level above which the price for a product/service is excessive, especially when cost-based analysis cannot be used. This is the case for many intellectual property rights, such as copyrights.[38]

In terms of SMPs, the situation with price for their services is even more complex. On the one hand, SMPs provide space for advertisement. Advertisers pay for this service by money. On the other hand, SMPs provide social networking services to their users. In this case, users pay by their attention and data.[39] On the latter market, the idea of abuse lies in SMPs *selling* their social networking services for too high price, i.e. harvesting of too much data[40] or based on unclear terms or processing them for wrong purposes. However, how can one establish that the price charged for social networking services is too high?

3.3. GERMAN FACEBOOK CASE

In March 2016, the German competition authority, *Bundeskartellamt*, initiated proceedings against *Facebook* for potential breach of German

[37] Kerber, W. (2016) Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection. *SSRN Electronic Journal*, p. 861. [online] doi: 10.2139/ssrn.2770479 [Accessed 15 March 2019].

[38] See for instance: Patakyová, M. (2018) How to Assess the Exploitative Practices of Collecting Societies? *European Competition and Regulatory Law Review*, 1 (4), pp. 306–319. [online] doi: 10.21552/core/2017/4/6 [Accessed 15 March 2019].

[39] Kerber, W. (2016) Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection. *SSRN Electronic Journal*, p. 860. [online] doi: 10.2139/ssrn.2770479 [Accessed 15 March 2019]; Newman, J. M. (2015) Antitrust in Zero-Price Markets: Foundations. *University of Pennsylvania Law Review*, 164 (1), pp. 149–206; Langhanke, C. and Schmidt-Kessel, M. (2015) Consumer Data as Consideration. *Journal of European Consumer and Market Law*, 4 (6), pp. 218–223.

[40] Colangelo, G. and Maggiolino, M. (2018) Data Accumulation and the Privacy-Antitrust Interface: Insights from the Facebook case for the EU and the U.S. *SSRN Electronic Journal,* p. 21. [online] Available from: https://ssrn.com/abstract=3125490 [Accessed 2 March 2019].

competition rules.[41] It was clear that *Bundeskartellamt* would connect infringement of data protection law with abuse of dominant position of *Facebook*, however, it was not clear how the authority would like to do that. This puzzle was solved recently, as in February 2019, *Bundeskartellamt* issued decision by which it prohibited *Facebook* from continuing its practice.[42] It was held that

> *"[t]he extent to which Facebook collects, merges and uses data in user accounts constitutes an abuse of a dominant position."*[43]

It was of crucial importance how *Bundeskartellamt* would define the relevant market. Eventually, the product market for social networks was chosen as the relevant one.[44] *Facebook* is thus considered to hold dominant position on this market, as

> *"[s]ervices like Snapchat, YouTube or Twitter, but also professional networks like LinkedIn and Xing only offer parts of the services of a social network and are thus not to be included in the relevant market. However, even if these services were included in the relevant market, the Facebook group with its subsidiaries Instagram and WhatsApp would still achieve very high market shares that would very likely be indicative of a monopolization process."*[45]

Therefore, apart from smaller German social networks, *Facebook* is essentially the only genuine social network, after *Google+* has disappeared from the market. *Facebook* holds market share of more than 90 %.[46] Moreover, the market power of *Facebook* is supported by the access

---

[41] Bundeskartellamt. (2016) *Bundeskartellamt initiates proceeding against Facebook on suspicion of having abused its market power by infringing data protection rules.* [press release] 2 March. Available from: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html [Accessed 9 March 2019].

[42] Bundeskartellamt. (2019) *Bundeskartellamt prohibits Facebook from combining user data from different sources. Background information on the Bundeskartellamt's Facebook proceeding.* [press release] 2 March. Available from: https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf__blob=publicationFile&v=5 [Accessed 9 March 2019].

[43] Ibid.

[44] It flows from the Background information on the *Bundeskartellamt's Facebook* proceeding that *Bundeskartellamt* conducted a substantial qualitative analysis, as it compared the type of service *Facebook* provides with other, similar, yet not identical services, such as *YouTube*.

[45] Bundeskartellamt. (2019) Op. cit.

[46] Bundeskartellamt. (2019) Op. cit.

to competitive relevant data or network effects.[47] The latter leads to high barriers to entry. Although virtually everyone can enter the market by creating their own social network, such new network will be of little use as far as there is not enough people to *network* together. The dominant position of *Facebook* was not threatened by possibility to simultaneous use of several different social networks (multi-homing), which was not proved according to the *Bundeskartellamt*.[48]

After establishment of the dominant position on the relevant market, *Bundeskartellamt* focused on the abusive practice *Facebook* committed. *Facebook's* lucrative advertising model relies on data collected not only on *Facebook*, but also by the use of third-party websites and apps via *Facebook's* embedded tools.[49] Such off-*Facebook* data collection[50] is usually not predicted by *Facebook* users.[51] As off-*Facebook* data are combined with on-*Facebook* data, they may be used for creating very extended profiles of users. It is true that users technically agree with such conditions, however, as there is no other option for them but to agree on terms set by *Facebook* (if they want to use *Facebook* at all), such consent cannot be considered as deliberately given. Taken together with *Facebook* market power, users have little to no choice. Pursuant to *Bundeskartellamt*, such practice is also a violation of personal data regulation and right to informational self-determination.[52]

In order to remedy this situation, the German competition authority did not impose any fine on *Facebook*. Rather, it said that its goal was to change the future behavior of *Facebook* to the benefit of both competitors and consumers. *Bundeskartellamt* considered the case to be too complex and

---

[47] Haucap, J. and Heimeshoff, U. (2013) Google, Facebook, Amazon, eBay: Is the internet driving competition or market monopolization? *DICE Discussion Paper*, (83) p. 3. [online] Available from: http://hdl.handle.net/10419/68229 [Accessed 9 March 2019]; Tucker, C. and Marthews, A. (2012) Social Networks, Advertising, and Antitrust. *George Mason Law Review,* 19 (5), p. 1217 *et seq*.

[48] Bundeskartellamt. (2019) Op. cit.

[49] Ibid.

[50] A similar situation was dealt by the CJEU: Judgment of 29 July 2019, Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV, C-40/17, ECLI:EU:C:2019:629.

[51] Botta, M. and Wiedemann, K. (2018) EU Competition Law Enforcement vis-à-vis Exploitative Conducts in the Data Economy Exploring the Terra Incognita. *Max Planck Institute for Innovation and Competition Research Paper*, 18-08, p. 64. [online] Available from: https://ssrn.com/abstract=3184119 [Accessed 4 March 2019].

[52] From the competition law perspective, the theory of harm for consumers was based on *Facebook* users' loss of control over how their personal data are used. Bundeskartellamt. (2019) Op. cit.

difficult from legal and economic perspective, therefore, at this stage, fine as an additional measure was not imposed.[53]

3.4. HAS AN EFFECTIVE REGULATORY MECHANISM BEEN ESTABLISHED?

The German Facebook case is fresh. As *Facebook* indicated its intention to appeal against the decision[54], we cannot be sure whether the decision will be overruled or not. Nonetheless, if we assumed that the *Bundeskartellamt* decision was upheld, would it mean that we have an effective mechanism for regulation of the SMPs? We remain skeptical as to the effects of such decision.

First, one should not overlook the particularities of German competition law. Even though national competition laws of the Member States converge to competition law of the EU, they are not the same. Particularly, since prosecution of abuse of dominant position is prosecution of a unilateral conduct, national competition law can go further than European competition law.[55] The German legislator detailed the methods of assessing market power in such manner that access to data should be taken into consideration. Therefore, the German legislation is better suited for putting together an infringement of personal data regulation with a breach of competition regulation than the EU legislation.

Second, apart from the wording of legal rules, it is vital to bear in mind that *supra*-competition interpretation of competition rules is on different level in Germany. It is explicitly recognized by *Bundeskartellamt* that the highest German court has ruled that constitutional or other legal principles may be considered in abuse of dominant position cases.[56] When we zoom in on case law of the EU institutions, it is apparent that they have been rather reluctant to broaden competition law analysis by personal data considerations.[57]

---

[53] Ibid.

[54] Dreyfuss, E. (2019) German Regulators Just Outlawed Facebook's Whole Ad Business. *Wired*, 7 February. [online] Available from: https://www.wired.com/story/germany-facebook-antitrust-ruling/ [Accessed 16 February 2019].

[55] See Article 3 para 2 of Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty.

[56] Bundeskartellamt. (2019) Op. cit.

[57] Judgment of 23 November 2006, *Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito, SL v Asociación de Usuarios de Servicios Bancarios (Ausbanc)*, C-235/05, ECLI:EU:C:2006:734, para 63.

Third, even if infringement of data regulation could support competition law case in a similar manner as in Germany, it is doubtful whether competition law may be considered as the effective regulation for SMPs. For instance, GDPR does not have to be violated in each case. If *Facebook* users gave effective consent to harvesting off-*Facebook* data, would it mean that there was no infringement of competition law? If so, this does not reflect the so-called privacy paradox, i.e. the fact that people care about their privacy, but do not act accordingly.[58] Due to very strong network effects, there are no real alternatives to specific platforms for a huge majority of users; the network effects imply high costs of opt-outs, which makes them impractical.[59] Furthermore, there is no product and service life-cycle or amortization, as the platform services are continuous with ongoing upgrades (SaaS). There are also very high entry barriers for any would-be competitors. Finally, the competitive advantage makes it easier for these resource-rich platforms to acquire competition or merge their products or features into their own products and services.[60] Therefore, if *Facebook* collects off-*Facebook* data based on a genuine consent only, it may easily happen that users will give their consent and that *Facebook* will have access to similar amount of data it has nowadays.

Fourth, *Bundeskartellamt's* decision is related to a highly specific situation. After *Facebook* put its data processing practices in line with German law, there will be no more ground for holding *Facebook* conducts accountable. However, as it was described in the first part of this article, issues related to *Facebook* are far more reaching.

Fifth, competition law is definitely not an effective regulatory mechanism when it comes to the speed of its procedure. Due to the plethora of economic and legal issues which need to be solved before a decision is issued, the investigation often takes months, even years.[61] In the meantime, damage caused to users or even to civil society may be significant and unrepairable.[62]

---

[58] Op. cit., p. 26.

[59] Farrell, J. and Klemperer, P. (2006) Coordination and Lock-In: Competition with Switching Costs and Network Effects. *SSRN Electronic Journal.* [online] doi: 10.2139/ssrn.917785 [Accessed 15 March 2019].

[60] For example, see the *Facebook's* acquisition of *Instagram* or *WhatsApp*.

[61] Let us remind that the investigation of *Facebook* in Germany started in March 2016 with decision rendered in February 2019.

[62] Let us assume that elections are at least partially influenced by *Facebook*. Therefore, if off--*Facebook* data collection and creation of users' profiles influenced elections, competition law would come too late to remedy the course of election.

Sixth, what should be the proper remedy once infringement of competition law is recognized? In the *German Facebook case*, behavioral remedies were imposed by *Bundeskartellamt*.[63] However, is such remedy genuinely effective? Who would be able to review whether off-*Facebook* data collection was truly stopped and that there was no technical or legal loop--hole which would allow its continuing? Last but not least, it seems that competition law is somehow forced to serve purposes it was not originally designed for. Although primary objectives of the competition law vary among states,[64] it is overall related to the protection of competition to the benefit of consumers. The position of SMPs, as well as all data giants, goes further than to potential deformation of (economic) competition.

4. CONCLUSION AND DISCUSSION

While platforms prefer to be understood as technology companies, rather than media companies, thus limiting their responsibility over users' content and behavior, they certainly mediate messages and information and clearly hold some responsibility for the intermediation channels they operate. Accountability in private or market sphere is often understood on a transactional basis; one could simply switch the service if one is not satisfied with the quality of product or service, the price or their ratio.[65] But the problem with accountability of SMPs does not lie in poor quality product or service, but rather in (i) negative externalities on communities, such as through election influencing, or facilitation of fake news proliferation, i.e. the service design problem; and (ii) the fact that users may not realize they may be paying too huge a price for the service, in provided personal data or attention, i.e. the price problem, as highlighted also by the recent *German Facebook case*.

---

[63] To the notion of behavioural remedies, see, for instance: Kalesná, K. and Patakyová, M. T. (2018) Behavioral vs. Structural Remedies in European and Slovak Competition Law. In: Humberto Ribeiro, Dora Naletina and Ana Lorga da Silva (eds.). *Economic and Social Development: 35th International Scientific Conference on Economic and Social Development – "Sustainability from an Economic and Social Perspective"*, Lisbon, Portugal, 15–16 November. Croatia: Varazdin Development and Entrepreneurship Agency, pp. 518–526.

[64] Blažo, O. (2017) Účel zákona o ochrane hospodárskej súťaže ako právno-ekonomické interpretačné pravidlo. In: Mária Patakyová (ed.). *Efektívnosť právnej úpravy ochrany hospodárskej súťaže – návrhy de lege ferenda.* Bratislava, Slovakia, 25 September. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, pp. 5–11.

[65] Bovens, M., Schillemans, T. and Goodin, R. E. (2014) Public Accountability. In: Mark Bovens, Robert E. Goodin and Thomas Schillemans (eds.). *The Oxford Handbook of Public Accountability.* Online edition. Oxford University Press.

Public accountability thus becomes more relevant and we argue that currently there is a lack of accountability of SMPs. Public accountability implies proper checks and balances and democratic control of power.[66] Accountability requires answerability (holding one to account), subjection to accountability, agent and principal and the right to require information or justification and a right to sanction if the principal fails.[67] In terms of the first identified problem, i.e. the service design problem, only very limited public accountability may be exerted on platforms, although recent public hearing of *Facebook's* CEO and main shareholder *Mark Zuckerberg* by *US Congress* shows the validity and necessity of such actions.[68] A regulatory regime needs to take into account all of the elements of accountability, not merely an *ad hoc* public inquiry by the legislative branch. As for the second problem, we see how limited the competition authorities can be in addressing the issue fully and in relation to the first issue.

Arguably, in case of SMPs the accountability regimes are not properly set as there is not a clear legal cause of holding platforms accountable for providing infrastructure (inadvertently) tailored to abusive behavior. In this regard, we analyzed the SMPs' self-regulatory efforts and three external regulatory regimes: data protection, consumer protection and competition law. Remedying through data protection and competition law, although the most promising, does not fulfil the requirements for effective and proper regulation of SMPs. This was proved by the *German Facebook case*. The key problem with the regulation of SMPs appears to lie in the fact that none of the regulatory regimes is able to change the SMP's design. The platforms' design is a crucial determinant of the options or *rights* users are granted, channels they use to disseminate various information, or what content is permitted or curated by the platforms.[69] In this sense, the code is the platforms' law, as *Lessig* put it.[70] Although certain platforms claim

---

[66] Han, Y. and Demircioglu, M. A. (2016) Accountability, Politics, and Power. *Global Encyclopedia of Public Administration, Public Policy, and Governance*, pp. 1–8. [online] doi: 10.1007/978-3-319-31816-5_2453-1 [Accessed 15 March 2019].

[67] Murphy, P. et al. (2019) *Public service accountability: rekindling a debate.* Cham, Switzerland: Palgrave Macmillan, p. 7.

[68] At the same time, it showed how limited such action was; many of the inquirers from among representatives possessed limited knowledge of how the platform actually operated or even the gravity of the situation.

[69] Lazer, D. (2015) The rise of the social algorithm. *Science*, 348 (6239), pp. 1090–1091. [online] doi: 10.1126/science.aab1422 [Accessed 15 March 2019].

[70] Lessig, L. (2006) *Code and other laws of cyberspace: version 2.0.* New York: Basic Books.

to seek also complementary objectives (*"Building a global community"* – *Facebook*)[71], the platforms' design is fundamentally driven by the market--oriented ambitions. Yet, if we recognize the importance of SMPs in contemporary society[72], we may reach a conclusion that platforms' design not only makes the processes more difficult, it may in fact contradict them.

As *Lazer et al.* proposed, we need to ask how we can build a news ecosystem and culture that value and promote truth.[73] In doing so we need to review platforms' inner regulations, i.e. the code, algorithms, information filters[74] and other in-built design features that regulate how information flows in the platform cyberspace. It is necessary to independently review biases of algorithms[75], consistency of the content regulation in individual cases, but also improve the information asymmetries the users face and safeguard the integrity of political competition. The oversight needs to be publicly appointed, independent on the platform and accountable to the formal democratic structures.[76] Such actions are warranted by the sheer importance of the platforms for our democracies.

LIST OF REFERENCES

[1] Act on Unfair Conditions in Commercial Relations with Food as the Object: *Zákon o neprimeraných podmienkach v obchodných vzťahoch, ktorých predmetom sú potraviny 2013.* SI 2012/369. Slovak Republic. In Slovak.

[2] Allcott, H. and Gentzkow, M. (2017) Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives*, 31 (2). [online] doi: 10.1257/jep.31.2.211 [Accessed 15 March 2019].

[3] Bartlett, J. (2018) Big data is watching you – and it wants your vote. *The Spectator*, 24 March. [online] Available from: https://www.spectator.co.uk/2018/03/big-data-is-

[71] Zuckerberg, M. (2018) *Building Global Community.* [press release] 16 February. Available from: https://www.facebook.com/notes/mark-zuckerberg/building-global-community/10154544292806634 [Accessed 15 March 2019].

[72] The platforms continue to grow in numbers of their users and they are also increasingly more important for socialization, as a news source, for political deliberation and communication and general marketing: Hitlin, P. and Rainie, L. (2019) *Facebook Algorithms and Personal Data. Pew Research Center: Internet, Science & Tech*, 16 January. [online] Available from: http://www.pewinternet.org/2019/01/16/facebook-algorithms-and-personal-data/ [Accessed 15 March 2019].

[73] Lazer, D. et al. (2018) The science of fake news. *Science*, 359 (6380), pp. 1094–1096. [online] doi: 10.1126/science.aao2998 [Accessed 15 March 2019].

[74] Ibid.

[75] Ibid.

[76] Needless to say, this will be difficult to achieve as most SMPs are global phenomena with dispersed country/region-specific regulators.

watching-you-and-it-wants-your-vote/ [Accessed 15 March 2019].

[4] Blažo, O. (2017) Účel zákona o ochrane hospodárskej súťaže ako právno-ekonomické interpretačné pravidlo. In: Mária Patakyová (ed.). *Efektívnosť právnej úpravy ochrany hospodárskej súťaže – návrhy de lege ferenda.* Bratislava, Slovakia, 25 September. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta.

[5] Botta, M. and Wiedemann, K. (2018) EU Competition Law Enforcement vis-à-vis Exploitative Conducts in the Data Economy Exploring the Terra Incognita. *Max Planck Institute for Innovation and Competition Research Paper.* 18-08. [online] Available from: https://ssrn.com/abstract=3184119 [Accessed 4 March 2019].

[6] Bovens, M., Schillemans, T. and Goodin, R. E. (2014) Public Accountability. In: Mark Bovens, Robert E. Goodin and Thomas Schillemans (eds.). *The Oxford Handbook of Public Accountability.* Online edition. Oxford University Press.

[7] *Brian C. Davison v. Loudon County Board of Supervisors et al.* (2017) 1:16cv932 (JCC/IDD).

[8] Bundeskartellamt. (2016) *Bundeskartellamt initiates proceeding against Facebook on suspicion of having abused its market power by infringing data protection rules.* [press release] 2 March. Available from: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html [Accessed 9 March 2019].

[9] Bundeskartellamt. (2019) *Bundeskartellamt prohibits Facebook from combining user data from different sources. Background information on the Bundeskartellamt's Facebook proceeding.* [press release] 2 March. Available from: https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf?__blob=publicationFile&v=5 [Accessed 9 March 2019].

[10] Calvert, C. (2018) Federal judge rules Trump's Twitter account is a public forum. *The Conversation*, 24 May. [online] Available from: http://theconversation.com/federal-judge-rules-trumps-twitter-account-is-a-public-forum-97159 [Accessed 15 March 2019].

[11] Ceron, A. (2018) *Social Media and Political Accountability Bridging the Gap between Citizens and Politicians.* Cham, Switzerland: Palgrave Macmillan.

[12] Civil Code: *Občiansky zákonník 2019.* SI 1964/40. Slovak Republic. In Slovak.

[13] Colangelo, G. and Maggiolino, M. (2018) Data Accumulation and the Privacy-Antitrust Interface: Insights from the Facebook Case for the EU and the U.S. *SSRN Electronic Journal*. [online] doi: 10.2139/ssrn.3125490. Available from: https://ssrn.com/abstract=3125490 [Accessed 2 March 2019].

[14] Commercial Code: *Obchodný zákonník 2019.* SI 1991/513. Slovak Republic. In Slovak

[15] Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation

of the rules on competition laid down in Articles 81 and 82 of the Treaty.

[16] Cox, J. (2018) Facebook Is Testing a Feature to Tell You If That DM Came from Russia. *VICE*, 10 July. [online] Available from: https://motherboard.vice.com/en_us/article/ne5wgw/facebook-testing-feature-direct-message-from-russia? [Accessed 15 March 2019].

[17] Davilla, M. (2017) Is Big Data a Different Kind of Animal? The Treatment of Big Data Under the EU Competition Rules. *Journal of European Competition Law & Practice*, 8 (6). [online] doi: 10.1093/jeclap/lpx039 [Accessed 15 March 2019].

[18] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council. *Official Journal of the European Union* (2011/L-304/64) 22 November.

[19] Dreyfuss, E. (2019) German Regulators Just Outlawed Facebook's Whole Ad Business. *Wired*, 7 February. [online] Available from: https://www.wired.com/story/germany-facebook-antitrust-ruling/ [Accessed 16 February 2019].

[20] Facebook Newsroom. (2018) *How Are We Doing at Enforcing Our Community Standards?* [press release] 15 November. Available from: http://newsroom.fb.com/news/2018/11/enforcing-our-community-standards-2/ [Accessed 15 March 2019].

[21] Facebook Newsroom (2018) *Fighting Election Interference in Real Time*. [press release] 18 October. Available from: https://newsroom.fb.com/news/2018/10/war-room/ [Accessed 15 March 2019].

[22] Farrell, H. J. and Schneier, B. (2018) Common-Knowledge Attacks on Democracy. *SSRN Electronic Journal*. [online] doi: 10.2139/ssrn.3273111 [Accessed 15 March 2019].

[23] Farrell, J. and Klemperer, P. (2006) Coordination and Lock-In: Competition with Switching Costs and Network Effects. *SSRN Electronic Journal*. [online] doi: 10.2139/ssrn.917785 [Accessed 15 March 2019].

[24] Ferrara, E. (2017) Disinformation and social bot operations in the run up to the 2017 French presidential election. *First Monday*, 22 (8). [online] doi: 10.5210/fm.v22i8.8005 [Accessed 15 March 2019].

[25] Goel, V. et al. (2018) How WhatsApp Leads Mobs to Murder in India. *The New York Times*, 18 July. [online] Available from: http://www.nytimes.com/interactive/2018/07/18/technology/whatsapp-india-killings.html [Accessed March 15 2019].

[26] Guess, A., Nagler, J. and Tucker, J. (2019) Less than you think: Prevalence and predictors of fake news dissemination on Facebook. *Science Advances*, 5 (1). [online] doi: 10.1126/

sciadv.aau4586 [Accessed 15 March 2019].

[27] Han, Y. and Demircioglu, M. A. (2016) Accountability, Politics, and Power. *Global Encyclopedia of Public Administration, Public Policy, and Governance*. [online] doi: 10.1007/978-3-319-31816-5_2453-1 [Accessed 15 March 2019].

[28] Hansen, I. and Lim, D. J. (2018) Doxing democracy: influencing elections via cyber voter interference. *Contemporary Politics*, 25 (2). [online] doi: 10.1080/13569775.2018.1493629 [Accessed 15 March 2019].

[29] Haucap, J. and Heimeshoff, U. (2013) Google, Facebook, Amazon, eBay: Is the internet driving competition or market monopolization? *DICE Discussion Paper*, (83). [online] Available from: http://hdl.handle.net/10419/68229 [Accessed 9 March 2019].

[30] Hintze, M. (2018) Viewing the GDPR through a De-Identification Lens: A Tool for Compliance, Clarification, and Consistency. *International Data Protection Law*, 8 (1).

[31] Hitlin, P. and Rainie, L. (2019) *Facebook Algorithms and Personal Data. Pew Research Center: Internet, Science & Tech*, 16 January. [online] Available from: http://www.pewinternet.org/2019/01/16/facebook-algorithms-and-personal-data/ [Accessed 15 March 2019].

[32] Isaak, J. and Hanna, M. J. (2018) User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*, 51 (8). [online] doi: 10.1109/mc.2018.3191268 [Accessed 15 March 2019].

[33] Jeweler, M. G. (2008) The Communications Decency Act of 1996: Why § 230 is Outdated and Publisher Liability for Defamation Should be Reinstated Against Internet Service Providers. *Pittsburgh Journal of Technology Law and Policy*, 8. [online] doi: 10.5195/tlp.2008.40 [Accessed 15 March 2019].

[34] Jones, A. and Sufrin, B. (2016) *EU Competition Law. Text, Cases and Materials*. 6th ed. Oxford: Oxford University Press.

[35] Judgment of 23 November 2006, *Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito, SL v Asociación de Usuarios de Servicios Bancarios (Ausbanc)*, C-235/05, ECLI:EU:C:2006:734.

[36] Judgment of 29 July 2019, Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV, C-40/17, ECLI:EU:C:2019:629.

[37] Kalesná, K. and Patakyová, M. T. (2018) Behavioral vs. Structural Remedies in European and Slovak Competition Law. In: Humberto Ribeiro, Dora Naletina and Ana Lorga da Silva (eds.). *Economic and Social Development: 35th International Scientific Conference on Economic and Social Development – "Sustainability from an Economic and Social Perspective"*, Lisbon, Portugal, 15–16 November. Croatia: Varazdin Development and

Entrepreneurship Agency.

[38] Kerber, W. (2016) Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection. *SSRN Electronic Journal*. [online] doi: 10.2139/ssrn.2770479 [Accessed 15 March 2019].

[39] Langhanke, C. and Schmidt-Kessel, M. (2015) Consumer Data as Consideration. *Journal of European Consumer and Market Law*, 4 (6).

[40] Lazer, D. (2015) The rise of the social algorithm. *Science*, 348 (6239). [online] doi: 10.1126/science.aab1422 [Accessed 15 March 2019].

[41] Lazer, D. et al. (2018) The science of fake news. *Science*, 359 (6380). [online] doi: 10.1126/science.aao2998 [Accessed 15 March 2019].

[42] Lessig, L. (2006) *Code and other laws of cyberspace: version 2.0.* New York: Basic Books.

[43] Müller, K. and Schwarz, C. (2017) Fanning the Flames of Hate: Social Media and Hate Crime. *SSRN Electronic Journal.* [online] doi: 10.2139/ssrn.3082972 [Accessed 15 March 2019].

[44] Murphy, P. et al. (2019) *Public service accountability: rekindling a debate.* Cham, Switzerland: Palgrave Macmillan.

[45] Newman, J. M. (2015) Antitrust in Zero-Price Markets: Foundations. *University of Pennsylvania Law Review*, 164 (1).

[46] Newton, C. (2019) The secret lives of Facebook moderators in America. *The Verge*, 25 February. [online] Available from: https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona [Accessed 15 March 2019].

[47] Patakyová, M. and Mazúr, J. (2018) Facebook – Global Issue without (Existing) Solution? In: Tomas Kliestik (ed.). *Globalization and Its Socio-Economic Consequences 18th International Scientific Conference, Proceedings, (Part V. – Digital Single Market).* Rajecké Teplice, 10–11 October. Žilina: University of Žilina.

[48] Patakyová, M. T. (2018) How to Assess the Exploitative Practices of Collecting Societies? *European Competition and Regulatory Law Review*, 1 (4). [online] doi: 10.21552/core/2017/4/6 [Accessed 15 March 2019].

[49] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union* (2016/L-119/1) 4 May.

[50] Silverman, C. (2017) Facebook Is Getting Rid Of Its Fact-Checking Label And Replacing It With This. *BuzzFeed News*, 20 December. [online] Available from: https://www.buzzfeed

news.com/article/craigsilverman/facebook-is-getting-rid-of-its-fact-checking-label-and#.vq128VVB1 [Accessed 15 March 2019].

[51] Stewart, E. (2018) Zuckerberg and Facebook are in trouble. Here's what the government might do about it. *Vox*, 10 April. [online] Available from: https://www.vox.com/policy-and-politics/2018/4/10/17208322/facebook-mark-zuckerberg-congress-testimony-regulation [Accessed 15 March 2019].

[52] Stucke, M. E. and Alan, G. P. (2016) *Big Data and Competition Policy.* 1st ed. Oxford: Oxford University Press.

[53] Senate Judiciary Committee. (2017) *Extremist content and Russian disinformation online: Working with tech to find solutions.* [online] Available from: www.judiciary.senate.gov/meetings/extremist-content-and-russian-disinformation-online-working-with-tech-to-find-solutions [Accessed 15 March 2019].

[54] Tucker, C. and Marthews, A. (2012) Social Networks, Advertising, and Antitrust. *George Mason Law Review*, 19 (5).

[55] Tufekci, Z. (2018) How social media took us from Tahrir Square to Donald Trump. *MIT Technology Review*. [online] Available from: http://www.technologyreview.com/s/611806/how-social-media-took-us-from-tahrir-square-to-donald-trump/ [Accessed 15 March 2019].

[56] Wagner, K. (2018) WhatsApp will drastically limit forwarding to stop the spread fake news, following violence in India and Myanmar. *Recode*, 19 July. [online] Available from: https://www.recode.net/2018/7/19/17594156/whatsapp-limit-forwarding-fake-news-violence-india-myanmar [Accessed 15 March 2019].

[57] Whish, R. and Bailey, D. (2012) *Competition Law.* 7th ed. Oxford University Press.

[58] Zuckerberg, M. (2018) *A Blueprint for Content Governance and Enforcement.* [press release] 15 November. [online] Available from: https://www.facebook.com/notes/mark-zuckerberg/a-blueprint-for-content-governance-and-enforcement/10156443129621634/ [Accessed 15 March 2019].

[59] Zuckerberg, M. (2018) *Building Global Community.* [press release] 16 February. Available from: https://www.facebook.com/notes/mark-zuckerberg/building-global-community/10154544292806634 [Accessed 15 March 2019].

[60] Zuckerberg, M. (2018) *Note.* [press release] 6 April. Available from: https://www.facebook.com/zuck/posts/10104784125525891 [Accessed 15 March 2019].

DOI 10.5817/MUJLT2019-2-5

GOFFMAN´S THEORY AS A FRAMEWORK FOR ANALYSIS OF SELF PRESENTATION ON ONLINE SOCIAL NETWORKS[*]

by

LUCIE MERUNKOVÁ[**], JOSEF ŠLERKA[***]

To investigate how people form their identity on social networks and control the impressions they invoke in their audiences, we analyzed personal profiles of 50 university student Facebook users using Erving Gofmann´s dramaturgical theory. We identified five basic forms through which users create and present their identities: The Public diary, The Influencer, The Entertainer, Job and education and Hobby, as well as the appropriate secondary roles performed by users who interact with them.

These findings are corroborated by 8 semi-structured interviews with respondents, which enable a more in-depth exploration of the way they use Facebook, the social interactions they participate in, their motivation for posting contributions, and how they engage in impression management, perceive privacy and resolve issues caused by multiple audiences.

A better understanding of how privacy is conceived and what motivates users to share their personal information online is essential for public authorities' cooperation on shaping company privacy policies and creation of appropriate legal regulations.

The key results confirm the presence of conscious effort to make a desired impression and prove Goffman's theory of face-to-face interactions to be relevant in the context of online social networks.

[*] This work was supported by the European Regional Development Fund-Project *Creativity and Adaptability as Conditions of the Success of Europe in an Interrelated World* (No. CZ.02.1.01/0.0/0.0/16_019/0000734).

[**] merunkova.lucie@seznam.cz, Mgr. Lucie Merunková, New Media Studies, Faculty of Arts, Charles University, Prague, The Czech Republic

[***] josef.slerka@ff.cuni.cz, Mgr. Josef Šlerka, Ph.D., Head of New Media Studies, Faculty of Arts, Charles University, Prague, The Czech Republic

KEY WORDS

Dramaturgical Theory, Erving Goffman, Facebook, Impression Management, Online Identity, Online Self-presentation, Online Social Interactions, Online Social Networks, Social Media

1. INTRODUCTION

The theatre and poetry of masks, their deceit and the reality that they help depict and the roles that they allow us to play have fascinated many great writers from *Shakespeare*, through *Pascal* to *Wilde*.

It was *William Shakespeare* who, four hundred years ago, likened life to the theatre, and *Erving Goffman* (1922–1982), a Canadian sociologist, drew inspiration from his words, being the first academic to use the theatre metaphor to describe and analyse a method of human self-representation in everyday social interactions occurring face-to-face.

In his book *The Presentation of Self in Everyday Life*, published in 1959, he perceives the individual and his behaviour in social situations as an actor performing his role on stage to the public. At the moment when the performance (interaction) ends, he may return behind the scenes where he shakes off his role, relaxes and potentially prepares for the next performance.

Over the last few years, a new stage where social interactions take place and where people play their roles has come into being in the form of online social networks.

The largest worldwide online social network is *Facebook*, founded in 2004, achieving 2.27 billion monthly active users in October 2018.[1] According to *Facebook* statistics, this network has 4.7 million users in the Czech Republic.[2]

Facebook users create personal user profiles where they publish any type of content and also consume and react to the content published by other users, make friends and chat with their friends from both the real and virtual world. Three-quarters of *Facebook* users log in daily, 91 %

---

[1] Facebook. (2018) *Facebook Reports Third Quarter 2018 Results*. [online] MENLO PARK, California: Facebook. Available from: https://investor.fb.com/investor-news/press-release-details/2018/Facebook-Reports-Third-Quarter-2018-Results/default.aspx [Accessed 11 December 2018].

[2] Dočekal, D. (2016) *TIP#650: Kolik má v Česku Facebook uživatelů? Jak je to s věkem? Proč jsou ta čísla tak podivná?* [blog entry] 6 November. Prague: *365tipu*. Available from: https://365tipu.wordpress.com/2016/11/06/tip650-kolik-ma-v-cesku-facebook-uzivatelu-jak-je-to-s-vekem-proc-jsou-ta-cisla-tak-podivna/ [Accessed 20 January 2019].

of teenagers at least sometimes using a mobile phone. The same percentage of teenagers goes online every day, which is an indication of the importance of cyberspace in their lives.[3]

The amount of data uploaded every day is immeasurable, bringing new opportunities for *Facebook* to monetize it and new challenges for users to protect their privacy. Although the collection and use of personal information are usually included in the terms of service, it might not be in accordance with users' expectations or even legal rights to privacy. Understanding how privacy is conceived among users and refining its definitions in the context of online social networks is necessary for policymaking and choosing the right legal approach to tackle privacy threats.

It is *Goffman's* theory of self-representation and social interaction that many academics follow up on in their studies of social networks. For instance, during research of identity creation, self-representation and content curation,[4] privacy,[5] during analysis of social interactions on the social networks and work with the audience[6] or when examining the technological limitations and affordances that computer-mediated communication involves.[7] The correlation between method of *Facebook* use

---

[3] Greenwood, S., Perrin, A. and Duggan, M. (2016) *Social Media Update*. [online] Washington: Pew Internet & American Life Project. Available from: http://www.pewinternet.org/2016/11/11/social-media-update-2016/ [Accessed 17 April 2018]; Lenhart, A. (2015) *Teens, Social Media & Technology Overview 2015*. [online] Washington: Pew Internet & American Life Project. Available from: http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/ [Accessed 8 June 2017].

[4] Zhao, S. (2005) The Digital Self: Through the Looking Glass of Telecopresent Others. *Symbolic Interaction*, 28 (3), pp. 387–405. [online] Available from: http://doi.wiley.com/10.1525/si.2005.28.3.387 [Accessed 27 October 2018]; Hogan, B. (2010) The Presentation of Self in the Age of Social Media: Distinguishing Performances and Exhibitions Online. *Bulletin of Science, Technology & Society*, 30 (6), pp. 377–386. [online] Available from: http://bst.sagepub.com/cgi/doi/10.1177/0270467610385893 [Accessed 11 October 2017]; Zhao, X. et al. (2013) The many faces of facebook. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems – CHI '13*, Paris, 27 April – 2 May. New York, USA: ACM Press, pp. 1–10. [online] Available from: http://dl.acm.org/citation.cfm?doid=2470654.2470656 [Accessed 18 January 2018]; Pospíšilová, M. (2016) *Facebooková (ne)závislost: identita, interakce a uživatelská kariéra na Facebooku*. Praha: Univerzita Karlova, nakladatelství Karolinum.

[5] Hewitt, A. and Forte, A. (2006) Crossing boundaries: Identity management and student/faculty relationships on the Facebook. In: *Proc 2006 CSCW*, Canada, 4–8 November. [online] Available from: http://andreaforte.net/HewittForteCSCWPoster2006.pdf [Accessed 7 March 2018]; Lewis, K. et al. (2008) The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network. *Journal of Computer-Mediated Communication*, 14 (1), pp. 79–100. [online] Available from: http://doi.wiley.com/10.1111/j.1083-6101.2008.01432.x [Accessed 26 April 2018].

[6] boyd, d. (2007) Why Youth (Heart) Social Network Sites: The Role of Networked Public in Teenage Social Life. In: David Buckingham (ed.). *MacArthur Foundation Series on Digital Learning – Youth, Identity, and Digital Media Volume*. Cambridge, MA: MIT Press.

and the user's personality is reflected for instance by *Gosling et al.*[8] or *Michikyan et al.*[9], and the effect of the use of *Facebook* on psychological well-being by *Lin*[10] and *Chou*[11].

Goffman's theory of self-representation has become the basis for a wider understanding of user behaviour and motivation known as impression management. Resulting studies show that even in the course of user activity outside their personal profile, such as "liking" a certain page, users are aware that their activity is part of the image they build of themselves.[12]

Public self-presentation and a certain level of self-disclosure are necessary to create an online identity. The degree of self-disclosure and the content shared by users depend on their goals, motivations and their audience as well as on their privacy concerns, the perceived value of personal information and the value of the service they receive in return.

Privacy is considered to be a protected human right by the *United Nations General Assembly* and its protection is ensured by many international regulations or guidelines (e.g. OCDS's *Recommendation on Cross-border Co--operation in the Enforcement of Laws Protecting Privacy* and *General Data Protection Regulation*) or in countries' constitutions.

Most social networks provide the user with the option to limit who sees the published content, but most of the users keep the default privacy

---

[7] Miller, H. (2016) *Investigating the Potential for Miscommunication Using Emoji*. [blog entry] 5 April. GroupLens. Available from: https://grouplens.org/blog/investigating-the-potential-for-miscommunication-using-emoji/ [Accessed 26 January 2019]; Walther, J. B. a D'addario, K. P. (2001) The Impacts of Emoticons on Message Interpretation in Computer-Mediated Communication. *Social Science Computer Review*, 19 (3), pp. 324–347. [online] Available from: http://ssc.sagepub.com/cgi/doi/10.1177/089443930101900307 [Accessed 21 May 2017]; Eisenlauer, V. (2014) Facebook as a third author – (Semi-)automated participation framework in Social Network Sites. *Journal of Pragmatics*, 72, pp. 73–85. [online] Available from: http://linkinghub.elsevier.com/retrieve/pii/S037821661400037X [Accessed 21 May 2017].

[8] Gosling, S. D. et al. (2011) Manifestations of Personality in Online Social Networks: Self--Reported Facebook-Related Behaviors and Observable Profile Information. *Cyberpsychology, Behavior, and Social Networking*, 14 (9). [online] Available from: http://www.liebertonline.com/doi/abs/10.1089/cyber.2010.0087 [Accessed 21 May 2017].

[9] Michikyan, M. et al. (2014) Can you tell who I am? Neuroticism, extraversion, and online self-presentation among young adults. *Computers in Human Behavior*, 33. [online] Available from: http://linkinghub.elsevier.com/retrieve/pii/S0747563214000156 [Accessed 21 May 2017].

[10] Lin, R. and Utz, S. (2015) The emotional responses of browsing Facebook: Happiness, envy, and the role of tie strength. *Computers in Human Behavior*, 52. [online] Available from: http://linkinghub.elsevier.com/retrieve/pii/S074756321500360X [Accessed 21 May 2017].

[11] Chou, H. G. and Edge, N. (2012) "They Are Happier and Having Better Lives than I Am": The Impact of Using Facebook on Perceptions of Others' Lives. *Cyberpsychology, Behavior, and Social Networking*, 15 (2). [online] Available from: http://online.liebertpub.com/doi/abs/10.1089/cyber.2011.0324 [Accessed 21 May 2017].

[12] Wallace, E., Buil, I., de Chernatony, L. and Hogan, M. (2014) Who " likes" You… and why? A Typology of Facebook Fans from "Fan" –atics and Self Expressives to Utilitarians and Authentics". *Journal of Advertising Research*, 54 (1), pp. 92–109.

settings untouched.[13] On top of that, the results of a study done by *Suh and Hargittai*[14] showed that the actual audience of two-thirds of posts users publish on *Facebook* is different than initially intended. The posts are thus usually visible to either bigger of smaller audience than planned.

The users' inability or reluctance to manage complex privacy settings as well as SNS' architecture inducing self-disclosure leads to users' data being exposed to corporations, employers, law enforcement authorities or governments, without the users realizing the value of their data and the possible harmful consequences of not keeping it private. The information may also be used for various attacks, including cyber bullying, identity theft, phishing, etc.

With the understanding of users' perception of private and public on online social networks, the process of selecting content for sharing and the challenges of segregating an audiences, the public authorities can more easily pressure on modification of social norms concerning privacy protections, come up with effective regulations for data collection and enforce compliance with it, improve online privacy literacy or for instance insist on changing the user interface to make it more usable and understandable.

The aim of our qualitative research was to analyse and describe methods of self-representation and the dynamics of social interaction on *Facebook* from the perspective of *Goffman's* dramaturgical approach. Due to its appropriate methodology and relevant findings, we chose to reproduce the research of *Jamie R. Riccio* from *Syracuse University*, which she presented in her thesis *All The Web's a Stage: The Dramaturgy of Young Adult Social Media Use*.[15]

Reproduction of the research allowed us to verify whether preceding research findings still apply, to investigate what influence a research sample with different demographic characteristics has on the results of the study and to record any potential differences discovered.

---

[13] Suh, J. J. and Hargittai, E. (2015) Privacy Management on Facebook: Do Device Type and Location of Posting Matter? *Social Media + Society*, 1 (2). [online] Available from: http://journals.sagepub.com/doi/10.1177/2056305115612783 [Accessed 21 May 2017].

[14] Ibid.

[15] Riccio, J. R. (2013) *All The Web's a Stage: The Dramaturgy of Young Adult Social Media Use*. Syracuse: Syracuse University, Theses – ALL. Paper 16. Magisterská práce (MA) Syracuse University. [online] Available from: http://surface.syr.edu/cgi/viewcontent.cgi?article=1007&context=thesis [Accessed 5 May 2017].

Through content analysis of user posts, we determined several basic ways in which users create and present their online identity and in semi--structured interviews with selected respondents, we focused closely on conscious impression management, perception of the front and back regions on *Facebook* and how users work with their audience.

2. THE ROLE OF ONLINE SOCIAL NETWORKS IN THE SOCIAL LIFE OF YOUNG PEOPLE

Certain situations occur in the lives of young people which their parents' generation would see as petty considerations that bear very little relation to real life. A *Facebook* friend has unfriended them. Colleagues have posted photos from a party that a given person was not invited to. Someone made rude comments on someone's photo etc.

Cyberspace has become an alternative world where people create and administer their online identity, make friends and maintain relationships using text, visual and audiovisual elements. It is a place,

> *"[…] in which people still meet face-to-face, but under new definitions of both "meet" and "face"."*[16]

Unlike the older generations, interactions in the environment of non--anonymous online networks are an important part of the identity and social life of today´s children and young adults. Even to such an extent that limited access to the Internet can lead to social exclusion.[17]

The skills that individuals require in online space to correctly interpret situations, to create an acceptable online identity and to be able to control the impression that their behaviour makes are different from those that they need to achieve the same goals in the real world.[18] More than in the real world, people are dependent primarily on the ability to formulate their thoughts verbally and to decode meanings and connotations from the written word, despite the fact that communication technologies make allowance for non-verbal manifestations in mediated communication and

---

[16] Stone, A. R. (1991) Will the Real Body Please Stand Up? Boundary Stories About Virtual Cultures. In: Michael Benedikt (ed.). *Cyberspace: First Steps*. Cambridge, MA: MIT Press, p. 85.

[17] Dijck, J. (2013) *The culture of connectivity: A critical history of social media*. New York: Oxford University Press, p. 51.

[18] boyd, d. (2007) Why Youth (Heart) Social Network Sites: The Role of Networked Public in Teenage Social Life.' In: David Buckingham (ed.). *MacArthur Foundation Series on Digital Learning – Youth, Identity, and Digital Media Volume*. Cambridge, MA: MIT Press, p. 12.

attempts partially to substitute it with audiovisual elements such as emoticons, emojis, photographs, gifs or videos.

One of the most notable differences from the real world is the existence of a diffuse audience composed of a broad variety of individuals and groups that not necessarily meet in time or space, and missing context which under normal circumstances provides meaning to words and events. Together with the absence of non-verbal manifestations and uncertainty in determining what is and what is not the intention, it is therefore more difficult to define a situation and the meaning of words, actions or manifestations and it is also more difficult to present one's identity in such a way as to be appropriate for all individuals who might become the audience of the user's performance.[19]

3. CENTRAL CONCEPTS OF ERVING GOFFMAN'S DRAMATURGICAL SOCIOLOGY

On the basis of extensive observation, in his book *The Presentation of Self in Everyday Life* (1959) *Goffman* concludes that an individual entering an interaction with others always tries to control the image they draw in their mind about that individual and the impressions the individual makes upon them. Such an effort to maintain control manifests itself in conscious alteration of the *façade* that the author defines as

> *"[…] expressive equipment of a standard kind intentionally or unwittingly employed by the individual during his performance."*[20]

The *façade* (social front) comprises two parts – of the stage (setting) [e.g. furniture or decorations at home], which serve as the stage for all social interaction, and the personal *façade* (personal front) which may be divided into the individual's appearance –

[19] Aspling, F. (2011) *The Private and the Public in Online Presentations of the Self: A Critical Development of Goffman´s Dramaturgical Perspective*. MA. Stockholm University; Marwick, A. E. and boyd, d. (2011) I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, 13 (1), pp. 114–133. [online] Available from: http://journals.sagepub.com/doi/10.1177/1461444810365313 [Accessed 10 December 2018]; Abercrombie, N. and Longhurst, B. (1998) *Audiences: A sociological theory of performance and imagination*. Thousand Oaks, California: Sage.

[20] Goffman, E. (1959) *The Presentation of Self in Everyday Life*. Garden City, N.Y.: Doubleday, p. 13.

> *"[…] those stimuli which function at the time to tell us of the performer's social statuses"*[21] (e.g. clothes, make-up…),

and manner –

> *"[…] those stimuli which function at the time to warn us of the interaction role the performer will expect to play in the on-coming situation."*[22] (behaviour, method of speaking, gesticulations…).

Generally, users modify these elements so that they correspond to the expectations of the anticipated audience (provided the participant knows his audience), to the stage, the role and the goal that the participant wishes to achieve. The audience normatively expects the separate parts of the *façade* to be aligned.[23]

Despite the fact that *Goffman* originally related his theory only to situations where people meet face-to-face, in our opinion his theory is also applicable to the environment of the social networks, in spite of certain limitations. All of the above-mentioned elements appear in the online environment too – the stage on *Facebook* is represented by the user interface, which is usually the user's profile. The personal *façade* consists of a profile picture and the manner in which the user communicates and the content he or she shares.

To fulfill the expectations of the audience and the social norms to gain positive feedback, the participating individual tries to present their "idealised" self and present themselves in the best possible light. Therefore they exaggerate certain aspects of their personality while suppressing or completely hiding the negative ones. This way the participant presents him or herself in a certain role and controls the impression he or she makes, thereby also influencing the opinion of him or her formed in the minds of the audience. *Goffman* calls this strategy impression management.[24]

---

[21] Goffman, E. (1959) Op. cit., p. 15.
[22] Ibid.
[23] Goffman, E. (1959) Op. cit., pp. 15–16.
[24] Goffman, E. (1959) Op. cit., pp. 23–44.

According to *Goffman*:

"The expressiveness of the individual (and therefore his capacity to give impressions) appears to involve two radically different kinds of sign activity: the expression that he gives, and the expression that he gives off."[25]

1. expressions given – verbal symbols that we use to transmit information and when trying to make a certain impression;
2. expressions given off – non-verbal involuntary features such as tone of voice, facial expression, gestures, proxemics...[26]

However, as *Goffman* also points out:

"The individual does intentionally convey misinformation by means of both of these types of communication, the first involving deceit, the second feigning."[27]

In *Goffman's* theory, performances by specific individuals (actors) take place invariably on a stage comprising two main regions – the front (frontstage) and the back (backstage). The front region is where the performance itself takes place. Here the individual plays a certain role (defined by appearance, the stage and the manner of performance) for the audience and strives to provoke a certain impression. The back region is the space where the individual may behave naturally and where he commonly switches over to more informal behaviour and speech, sometimes even contradicting their carefully delivered performance of just moments before.[28] It is therefore important for access to the back region to be restricted and for behind-the-scenes behaviour not to be seen by anybody else but by members of the team participating in the performance.

Regions may also be found in the environment of an online network. Some studies present online social networks where the user has control over access to the content he publishes, primarily as private space and therefore back region.[29] However, we believe that also on online social networks the user plays a role for his audience and therefore this space comprises

[25] Goffman, E. (1959) Op. cit., p. 2.
[26] Ibid.
[27] Ibid.
[28] Goffman, E. (1959) Op. cit., pp. 66–86.

both the front and back region. Another of the aims of this study is also to establish whether the regions are fixed or they shift, and how much user behaviour differs according to the region and the perceived privacy.

4. HOW DO USERS CREATE AND PERFORM THEIR OWN IDENTITY?

4.1. ONLINE SOCIAL NETWORK SITES

Methods for creation and performance of identity are partially determined by the user interface and the functional elements of online social networks.

One of the most cited definitions of an online social network comes from an article by *boyd and Ellison* and says that social network sites are

> *"web-based services that allow individuals to (1) construct a public or semi--public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system."*[30]

In her further works, *dannah boyd* presents four more properties that differentiate the environment of an online social network and interactions and communication taking place online from the real world. These properties are:

1. *persistence* – unlike unmediated communication, network communication is archived for long periods;
2. *searchability* – thanks to the fact that both the content and identity of individuals is recorded in text, individual people can be searched in online social networks;
3. *replicability* – posts and any data may be copied from one place and used in another so that you cannot tell the copy apart from the original;

---

[29] boyd, d. (2006) Friends, friendster and MySpace top 8: Writing community into being on social network sites. *First Monday*, 11 (12). [online] Available from: http://firstmonday.org/issues/issue11_12/boyd/index.html [Accessed 20 January 2019]; Lewis, K., Kaufman, J. and Christakis, N. (2008) The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication*, 14 (1), pp. 79–100. [online] Available from: https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1083-6101.200801432.x [Accessed 12 March 2017].

[30] boyd, d., and Ellison, N.B. (2007) Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13 (1), p. 211. [online] Available from: http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html [Accessed 7 March 2017].

4. *invisible audiences* – due to the three characteristics above, it is impossible to determine exactly who may come into contact with communication or content created on online social networks.[31]

4.1.1. DESCRIPTION OF BASIC ELEMENTS AND FUNCTIONS OF FACEBOOK

The mainstay of the *Facebook* are personal, non-anonymous profiles – partially personalisable pages presenting the user via name, profile photo and basic information concerning age, sex and typically a space for a narrative that the user may use to describe himself.

User profiles serve as a type of notice board where the user publishes his content – statuses, photos, videos or where they can share other users' content. These data are then visible for other users via their news feed (main page on *Facebook* where new posts are ordered either chronologically or according to relevance) or they can view them on the user profile in question.

Separate user profiles are connected by two-way bonds that manifest themselves in the form of users' "friends" or by a one-way bond when a user follows another user, typically a celebrity or influencer.

The fundamental, static presentation element which, if we use *Goffman's* term, serves partially as a stage and partially as a *façade* is, therefore, the user profile. Here the user creates his own identity by means of:

1. a profile photo which accompanies all and any of his activities on the social network;
2. a cover photo that the user may use to add context to his identity;
3. the "About" tab – the textual part of the profile where the user completes information about himself, such as date of birth, education, employment, etc.;
4. a list of friends – in other words, a public illustration of social links;
5. a list of favourite films, books, videos, music, etc. which demonstrates his tastes and interests;

[31] boyd, d. (2007) Why Youth (Heart) Social Network Sites: The Role of Networked Public in Teenage Social Life.' In: David Buckingham (ed.). *MacArthur Foundation Series on Digital Learning – Youth, Identity, and Digital Media Volume*. Cambridge, MA: MIT Press.

6. a list of pages that the user has "Liked", by which he shows either his interest in their content or this serves to present the user's tastes and opinions;
7. a list of groups of which he is a member – this shows his interests, activities, etc.

In addition to these static elements of the profile, which are more presentational than interactive in nature, the user creates his identity and performs primarily by publishing and sharing text, visual or audiovisual content on his profile. As well as the participant, his *Facebook* friends participate in this activity too, reacting to his published content with Likes and comments.

5. RESEARCH

5.1. RESEARCH QUESTIONS

The aim of the research is to describe user behaviour on *Facebook* from a perspective of *Goffman's* dramaturgical theory. In order to define our topics of interest more precisely, we set several research questions:

1. What methods do *Facebook* users employ to create and present their identity?;
2. Do *Facebook* users proceed with an awareness of what impression they leave on their audience?;
3. Where in the users' opinion do the front and back region lie on *Facebook*, and does user behaviour differ in the separate regions?

5.2. METHOD AND PROCEDURE

The methodology for our research is based on research by *Jamie R. Riccio* conducted as part of her thesis entitled *All the Web´s a Stage – The Dramaturgy of Young Adult Social Media Use*[32], which we have partially modified to make it more suitable for the needs of our research. The method for acquiring respondents and also their demographic characteristics are both different and we have also decided not to focus on *Twitter*, but investigate *Facebook* primarily, as the most used social network in the Czech

[32] Riccio, J. R. (2013) *All The Web's a Stage: The Dramaturgy of Young Adult Social Media Use*. Syracuse: Syracuse University, Theses – ALL. Paper 16. Magisterská práce (MA) Syracuse University. [online] Available from: http://surface.syr.edu/cgi/viewcontent.cgi?article=1007&context=thesis [Accessed 5 May 2017].

Republic. The second part of the study is composed of semi-structured interviews.

Our research builds on the grounded theory method and comprises two parts. The first part is a qualitative content analysis of *Facebook* posts which provides data on the methods used by users to perform their own identity and what role they play.

After initial contact and gaining their consent, the posts of 50 respondents published on their personal *Facebook* profiles over the course of one month were subjected to qualitative analysis. By scrutinising the content and both apparent and underlying meaning of the posts it was possible to determine several predominant themes and methods of identity presentation. A total of 733 posts were gathered and coded. *Goffman's* terminology was used for analysis of the secondary roles played by those commenting on the posts.

The second part of the study are semi-structured interviews with eight selected respondents which reflect the findings from the first part and allow for a more detailed examination of the functioning of the fundamental elements of *Goffman's* theory on the social networks, such as impression management and the regions.

5.3. PARTICIPANTS

50 respondents were selected for the purposes of this study, 25 women, 25 men, between 23–29 years of age, university graduates or current university students. The respondents were chosen from among the researchers' *Facebook* friends, which facilitated better analysis of the real meaning of posts due to knowledge of the context. All respondents are of European origin and live in the Czech Republic, predominantly living in Prague.

The main difference to the research being reproduced is the selection of respondents of higher age and education (*Jamie R. Riccio* focused especially on young adults between 18–22 years of age) and of course European as opposed to American origin.

5.4. RESULTS

The respondents' published *Facebook* posts were first written down in the form of a table with a description of the content and format, as well as the number and form of reactions. The thematic category of the method

of identity presentation was determined and the topic of the post described in more detail on the basis of the content.

#	Format	Content	Coding	Topic	Likes	Shares	Comments	Type of Comments	Number of Interactions
post 1	status	cynically joking text status about non-functioning technologies (e-mail, internet, slack)	public diary	personal experience	2	0	2	joking	**4**
post 2	article	a broadcast from Chamber of Deputies regarding frauds of Czech prime minister	current events	politics	1	0	0	0	**1**
post 3	video	music video	culture	music	3	0	2	supporting	**5**
post 4	photography	photography of old textbooks from high school	public diary	personal memory	9	0	6	joking	**15**
post 5	article	infographics concerning presidential candidates	current events	politics	1	0	3	expressing opinion	**4**
post 6	video	funny video	entertainment	humor	0	0	0	0	**0**
post 7	article	an article with expert´s opinions of current marketing campaigns	job	marketing	0	0	3	criticizing	**3**

Table 1: Example of coding of content

Recurring themes soon appeared in the course of coding the posts. Ordered according to frequency, the themes were:

- Information and photos relating to the user – personal experiences, successes, feelings, opinions, photos from their travels, etc.;
- Entertaining content – humorous stories, observations or content such as comics, pictures, videos, etc.;
- (Pop)cultural content – music videos, film trailers, invitations to exhibitions, concerts, theatre reviews, etc.;
- Content concerning users' job or hobby;
- Content concerning current affairs – comments, articles, satire, etc.;
- Interesting content – various formats of posts presenting what the user is interested in and what they think is important or beneficial for others;
- Content concerning university study.

We have decided to name the categories of identity presentation and the primary roles of the participants resulting from the content analysis thus: *The Public diary*, *The Influencer*, *The Entertainer*, *Job and education* and *Hobby* (ordered according to user usage frequency). It should be emphasised again that user presentation is generally composed of various methods and more than one thematic category.

Topic of posts		**Prevalent topics**		**Ways of creating and presenting personal identity**	
Topic	**Number of posts**	**Topic**	**Number of posts**	**Way of self--presentation**	**Number of posts**
Current events	**47**	Public diary (A)	269	The Public diary (A)	269
Hobby	**39**	Entertainment (B)	147	The Influencer (C, F, G)	182
Hobby/Job	9	Culture (C)	93	The Entertainer (B)	147
Hobby/Public diary	5	Job (D)	73		
Culture	**93**	Hobby (E)	53	Job and education (D, H)	82
Job	71	Current events (F)	47		
Job/Public diary	2	Interesting stuff (G)	42	Hobby (E)	53
Public diary	**269**	Education (H)	9		
Education	9				
Entertainment	**147**			**Total number of posts**	**733**
Interesting stuff	**42**				

Table 2: Topic representation in the self-presentation on Facebook

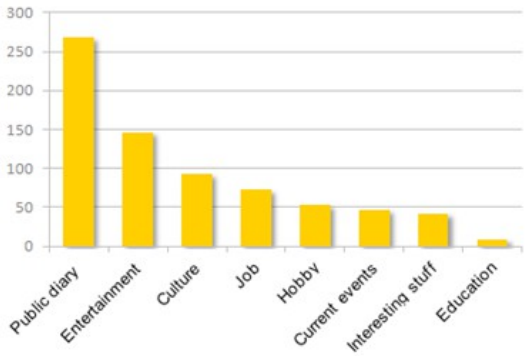


Figure 1: Themes of posts analysed

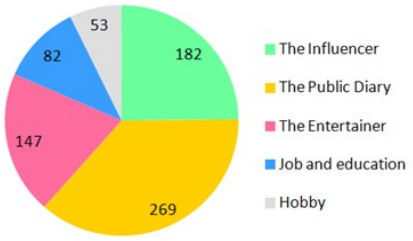


Figure 2: Methods of identity creation and presentation

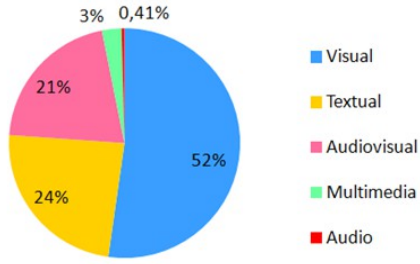


Figure 3: Formats of analyzed posts

5.4.1. DIFFERENCES IN FINDINGS

Jamie R. Riccio determined four methods of identity presentation and five roles that users play for their audience, thereby answering the question of how users present their identity on *Facebook* and which version of self they present there.

We decided to merge methods and roles into one category and to describe the methods used by the users to create and present their identity online. Certain findings of the reproduced research proved possible to confirm, while others did not feature in our findings.

Jamie R. Riccio's Findings		**Our Findings**
Methods for performing identity	**Primary performer roles**	**Ways of creating and performing identity**
~~Association with Influential Others~~	~~The Healthy Lifestyler~~	The Public diary
Emphasis on Career	The Local Celebrity	The Influencer
Highlighting a Hobby	The Pop Culture Maven	The Entertainer
The "Public Diary" Effect	~~The Sports Insider~~	Job and education
	~~The Girls' Girl (or Not)~~	Hobby

Table 3: The comparison of discovered patterns

According to *Riccio*, one of the main methods of identity presentation was linking oneself to public figures, celebrities, important members of the community, but also personal partners or brands, by means of Liking a relevant page or sharing its content. This method did not feature in our study sample, partially because the lists of Likes for pages, public figures, films, etc. are no longer such a visible component of the personal profile as they used to be and therefore do not function as a component to identity presentation. On the other hand we managed to confirm the enduring

existence of the methods *Emphasis on Career*, *Highlighting a Hobby* and *The "Public Diary" Effect.*

As for the roles that the users play, three of the five roles defined by *Riccio* did not appear in our respondent sample: *The Healthy Lifestyler*, *The Sports Insider* and *The Girls' Girl (or Not)*. The reason for this may be the existence of certain trends at certain times in certain places (healthy lifestyle in America) or the higher age and level of education of our respondents who might be less prone to succumb to mass trends and presentation by using them. The role *The Girls' Girl (or Not)*, which is characterised by

> *"messages of female friendship and sisterhood, but punctuated by public displays of relational aggression"*

is a phenomenon arising particularly amongst girls of adolescent age,[33] and therefore it is not surprising that it did not emerge amongst respondents of university graduate status.

We categorised the *Local Celebrity* role under *The Public Diary* because they differ from each other only in the higher frequency of publishing posts. The role of *The Pop Culture Maven* has become a component of the identity presentation method that we call *The Influencer*.

We subject the separate identity presentation methods to the more detailed analysis below.

[33] Steinberg, L. (2008) *Adolescence*. 8th ed. New York: McGraw-Hill.

5.4.2. THE PUBLIC DIARY

Picture 1: The Public Diary

The most frequently used method of identity creation and performance was using *Facebook* as a public diary. This manifested itself in the user publishing posts about himself on his profile page – what he does and experiences, funny things that happened to him, what achievements he has made, his thoughts, observations and opinions, photos of himself with friends or his partner, photos from journeys abroad, pictures of pets etc.

Users obviously see *Facebook* as a self-representation platform, a place where they can attract the attention of others in them and in their lives. However, they do this in a well-thought-out form and attempt to create content in such a way as not to make it look like they are "seeking attention" (which for instance posting a daily selfie would look like), but rather to bring a certain value to other users too – either by the funniness, interestingness or importance of the content. Along with posts thematically relating to the user's job, "Public Diary" type posts would receive the most reactions (Likes and comments) from the user's friends.

5.4.3. THE INFLUENCER

The second most frequent method of identity creation and presentation was the method we have called *the Influencer*. This typically means the sharing of others' posts, articles, photos, videos, etc. The poster, therefore, shares in creating the range of posts that appear in his friends' *News Feed*, but rather than attracting attention to himself, he shares content that he considers for whatever reason to be of value for other users, in most cases adding his own opinion to the post. In this way he presents his interests and opinion in an unforced manner.

Picture 2: The Influencer

In the case of the research respondents, this most often concerned cultural themes – music videos, movie trailers or humorous GIFs and memes containing pop--cultural references. In accordance with his desire to conform,[34] the user makes it clear to other users that he consumes the same cultural content as they do and therefore can engage in conversation and share his experiences, feelings and opinions on topics that interest them too.[35]

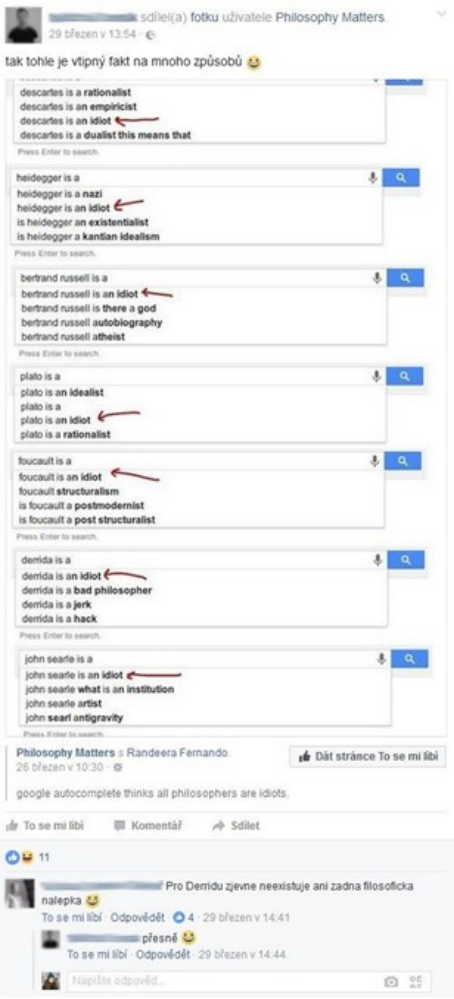
The second most frequent were posts concerning current affairs, especially domestic politics and foreign policy and social themes such as racism or the refugee crisis, primarily in the form of shared articles with the poster's comment. Posts falling in the category of "current affairs" and

[34] Macek, J. (2013) More than a desire for text: Online participation and the social curation of content. *Convergence: The International Journal of Research into New Media Technologies*, 19 (3). [online] Available from: http://con.sagepub.com/cgi/doi/10.1177/1354856513486530 [Accessed 15 January 2019].

[35] Studýnková, N. (2010) *Konzumace pirátských kopií televizních seriálových narací*. Bakalářská práce. Masarykova univerzita, Fakulta sociálních studií. Vedoucí práce Jakub Macek. Available from: http://con.sagepub.com/cgi/doi/10.1177/1354856513486530 [Accessed 28 December 2018].

"culture" generated the highest proportion of comments of all topics and categories.

5.4.4. THE ENTERTAINER



Picture 3: The Entertainer

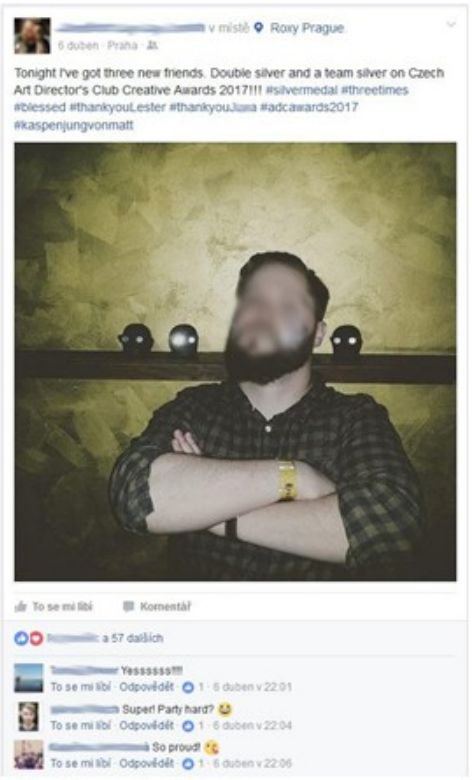
The attempt to entertain was one of the major motivations in all of the categories mentioned. Regardless of whether this concerned personal posts, comments on political affairs or on users' own hobby, users tried to do it in an entertaining and humorous form and their reward was feedback in the form of Likes and comments.

For some, the aim to entertain was in the very first place, and so on their profiles they shared funny cartoons, satirical memes, funny videos, humorous observations on life, screenshots of entertaining or absurd things, the results of various *Facebook* quizzes, etc. The content of the shared posts was varied, but regularly included political topics, current affairs, pop-culture references, references to the user's hobby, field of employment or study, or pets. Funny posts were often also compounded by reactions of friends who continued joking in their comments.

5.4.5. JOB AND SCHOOL

Job or career was a fairly strong identity creation element, particularly in users with interesting or unusual jobs – television presenter, game designer, filmmaker, assistant to people with autism spectrum disorders, saxophonist or political party spokesperson.

Users mainly shared photos from the work process or from after-work social activities with colleagues, shared their successes, experiences or observations and, in the case of musicians, invited their friends to concerts.



Picture 4: Job and School

Conversely, users wrote about school only very exceptionally and mostly to boast about finishing their thesis, photos of the degree ceremony or a school event with schoolmates. Posts concerning success, for the most part, generated a large number of reactions in the form of Likes and also comments, where the users congratulated the author and expressed support.

5.4.6. THE HOBBY

Picture 5: The Hobby

If the users did not profile themselves via their jobs, they often did it via their hobbies, i.e. activities of personal interest or to which they regularly devote their free time. They did this by posting photos and statuses referring to a concrete activity.

Musicians usually invited people to their concerts and posted photos from rehearsals and foreign tours, users interested in cooking and baking shared photos of their creations sometimes even with recipes. In general, users highlighting their hobby tended to do so via their successes. It was interesting that sport appeared as a more or less regular hobby for only a very small section of the respondents.

5.5. IMPRESSION MANAGEMENT, AUDIENCE, AND PRIVACY

Published content on the user´s profile and his activity on *Facebook* is the most noticeable way of expressing one´s identity. In the first part of the research we determined categories for the content most frequently published by users, thereby confirming that *Facebook* is used by the users, not just for conduct of social interactions, but also serves as a podium for self-representation.

One of the central themes of *Goffman's* theory is the concept of impression management, in other words the effort to control the impression that an individual's presentation makes in his audience. It is the confirmation or rejection of the existence of conscious control and

adaptation of self-presentation on *Facebook* which was one of the aims of the second part of the research, interviews with selected respondents.

Conscious management of the creation of a good impression manifested itself for instance in a respondent who uses his *Facebook* profile for making professional contacts. In the course of the interview, respondent and musician, *Jan*, described in detail how he builds his image of a good saxophonist:

> *Jan*: *"I used to post a lot of jokey ones (posts) but now I almost only post things about saxophones. And it's always to let someone know where I am and it's always self-presentation of me as a saxophonist and a cool guy. On my Facebook I have professionals and then a band of fellow students and it all mingles on Facebook and everyone knows everything about each other and all chat away together and I post things to suit everybody. So that maybe the old musicians say, oh right, that must be somewhere in Prague and that's that person and everybody thinks that I'm a good saxophonist and so I don't post my recordings there so that the people who are under the illusion that I'm good don't start thinking otherwise. (laughter) I have to listen to all of my recordings three times before posting them so that when someone listens to it, it confirms what he already thinks. Even though it is partially a pose, of course. Or maybe I post something casual, like I take a photo of us sitting at the table and lying on the table there is some sheet music for something that's really difficult and that I play and I want the others to know that I can play […]."*

Other respondents emphasised mostly the authenticity of their activity; they did not want their presentation to seem different than in real life. In response to the question whether she has an image that she would like to present herself under on *Facebook*, *Anna* alone openly admitted that the image that she creates about herself on the social networks does not fully correspond with how she really spends her time:

> *Anna*: *"Well of cooourse… (laughter) As the beautiful, successful Anna who's awfully funny and has loads of friends. But the fact that I go home from work every day and open a bottle of beer in front of the TV... and I can't even be bothered to go out for a beer is another matter."*

The selection of topics published on *Facebook* is influenced by users' interests, the goal behind the content that they post on *Facebook*, but also of course by the audience at whom the post is targeted. Most of the respondents agreed that they aim at groups of people with similar interests and opinions, friends whom they see often or else they have a specific person in mind who they would like to see the post.

The trouble is that in social networks not only do we not know who, when and whether someone at all is following our presentation, but we do not even have any opportunity to monitor direct feedback from viewers in the form of non-verbal reactions. Additionally, we might encounter completely disparate groups of users in the unknown audience – parents, friends, colleagues, acquaintances or neighbours. These groups differ not only in the intensity of their links to the individual but also they expect different *façades* and disparate roles from the individual.

For this reason, as *Hogan* rightly points out, two groups of users are particularly important for the individual – those whom the user wishes to present his idealised self to and the group for whom his presentation might be potentially offensive.[36] According to *Hogan*, it is the people who are not the intended audience of the content, but have access to it who

> *"define the lowest common denominator of what is normatively acceptable"*.[37]

Although *Facebook* does provide a tool for segregating the audiences and allows the user to restrict the circle of users who can see every single artifact, most users leave the decision of who the audience will be to *Facebook* algorithms and set privacy settings to just for friends only, or friends of friends.[38]

It became clear from our interviews that users think about the audience of their post, and some actually adjust the visibility settings, but in most cases, they try to publish only generally inoffensive content. Despite the fact

---

[36] Hogan, B. (2010) The Presentation of Self in the Age of Social Media: Distinguishing Performances and Exhibitions Online. *Bulletin of Science, Technology & Society*, 30 (6), p. 383. [online] Available from: http://bst.sagepub.com/cgi/doi/10.1177/0270467610385893 [Accessed 21 May 2017].

[37] Ibid.

[38] Suh, J. J. and Hargittai, E. (2015) Privacy Management on Facebook: Do Device Type and Location of Posting Matter? *Social Media + Society*, 1 (2). [online] Available from: http://journals.sagepub.com/doi/10.1177/2056305115612783 [Accessed 21 May 2017].

that usually the audience is primarily a group of friends, the *Facebook* space is treated as publicly accessible.

> *Ota*, 28 years of age: *"[...] today, for instance, I did it with a post which nobody from work can see, because I posted it during a meeting. (laughter) But of course, it´s not a big deal, I don't know why I hid it. Otherwise, now I mostly post things public really, apart from things like let´s meet at Náplavka today, but things like films and advertising are public because it doesn't matter who sees them."*

In the first part of the research, we mentioned the respondent's effort to post interesting, enlightening or humorous content. The criterion according to which they assess the success and quality of their and others' posts is, amongst other factors, the number of Likes and comments.

The feedback was understood amongst other things as an evaluation of the quality of a post and served as motivation to publish content on *Facebook*, as one of the respondents, *Karel*, mused:

> *"[…] otherwise you wouldn't post anything really, you could just go outside and shout something."*

A post that gets no feedback was perceived as unsuitable for *Facebook* and was often deleted by the users. The absence of feedback may be understood as a sign that the post is bad, boring or bothersome, but it might also secondarily imply that the user in question is not popular or nobody is interested in the content that he posts – and so might damage the image so carefully created by the user.

5.5.1. REGIONS

The term regions established by *Goffman* also relates to the issue of conscious impression management on online social networks. *Goffman* defines the back region (backstage) as

> *"[…] a place, relative to a given performance, where the impression fostered by the performance is knowingly contradicted as a matter of course."*[39]

The back region, therefore, relates to a specific performance, to a specific front region. This means that in real life every stage has its backstage.

[39] Goffman, E. (1959) *The Presentation of Self in Everyday Life*. Garden City, N.Y.: Doubleday, p. 69.

In the environment of the online social networks it is a little more complicated – an environment which in certain situations and in relation to the audience is the front region, in a different situation may be behind the scenes and vice-versa. For example a private group may serve as a front region and back region simultaneously, only the potential audience making the difference.

However, despite this variability of regions, the respondents themselves see their borders quite clearly – they consider their user profile to be the front region, and messages with a friend or group chats to be the back region. Both the content and form of communication adapt to the regions:

> *Magda*: *"Well, the front region is certainly my wall where I put my posts... And the back one is probably chat where I can discuss what I can't perhaps write on my profile page; those negative things, what is bothering me, serious things and so on."*
>
> Researcher: *"Do you think that your behaviour varies in the front and the back region?"*
>
> *Karel*: *"Certainly, like when I communicate with all of those different people, it's like one minute you are talking in the pub with mates and the next you are talking on stage in front of 50 people."*

The way the respondents understand the back and front region corresponds to the duality of public and private life just as *Aspling* described in his work.[40] Behaviour in these two regions differs – users decide which information to post "publically" on their profile, thereby giving almost anybody the opportunity to read it, and which information they intend to share only with selected persons via private messages. Instead of bothering with difficult private settings the users rather treat their profiles like a public space, carefully choosing appropriate content for the wide possible audience. Instead of taking advantage of their privacy rights being protected by the law, they choose a self-regulating tactic to restrict what they share.

[40] Aspling, F. (2011) *The Private and the Public in Online Presentations of the Self: A Critical Development of Goffman's Dramaturgical Perspective*. MA. Stockholm University.

5.6. LIMITATIONS

This research serves only as a pilot study – its findings cannot be applied universally, but rather should serve as a starting point for a more detailed and longer study of user behaviour.

The first limitation is the fact that the study was conducted on a relatively demographically homogenous sample of 50 respondents. In order to get more representative results, we would have to include respondents of various ages, education, locations, and activity level on the online social network.

For methodological reasons, we made our selection from fairly active users publishing at least one post a week, so to achieve more neutral results longitudinal research would be required, which would allow the inclusion of less active users too and also it would reduce the impact of various exceptional situations (holidays, presidential elections, floods, etc.) and cultural and social trends on the content and form of social interactions, and on the primary roles that users play on *Facebook*.

A certain limit of the research may also be the subjectivity of the researchers, especially if the researcher knows the respondents personally. In that case, we would like to argue that personal acquaintance between the researchers and respondents may well be of benefit because it enables the researchers to better decipher the context of the message, its real meaning and therefore be able to code the posts more precisely.

The users themselves knowing that they are being observed and possibly changing their behaviour might also be a threat to the validity of the research. However, we tried to avoid this by notifying the users that even posts preceding recruitment of respondents would be analysed and in the end also analysing posts published about two months after our first contact with the respondents, by which time most of them had already forgotten about the research.

A special problem is the question as to how much is creation and confirmation of identity on *Facebook* influenced by *Facebook's* own algorithm for arranging posts into the so-called news feed.

The news feed itself does not contain all posts from friends, pages, etc., but only a selection. *Facebook* talks about it like this:

> *"The stories that show in your News Feed are influenced by your connections and activity on Facebook. This helps you to see more stories that*

> *interest you from friends you interact with the most. The number of comments and likes a post receives and what kind of story it is (e.g. photo, video, status update) can also make it more likely to appear in your News Feed."*[41]

The procedure applied by *Facebook* for showing *Stories* (as they call posts in this context) is not publicly known, it is a commercial secret of *Facebook* and is being constantly developed. The content that *Facebook* offers in this way to its users is tailored to the interests of each user.

The emphasis on interconnection between users influencing what content we see in our news feed is linked fundamentally to a principle called *homophily*[42]. This may be simply described as the fact that the friends we have are primarily individuals with whom we share certain properties and values. This principle dominates both in real-life networks[43] and in online social networks, as much research has confirmed. This applies for example to age or nationality-related homophily[44] or racial homophily[45].

At the same time, this algorithm also makes it extremely unclear who of our friends see our posts and react to them. Reactions of friends to users' posts provoke reinforcement (confirmation) of the created identity. However, not knowing whether they ever saw a post may result in considerable distortion. In a way, we may be seeing a special variation of a phenomenon known as the echo chamber.

6. CONCLUSION

The aim of this study was to investigate how users form and present their identity on the online social networks from the perspective of *Erving Goffman's* dramaturgical sociology.

---

[41] Facebook. (2019) *How News Feed Works. What kinds of posts will I see in News Feed?* [online] Available from: https://www.facebook.com/help/www/1155510281178725 [Accessed 24 January 2019].

[42] Wikipedia. (2019) *Homophily.* [online] Available from: https://en.wikipedia.org/wiki/Homophily [Accessed 24 January 2019].

[43] McPherson M., Smith-Lovin L. and Cook J.M. (2001) Birds of a feather: Homophily in social networks. *Annual Review of Sociology*, 27, pp. 415–444.

[44] Ugander, J., Karrer. B., Backstrom, L., Marlow, C. (2011) The Anatomy of the Facebook Social Graph. *arXiv*, 1111.4503. [online] Available from: https://www.researchgate.net/publication/51956889_The_Anatomy_of_the_Facebook_Social_Graph [Accessed 24 January 2019].

[45] Wimmer, A. and Lewis K. (2010) Beyond and Below Racial Homophily: ERG Models of a Friendship Network Documented on Facebook. *American Journal of Sociology*, 116 (2), pp. 583–642; Bakshy, E., Messing S. and Adamic. L. (2015) Exposure to ideologically diverse news and opinion on Facebook. *Science*, 348 (6239), pp. 1130–1132.

The complexity of this issue comprising the themes of impression management, roles, communication, privacy and audience, demanded the conduct of a qualitative content analysis of *Facebook* posts and subsequent interviews with the respondents, which allowed us to understand and describe in detail how people perform on *Facebook*, whether they consciously influence the impression they make in their audience and whether their behaviour differs in the front and back region.

We were able to establish five methods of creation and presentation of identity that the users apply on their *Facebook* profiles. We have named these categories *The Public Diary*, *The Influencer*, *Job and Education*, *Hobby* and *The Entertainer*. On most user profiles we find posts in all five categories. The fact that the most frequent method of presentation on *Facebook* were *Public Diary* type posts drawing attention to the person and the personal life of that user proves that *Facebook* is a self-presentation platform.

Interviews with *Facebook* users, the second part of the research, allowed us to confirm that users consciously adapt the method of presenting themselves to suit the anticipated audience, the intended goal and the image the users want to present of themselves. Users consciously control the language they use and try to make their presentation match their real-life behaviour. They build their image using profile and cover photos, shared posts, their interests and also photos where they tag their friends. They post only the inoffensive and desirable ones on their profile. They delete content from their profile which for some reason they consider to be unsuitable, either for their audience or they do not want to be publicly connected with it.

The users themselves confirmed that both the form and the content of their presentation and interaction that take place in the front region (in the personal profile) and in the back region (during chat) differ, thereby confirming our hypothesis that *Facebook* is not just a back region, where the user enjoys his privacy, but also a front region where the user presents his carefully prepared identity. The line between private and public is blurred in the context of social media. Users perceive the front region almost as a public space and the published content is adapted for that space, while chat is perceived as being similar to a private get-together with friends and the form and topics of conversation correspond with this, being more relaxed and personal than in the front region. Although the users are

aware of their right to privacy, they willingly choose to disclose certain personal information online.

As *Sarikakis and Winter* note:

> *"The vast number of users and the publicness of "their" information pose new challenges to privacy and, thus, social media usage actively shapes and challenges notions of privacy. Even loss of privacy is renegotiated and reframed as transparency and connectedness, underpinning legal dilemmas regarding withholding privacy rights in the fight against terrorism."*[46]

Even though the research was conducted on a fairly small sample of respondents, we believe that we have successfully proved that *Goffman's* dramaturgical theory is a suitable framework for researching presentation and social interaction on the online social networks and helped define the current situation with regard to administration of user profiles, user presentation and the advantages and also the pitfalls of building and maintaining relationships on *Facebook*.

In view of the small sample of respondents, the research serves more as a pilot study and should be followed up on by a longitudinal study conducted on a more representative sample of *Facebook* users. Future research could focus on the content of comments, the way in which *Facebook* interactions influence real interaction or the effect that "growing up" on online social networks has on the younger generation.

Future research regarding privacy could focus on evaluating the sensitivity of published content, exploring the level of legal consciousness and users' understanding of how personal data are used. It would also be useful to map the different privacy protection laws and regulations in various countries in relation to global online social networks.

The discussion about privacy is also a philosophical discussion about the freedom of expression, the nature of online space and its commercialization, the governments' duties and the technological and legal literacy, and future studies can help with addressing these issues.

From the social point of view, further research into users' perception of the public/private dichotomy in an online world, the commodification

[46] Sarikakis, K. and Winter L. (2017) Social Media Users' Legal Consciousness About Privacy. *Social Media + Society*. [online] Available from: https://journals.sagepub.com/doi/full/10.1177/2056305117695325#articleCitationDownloadContainer [Accessed 26 August 2019].

of privacy and the limits to which users are willing to go to gain access to an online social world, would be also beneficial.

LIST OF REFERENCES

[1] Abercrombie, N. and Longhurst, B. (1998) *Audiences: A sociological theory of performance and imagination*. Thousand Oaks, California: Sage.

[2] Aspling, F. (2011) *The Private and the Public in Online Presentations of the Self: A Critical Development of Goffman's Dramaturgical Perspective*. MA. Stockholm University.

[3] Bakshy, E., Messing S. and Adamic. L. (2015) Exposure to ideologically diverse news and opinion on Facebook. *Science*, 348 (6239).

[4] boyd, d. (2006) Friends, friendster and MySpace top 8: Writing community into being on social network sites. *First Monday*, 11 (12). [online] Available from: http://firstmonday.org/issues/issue11_12/boyd/index.html [Accessed 20 January 2019].

[5] boyd, d. (2007) Why Youth (Heart) Social Network Sites: The Role of Networked Public in Teenage Social Life. In: David Buckingham (ed.). *MacArthur Foundation Serieson Digital Learning – Youth, Identity, and Digital Media Volume*. Cambridge, MA: MIT Press.

[6] boyd, d. and Ellison, N.B. (2007) Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13 (1). [online] Available from: http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html [Accessed 7 March 2017].

[7] Chou, H. G. and Edge, N. (2012) "They Are Happier and Having Better Lives than I Am": The Impact of Using Facebook on Perceptions of Others' Lives. *Cyberpsychology, Behavior, and Social Networking*, 15 (2). [online] Available from: http://online.liebertpub.com/doi/abs/10.1089/cyber.2011.0324 [Accessed 21 May 2017].

[8] Dijck, J. (2013) *The culture of connectivity: A critical history of social media*. New York: Oxford University Press.

[9] Dočekal, D. (2016) *TIP#650: Kolik má v Česku Facebook uživatelů? Jak je to s věkem? Proč jsou ta čísla tak podivná?* [blog entry] 6 November. Prague: *365tipu*. Available from: https://365tipu.wordpress.com/2016/11/06/tip650-kolik-ma-v-cesku-facebook-uzivatelu-jak-je-to-s-vekem-proc-jsou-ta-cisla-tak-podivna/ [Accessed 20 January 2019].

[10] Eisenlauer, V. (2014) Facebook as a third author – (Semi-)automated participation framework in Social Network Sites. *Journal of Pragmatics*, 72. [online] Available from: http://linkinghub.elsevier.com/retrieve/pii/S037821661400037X [Accessed 21 May 2017].

[11] Facebook. (2018) *Facebook Reports Third Quarter 2018 Results*. [online] MENLO PARK, California: Facebook. Available from: https://investor.fb.com/investor-news/press-release

-details/2018/Facebook-Reports-Third-Quarter-2018-Results/default.aspx [Accessed 11 December 2018].

[12] Facebook. (2019) *How News Feed Works. What kinds of posts will I see in News Feed?* [online] Available from: https://www.facebook.com/help/www/1155510281178725 [Accessed 24 January 2019].

[13] Goffman, E. (1959) *The Presentation of Self in Everyday Life*. Garden City, N.Y.: Doubleday.

[14] Gosling, S. D. et al. (2011) Manifestations of Personality in Online Social Networks: Self--Reported Facebook-Related Behaviors and Observable Profile Information. *Cyberpsychology, Behavior, and Social Networking*, 14 (9). [online] Available from: http://www.liebertonline.com/doi/abs/10.1089/cyber.2010.0087 [Accessed 21 May 2017].

[15] Greenwood, S., Perrin, A. and Duggan, M. (2016) *Social Media Update*. [online] Washington: Pew Internet & American Life Project. Available from: http://www.pew internet.org/2016/11/11/social-media-update-2016/ [Accessed 17 April 2018].

[16] Hewitt, A. and Forte, A. (2006) Crossing boundaries: Identity management and student/faculty relationships on the Facebook. In: *Proc 2006 CSCW*, Canada, 4–8 November. [online] Available from: http://andreaforte.net/HewittForteCSCWPoster 2006.pdf [Accessed 7 March 2018].

[17] Hogan, B. (2010) The Presentation of Self in the Age of Social Media: Distinguishing Performances and Exhibitions Online. *Bulletin of Science, Technology & Society*, 30 (6). [online] Available from: http://bst.sagepub.com/cgi/doi/10.1177/0270467610385893 [Accessed 11 May 2017].

[18] Lenhart, A. (2015) *Teens, Social Media & Technology Overview 2015*. [online] Washington: Pew Internet & American Life Project. Available from: http://www.pewinternet.org/2015/ 04/09/teens-social-media-technology-2015/ [Accessed 8 June 2017].

[19] Lewis, K., Kaufman, J. and Christakis, N. (2008) The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer--Mediated Communication*, 14 (1). [online] Available from: https://onlinelibrary.wiley.com/ doi/pdf/10.1111/j.1083-6101.2008.01432.x [Accessed 12 March 2017].

[20] Lin, R. and Utz, S. (2015) The emotional responses of browsing Facebook: Happiness, envy, and the role of tie strength. *Computers in Human Behavior*, 52. [online] Available from: http://linkinghub.elsevier.com/retrieve/pii/S074756321500360X [Accessed 21 May 2017].

[21] Macek, J. (2013) More than a desire for text: Online participation and the social curation of content. *Convergence: The International Journal of Research into New Media Technologies*,

19 (3). [online] Available from: http://con.sagepub.com/cgi/doi/10.1177/1354856513486530 [Accessed 15 January 2019].

[22] Marwick, A. E. and boyd, d. (2011) I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, 13 (1). [online] Available from: http://journals.sagepub.com/doi/10.1177/1461444810365313 [Accessed 10 December 2018].

[23] McPherson M., Smith-Lovin L. and Cook J.M. (2001) Birds of a feather: Homophily in social networks. *Annual Review of Sociology*, 27.

[24] Michikyan, M. et al. (2014) Can you tell who I am? Neuroticism, extraversion, and online self-presentation among young adults. *Computers in Human Behavior*, 33. [online] Available from: http://linkinghub.elsevier.com/retrieve/pii/S0747563214000156 [Accessed 21 May 2017].

[25] Miller, H. (2016) *Investigating the Potential for Miscommunication Using Emoji*. [blog entry] 5 April. GroupLens. Available from: https://grouplens.org/blog/investigating-the-potential-for-miscommunication-using-emoji/ [Accessed 26 January 2019].

[26] Pospíšilová, M. (2016) *Facebooková (ne)závislost: identita, interakce a uživatelská kariéra na Facebooku*. Praha: Univerzita Karlova, nakladatelství Karolinum.

[27] Riccio, J. R. (2013) *All The Web's a Stage: The Dramaturgy of Young Adult Social Media Use*. Syracuse: Syracuse University, Theses – ALL. Paper 16. Magisterská práce (MA) Syracuse University. Available from: http://surface.syr.edu/cgi/viewcontent.cgi?article=1007&context=thesis [Accessed 5 May 2017].

[28] Sarikakis, K. and Winter L. (2017) Social Media Users' Legal Consciousness About Privacy. *Social Media + Society*. [online] Available from: https://journals.sagepub.com/doi/full/10.1177/2056305117695325#articleCitationDownloadContainer [Accessed 26 August 2019].

[29] Steinberg, L. (2008) *Adolescence*. 8th ed. New York: McGraw-Hill.

[30] Stone, A. R. (1991) Will the Real Body Please Stand Up? Boundary Stories About Virtual Cultures. In: Michael Benedikt (ed.). *Cyberspace: First Steps*. Cambridge, MA: MIT Press.

[31] Studýnková, N. (2010) *Konzumace pirátských kopií televizních seriálových narací*. Bakalářská práce. Masarykova univerzita, Fakulta sociálních studií. Vedoucí práce Jakub Macek. Available from: http://con.sagepub.com/cgi/doi/10.1177/1354856513486530 [Accessed 28 December 2018].

[32] Suh, J. J. and Hargittai, E. (2015) Privacy Management on Facebook: Do Device Type and Location of Posting Matter? *Social Media + Society*, 1 (2). [online] Available from: http://journals.sagepub.com/doi/10.1177/2056305115612783 [Accessed 21 May 2017].

[33] Ugander, J., Karrer. B., Backstrom, L., Marlow, C. (2011) The Anatomy of the Facebook Social Graph. *ArXiv*, 1111.4503. [online] Available from: https://www.researchgate.net/publication/51956889_The_Anatomy_of_the_Facebook_Social_Graph [Accessed 24 January 2019].

[34] Wallace, E., Buil, I., de Chernatony, L. and Hogan, M. (2014) Who " likes" You… and why? A Typology of Facebook Fans from "Fan" –atics and Self Expressives to Utilitarians and Authentics". *Journal of Advertising Research*, 54 (1).

[35] Walther, J. B. a D'addario, K. P. (2001) The Impacts of Emoticons on Message Interpretation in Computer-Mediated Communication. *Social Science Computer Review*, 19 (3). [online] Available from: http://ssc.sagepub.com/cgi/doi/10.1177/089443930101900307 [Accessed 21 May 2017].

[36] Wikipedia. (2019) *Homophily*. [online] Available from: https://en.wikipedia.org/wiki/Homophily [Accessed 24 January 2019].

[37] Wimmer, A. and Lewis K. (2010) Beyond and Below Racial Homophily: ERG Models of a Friendship Network Documented on Facebook. *American Journal of Sociology*, 116 (2).

[38] Zhao, S. (2005) The Digital Self: Through the Looking Glass of Telecopresent Others. *Symbolic Interaction*, 28 (3). [online] Available from: http://doi.wiley.com/10.1525/si.2005.28.3.387 [Accessed 27 October 2018].

[39] Zhao, X. et al. (2013) The many faces of facebook. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems – CHI '13*, Paris, 27 April – 2 May. New York, USA: ACM Press. [online] Available from: http://dl.acm.org/citation.cfm?doid=2470654.2470656 [Accessed 18 January 2018].

DOI 10.5817/MUJLT2019-2-6

SHAREHOLDER LEDGER USING DISTRIBUTED LEDGER TECHNOLOGY: THE ESTONIAN PERSPECTIVE

by

ANNE VEERPALU*

The article focuses on whether it is possible to use new technologies such as distributed ledger technology (DLT) in shareholder ledger maintenance systems. The article uses Estonia as an example to describe the shortcomings of shareholder ledger maintenance regulation and possible suggestions for reform and applies the principle of technology-neutrality to the subject matter to assess whether the regulation allows the adoption of new technologies, such as DLT, in ledger maintenance. The aim of the principle of technology-neutrality is to secure that the regulator does not create regulation that prefers any particular technology and discriminates against other technologies. Any regulation that is built around a pre-existing technology could suffer from preferring the use of that particular technology and consequently hinder innovation. In the article it is examined whether the ledger maintenance models used in Estonia are benefitting or suffering from the non-existence of technology-neutral technical standards for ledger maintenance and whether the differentiation of treatment of shareholder ledger administrators is justified on the basis of the principle of technology-neutrality.

KEY WORDS

Distributed Ledger Technology, DLT-Specific Legislation, Shareholder Ledger Administration, Technology-Neutrality Principle

* anne.veerpalu@njordlaw.ee, Ph.D. Candidate in Information Technology Law, Law School, Tartu University, Estonia.

1. INTRODUCTION

Shareholder ledgers are used to indicate the names of the shareholders of a business entity divided by shares. Typically, nowadays shares are held in book entry form and no certificates are issued to shareholders. This means that the ownership of a share is proven primarily on the basis of the ledger data – usually in computerized- or paper-format. Consequently, a ledger is also the source of data on the eligibility to earn dividends and on who controls the company. There can be only one trustworthy source of truth regarding shareholders and the shareholding structure. The ledger data must be complete and accurate at all times. Therefore, the ledger´s reliability is of crucial importance and in order to ensure the reliability of ledger data – appropriate rules and safeguards must be placed on the procedures to amend the ledger data. Hence, the regulation on shareholder ledger administration is concerned with certainty about the ledger data and the transparency regarding how the ledger data can be amended. However, the rules and procedures regulating ledgers should make it easy to access it, yet, at the same time easy for shareholders to transfer the share.

The article will use Estonia as a use case to test whether the existing regulation allows the use of new innovative technology such as DLT in shareholder ledger maintenance. Why specifically DLT? Primarily, because DLT is a ledger technology and shareholder ledger is primarily a ledger – hence, the question: *Would this be a beneficial match for the obligated parties tasked with ledger maintenance and for the shareholders desiring liquidity and transparency?* Secondly, because France and the State of Delaware in the US have introduced DLT-specific legislation in similar context hoping to innovate their shareholder ledger maintenance system. Estonia was chosen as a use case because Estonia continues to market itself as the "blockchain nation"[1] due to the almost decade long use of timestamping technologies (now also referred to as private blockchain) on its public registries. Given this background Estonia should be an ideal testbed for DLT applications in shareholder ledger maintenance.

The article focuses on shareholder ledgers of private limited liability companies in Estonia – *osaühing (OÜ)* because the majority of the Estonian

[1] Korjus, K. (2017) *Welcome to the blockchain nation*. [blog entry] Medium Blog, 7 July 2017. Available from: https://medium.com/e-residency-blog/welcome-to-the-blockchain-nation-5d9b46c06fd4 [Accessed 20 January 2019].

legal entities are OÜs. According to § 148(6) of the Estonian Commercial Code[2] (CC), no certificates are issued for the shares of OÜs and shares are held in book entry form. CC requires that a shareholder ledger must be administered (meaning it is not optional) and there can be only one ledger per business entity.

At the moment there are two ways to administer an OÜ´s shareholder ledger in Estonia: (i) management board as the administrator or (ii) *Central Securities Depository (CSD)* as the administrator. As of March 2018, only 1.7 % of all OÜs (178,513 in total) had registered their shares at the CSD.[3] This means that although this alternative has been around for almost two decades, most companies have chosen not to register their shares at the CSD. The popularity of the use of the service of CSDs has not increased also after the transposition of CSDR[4] in Estonia which opened the national market for cross-border services of other CSDs. While the unpopularity of the CSDs is most likely linked to applicable fees and the difficulty in fulfilling the precondition for registration – the need to have a bank and securities account in an Estonian commercial bank for each shareholder – due to anti-money laundering (AML) requirements applicable to banks. This precondition virtually excludes companies with non-resident shareholders from using CSD alternative.

Consequently, vast majority of shareholder ledgers in Estonia are administered by management boards. This coincides with the dominant practice in other European countries, e.g. the UK, Sweden, Finland, Latvia, Germany, the Netherlands and Denmark where companies administer their shareholder ledgers themselves.[5] This said, however, the reality at the moment is that management boards in Estonia are administering the ledgers rather poorly or not at all.

---

[2] Commercial Code (*Äriseadustik*) 1995. Estonia: Riigi Teataja (State Gazette). RT I 1995, 26, 355 in Estonian.

[3] Chamber of Notaries. (2018) Notarite Koja arvamus ühinguõiguse revisjoni muudatusettepanekute kohta, *Opinion on the analysis-concept paper of company law revision working group*, 17th December 2018, p. 2. [online] Available from: https://www.just.ee/sites/www.just.ee/files/notarite_koja_arvamus_18.12.2018.pdf [Accessed 12 January 2019].

[4] Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012. Text with EEA relevance. OJ L 257, 28. 8. 2014, pp. 1–72 (CSDR).

[5] Ministry of Justice. (2018) *Ühinguõiguse revisjon Analüüs-kontseptsioon* (Revision of Company Law, hereinafter Analysis-concept paper), 15 September 2018, p. 489. [online] Available from: https://www.just.ee/sites/www.just.ee/files/uhinguoiguse_revisjoni_analuus-kontseptsioon.pdf [Accessed 12 January 2019].

While globally registries and ledgers have seen a shift from offline to online, no such development regarding shareholder ledgers has taken place in Estonia as majority of the ledgers maintained by the management boards are kept in oral- or paper-format. Furthermore, this means that under the CC the majority of share transfer transactions in Estonia need to be authenticated by the notary. As can be seen in section 3 of the article, the notaries authenticating these share transfer transactions do not trust the shareholder ledgers maintained by management board but rather trust the "unofficial" duplication of ledger data by Commercial Register (CR).[6] Neither the national nor regional law[7] requires such duplication or disclosure of shareholder data in the CR. Consequently, such practice of "unofficial" duplication of records at CR devalues the CR data as majority of CR data is reliable and official. However, the shareholder data the CR contains is not constitutive, not binding and unreliable under the law. This concerning practise among other issues has led the *Ministry of Justice* as part of their company law codification plan to take the initiative to reform also the current shareholder ledger maintenance regulation.

Consequently, the research question posed in the article is whether the existing regulation and reform ideas of ledger maintenance in Estonia are open to the use of new innovative technologies, such as DLT, or are there amendments needed for any technological innovation to be used in this area of application?

In order to address the research question, first, in section 2, an introduction will be provided to DLT including an overview of the developments in the area of DLT-specific regulatory initiatives addressing share registries and shareholder ledgers in France and the State of Delaware in the US. Thereafter, in section 3 the development of the regulation of the two separate ledger maintenance models in Estonia are discussed along with the concerns these face. Each concern is followed

---

[6] Commercial Register is the registration department of *Tartu County Court* that maintains the register of the enterprises of sole proprietors and companies located in Estonia. Section 22(1) of CC.

[7] Directive 2009/101/EC of the European Parliament and of the Council of 16 September 2009 on coordination of safeguards which, for the protection of the interests of members and third parties, are required by Member States of companies within the meaning of the second paragraph of Article 48 of the Treaty, with a view to making such safeguards equivalent (Text with EEA relevance). OJ L 258, 1. 10. 2009, pp. 11–19. Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law (Text with EEA relevance). OJ L 169, 30. 6. 2017, pp. 46–127.

by a theoretical applications of DLT-based ledger system to solve these concerns.

Finally, in section 4 the author addresses the possibility to use DLT in ledger maintenance addressing the regulation´s susceptibility to the use of new technologies. The approach is primarily based the application of the principle of technology-neutrality, which is a principle supporting both innovation and competition, and the author assesses the compliance of the current regulation and reform ideas with the said principle. As the author has discussed the principle at length in one of her previous articles,[8] the principle will be introduced only briefly in section 4 of the article.

Although the issues are approached as a case study from the point of view of Estonian law, similar questions can be raised in other legal systems, hence, the topic is both relevant and has global application.

2. DLT AND DLT-SPECIFIC LEGISLATION

In this section technology at hand and legislative initiatives targeting shareholder ledgers or share registries with the said technology from the State of Delaware, US and France are briefly discussed in order to contextualize the discussion that follows.

2.1. INTRODUCTION TO DLT

As regards technology, this article is concerned with the use of blockchain and distributed ledger technology (DLT). It can be argued that every blockchain is a distributed ledger, but not every distributed ledger is a blockchain.[9] For the purposes of this article, no distinction is made between blockchain and DLT.

Why is the technology at all called blockchain? Blockchain technology bears such a name for the reason that it groups data into blocks and the blocks into a secured chain using cryptography.[10] The chain grows

---

[8] Veerpalu, A. (2018) Decentralised Technology and Technology Neutrality in Legal Rules: An Analysis of De Voogd and Hedqvist. *Baltic Journal of Law & Politics*, 11 (2), pp. 61–94. doi: https://doi.org/10.2478/bjlp-2018-0011

[9] Shaan, R. (2018) *The Difference Between Blockchains & Distributed Ledger Technology*. [blog entry] Medium Blog Towards Data Science. Available from: https://towardsdatascience.com /the-difference-between-blockchains-distributed-ledger-technology-42715a0fa92 [Accessed 01 May 2018].

[10] Cuccuru, P. (2017) Beyond bitcoin: An early overview on smart contracts. *International Journal of Law and Information Technology*, 25 (3), pp. 179–195. [online] Available from: https://doi.org/10.1093/ijlit/eax003 [Accessed 30 May 2018].

indefinitely forming a list of records of transactions which only allows to append to it and does not allow to delete a block in between blocks. The block contains information about previous blocks of transactions and the current ledger entries and timestamps the status of the ledger making the ledger theoretically immutable. Immutability makes blockchain technology well-suited for administering registries, processing transactions and tracing ownership.

And what exactly is a distributed ledger? In the case of traditional databases a single entity or a person keeps the original copy of the database, while there may be other copies, these are merely backups of the original and not authoritative source of data. For this reason, these databases are also referred to as centrally governed or centralised databases. However, any database that is not centrally governed or centralised but instead the administration of which is distributed among various parties (i.e. nodes) can be called a distributed database or simply a distributed ledger.

Yet, DLT is not only about the database. DLT binds together many technologies that already existed earlier – such as peer-to-peer networks[11], consensus mechanism[12], cryptography[13] and linked timestamping[14]. The aim of the mix of these technologies is to achieve a transparent, highly resilient, tamper-resistant database operated by a decentralized or distributed network.[15]

There are two primary types of distributed ledgers depending on the openness to participation and consensus typology: permissionless (public) and permissioned (private). Permissioned means that participants in the consensus mechanism are pre-selected and access to the network is

[11] Nakamoto, S. (2008) *Bitcoin: Peer-to-peer Electronic Cash System*. [online] Available from: https://bitcoin.org/bitcoin.pdf [Accessed 12. April 2018].

[12] According to *De Filippi, P.* and *Wright, A.*: *"a consensus mechanism – a set of strict rules with predefined incentives and cost structures – which makes it difficult and costly for any one party to unilaterally remove or modify data stored on a blockchain. Consensus mechanisms help a blockchain-based network periodically reach agreement as to the current state of the shared database – even if members do not know or trust one another."* De Filippi, P. and Wright, A. (2018) *Blockchain and the Law: The rule of code*. Harvard University Press, p. 2.

[13] Ibid.

[14] Among one of the fundamental concepts behind *Bitcoin* protocol is something called linked timestamping, the two cryptographers from an Estonian technology company *Guardtime* – *Ahto Buldas* and *Märt Saarepera* – were the first to provide scientific evidence already in 2003 on what hash-functions and data structures are needed to give formal security proof. Guardtime (2019). [online] Available from: https://guardtime.com/technology [Accessed 14 January 2019].

[15] De Filippi, P. and Wright A. (2018) Op. cit., p. 2.

restricted (e.g. *R3 Corda*[16] and *Hyperledger Fabric*[17]). Permissionless ledgers, on the other hand, allow anyone to participate in the network and also in the consensus mechanism (e.g. *Bitcoin* and *Ethereum*[18]). Both *Bitcoin´s* and *Ethereum´s* protocol is open-sourced. The most well-known DLT network is based on permissionless *Bitcoin* protocol, which

> *"supports decentralized, global value transfer systems that are both transnational and pseudonymous."*[19]

Ethereum is a permissionless ledger that

> *"has a Nakamoto-style consensus protocol that relies on a distributed set of miners"*[20]

to continue existing and takes the protocol further than Bitcoin allowing scripts that are generally referred to as "smart contracts".[21]

Broadly speaking, the protocol of blockchain and DLT can be used to maintain a ledger of data, assets or rights. The unit of the ledger is the "vehicle of data" for anything – reprsenting tangible assets (house, car, key) or intangible assets (license, access keys, in-game items, securities).

After this short introduction to DLT, the next subsection will introduce the regulative initiatives in using DLT in shareholder ledger maintenance systems.

2.2. DLT-SPECIFIC RELEVANT LEGISLATION

Some jurisdictions are more prepared for the use of DLT than others and have as a result created DLT-specific legislation. For the purposes of the current article only the ones applicable to shareholder ledgers and share registries will be introduced. By no account does this section aim

---

[16] *Corda*, a protocol of a distributed database technology company *R3CEV LLC* that leads a consortium of more than 200 firms in research and development of distributed ledger usage in the financial system. Wikipedia. (2018) *Corda*. [online] Available from: https://en.wikipedia.org/wiki/R3_(company)#Corda [Accessed 14 January 2018].

[17] *Hyperledger Fabric* is a *Linux Foundation* built blockchain framework and operates as plug--and-play model.

[18] Wikipedia. (2019) *Ethereum.* [online] Available from: https://en.wikipedia.org/wiki/Ethereum [Accessed 14 January 2019].

[19] De Filippi, P. and Wright A. (2018) Op. cit., p. 3. Pseudonyms are identifiers of a person or persons that operate like placeholders as they mark an identity, yet the identity is unknown.

[20] McCorry, P., Hicks, A. and Meikeljohn, S. (2018) Smart contracts for bribing miners. *Conference Proceedings The 5th Workshop on Bitcoin and Blockchain Research 2nd March 2018*, p. 4. Available from: https://fc18.ifca.ai/bitcoin/schedule.html [Accessed 03 May 2018].

[21] Ibid.

to provide a comprehensive overview of these sort of initiatives as there might be others with the same aim the author is not aware of.

2.2.1. STATE OF DELAWARE, US

On 2nd of May 2016 Delaware's Governor announced the launch of *Delaware Blockchain Initiative*. For Delaware, the change embracing DLT was revolutionary as it allows a leap from record-keeping of ownership of public companies that was based on

> *"1970s-era technologies of depository institutions, jumbo paper certificates, and a centralized ledger".*[22]

Most public company equities issued in the United States are held on the ledger not under their owner´s names but under the name of an intermediary "record holder" and a broker keeps a second database of the actual shareholders behind the intermediary.[23] The DLT-specific amendments allow

> *"companies and stockholders to enjoy the benefits of electronic trading while maintaining direct ownership of their shares".*[24]

So the aim of the amendments was to increase transparency, liquidity and access to shares as DLT use allows for easy access, easy transfer and transparency regarding shareholders. The amendments allowing DLT´s use entered into effect on 1st August 2017 with the Senate Bill 69.[25] As explained in the *Synopsis*[26] of the Senate Bill 69 to amend the General Corporation Law of the State of Delaware (DGCL):

---

[22] Stromberg G. T. et al. (2018) *Are Headwinds Hampering Delaware's Blockchain Initiative?* [blog entry] Law 360 blog, 23 March 2018. Available from: https://jenner.com/system/assets/publications/17844/original/stromberg%20Law360%20March%2023%202018.pdf?1521837416 [Accessed 14 January 2019].

[23] Ibid.

[24] Lucking, D. (2017) *Delaware Passes Law Permitting Companies to Use Blockchain Technology to Issue and Track Shares*. Allen & Overy publications, 26 September 2017. [online] Available from: http://www.allenovery.com/publications/en-gb/Pages/Delaware-Passes-Law-Permitting-Companies-to-Use-Blockchain-Technology-to-Issue-and-Track-Shares-.aspx [Accessed 05 May 2019].

[25] Polner, G. et al. (2017) Delaware Approves Use of Blockchain in New DGCL Amendments. *Gibson Dunn Securities Regulation and Corporate Governance Monitor*, 31 July 2017. [online] Available from: http://securitiesregulationmonitor.com/Lists/Posts/Post.aspx?ID=299 [Accessed 07 May 2018].

[26] Delaware State Senate 149th General Assembly Senate Bill No. 69 An act to amend title 8 of the Delaware Code Relating to the General Corporation Law. [online] Available from: https://legis.delaware.gov/json/BillDetail/GenerateHtmlDocument?legislationId=25730&legislationTypeId=1&docTypeId=2&legislationName=SB69 [Accessed 07 May 2018].

> *"amendments to Sections 219, 224 and 232 and related provisions are intended to provide specific statutory authority for Delaware corporations to use networks of electronic databases (examples of which are described currently as "distributed ledgers" or a "blockchain") for the creation and maintenance of corporate records, including the corporation's stock ledger."*

There are certain legislative requirements for the ledger, such as that it must:

> *"(i) allow the production of a record of the company's stockholders; (ii) record certain mandatory information; and (iii) permit transfer of stock".*[27]

Plus the ledger must also *"be capable of being converted into 'clearly legible paper form'"*[28], which must be *"valid and admissible in evidence"*.[29] Furthermore, the *Delaware Division of Corporations* also operates a node on the permissioned DLT network for authenticating the stock issuance.[30]

For the purpose of providing a solution in line with the registration, the state of Delaware partnered with a DLT start-up called *Symbiont*[31] who built an application called *Smart Securities*.[32] *Symbiont* itself runs a permissioned private ledger on its own non-open-sourced protocol.

Since then several other states in the United States (e.g. Arizona, Nevada, Wyoming) have followed this example and amended their laws to cater to the use of DLT technology in corporate governance.[33] Among these, the most noteworthy is a bill entitled "Corporate stock-certificate tokens" that was proposed on 16th January 2019 in Wyoming – after earlier

---

[27] Lucking, D. (2017) Op. cit.

[28] Ibid.

[29] Ibid.

[30] Ibid.

[31] According to a blog by the chairman and president of *Symbiont Caitlin Long* its legal team also assisted also in drafting the DGCL's DLT-specific amendments. Long, C. (2018) *Blockchain crosses the Delaware*. [blog entry] Mediamarkets blog, 31 July 2018. Available from: https://www.marketsmedia.com/blockchain-crosses-delaware/ [Accessed 07 May 2018].

[32] Allison, I. (2015) Smart securities issuer Symbiont fires shots in the private blockchain arms race. [online] *International Business Times*, 28 September 2015. Available from: https://www.ibtimes.co.uk/smart-securities-issuer-symbiont-fires-shots-private-blockchain-arms-race-1521449 [Accessed 08 May 2018].

[33] Song, W. (2018) Bullish on blockchain: examining Delaware's approach to distributed ledger technology in corporate governance law and beyond. *Harvard Law Review*. Available from: http://www.hblr.org/2018/01/bullish-on-blockchain-examining-delawares-approach-to-distributed-ledger-technology-in-corporate-governance-law-and-beyond/ [Accessed 07 May 2018].

DLT-specific legislative initiatives[34] – with the aim to tokenize shares and place certificates of share ownership on blockchain.[35] This proposal would be replacing the paper-format certificates used in Wyoming for digital share certificates.[36]

2.2.2. FRANCE

DLT-specific legislative initiatives also sprung up in Europe: in Malta, Switzerland, Gibraltar, yet, the most relevant for the current article are the legislative initiatives of France. Similarly to Estonia, securities are issued in book-entry form in France.[37] The title to securities is reflected by way of amending the records of

> *"a securities account held by the issuer, a central securities depository (CSD) or a securities custodian".*[38]

France first implemented regulation in relation to blockchain technology[39] in relation to trading of minibonds in 2016. In 2017 it expanded the regulation also to securities.[40] On 9th December 2017, the French government presented order No 2017-1674 (DLT Order) regarding the use of DLT for the recording and transmission of securities.[41] The DLT Order

---

[34] ConsenSys. (2018) *Wyoming Passes 5 Pro-Blockchain Laws, Points the Way in Digital Asset Regulation*. [blog entry] Medium blog, 15 March 2018. Available from: https://media.consensys.net/wyoming-passes-5-pro-blockchain-laws-points-the-way-in-digital-asset-regulation-6fae9e07d129 [Accessed 27 January 2019].

[35] Nicholson, G. (2019) *Wyoming Proposes Bill for Issuance of Tokenised Certificates with Stocks*. [blog entry] TokenMarket, 17 January 2019. Available from: https://tokenmarket.net/news/regulation/wyoming-proposes-bill-issuance-tokenised-certificates-stocks/ [Accessed 23 January 2019].

[36] Proposal HB0185 named Corporate stock-certificate tokens. [online] Available from: https://www.wyoleg.gov/Legislation/2019/HB0185 [Accessed 23 January 2019].

[37] Report to the President of the Republic relating to Ordinance No. 2017-1674 of 8 December 2017 on the use of a shared electronic registration device for the representation and transmission of financial securities, *Rapport au Président de la République relatif à l'ordonnance n° 2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers. Published in JORF n°0287 du 9 décembre 2017 texte n° 23*. [online] Available from: https://www.legifrance.gouv.fr/eli/rapport/2017/12/9/ECOT1729053P/jo/texte [Accessed 01 May 2018].

[38] Clifford Chance. (2018) France pioneers blockchain legal framework for unlisted securities. *Law Firm Briefing Note*, January 2018. Available from: https://www.cliffordchance.com/content/dam/cliffordchance/PDFDocuments/Client%20Briefing%20-%20France%20-%20Blockchain%20for%20unlisted%20securities%20180750-4-2....pdf [Accessed 22 April 2018].

[39] Vocabulaire de l'informatique (liste de termes, expressions et définitions adoptés) published in JORF n°0121 du 23 mai 2017 texte n° 20. Available from: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000034795042&categorieLien=id [Accessed 1 May 2018].

[40] *DLT* was defined as *"a method of recording continuously generated data as blocks linked to each other in the chronological order of their validation, each block and its sequence being protected against modification"*.

[41] Clifford Chance. (2018) Op. cit., p. 1.

covers only the categories of securities not admitted to the CSD under CSDR. Hence, the DLT Order regulates unlisted equity securities issued by joint stock companies,[42] units or shares of collective investment undertakings, negotiable debt securities such as bonds.[43]

The main advantage of the DLT Order is that it allows for multiplicity of shareholder ledger administrators to advance competition and better user experience in addition to CSD. Furthermore, the registration of securities on DLT is under the law comparable in effect to the registration of securities at CSD, so that all benefits CSD-registered instruments enjoy are extended to DLT-registered instruments also. The intention of the French initiative was to increase liquidity so that the transfer of securities isallowed from account-to-account or wallet-to-wallet seamlessly.[44]

3. REGULATION AND REFORM IDEAS OF LEDGER ADMINISTRATION IN ESTONIA

In this section the existing regulation on and reform ideas of shareholder ledger maintenance in Estonia are introduced. The section also portrays observations made about ledger maintenance practise and draws out the concerns with the system in order to conduct the analysis of the research question in section 4.

3.1. CURRENT LEGISLATION ON SHAREHOLDER LEDGERS IN ESTONIA

Under the CC, there are two ways to administer shareholder ledger of an OÜ: (i) by the management board or (ii) by CSD, which maintains the Estonian register of securities under an administrative agreement with the state. The latter option is voluntary and quite unpopular as it is used only by 1.7 % of OÜs in Estonia. This means that most of the shareholder ledgers are administered by management boards. This coincides with the dominant practice in other European countries such as, for instance, the UK, Sweden, Finland, Latvia, Germany, the Netherlands and Denmark.[45]

---

[42] Ibid, p. 2.
[43] Ibid, p. 1.
[44] Ibid, pp. 1–2.

3.2. ROLE OF COMMERCIAL REGISTER

The Commercial Register (CR) is for information purposes replicating majority of the ledger data directly from the source or the notaries. The national and regional[46] law does not obligate CR to record this data. The data entered into the CR about the shareholders[47] has (i) no legal meaning, (ii) no constitutive value and (iii) cannot be relied on by third parties as binding.[48]

3.3. CSD-ADMINISTERED SHAREHOLDER LEDGER

The possibility to register OÜ´s shares in the CSD and to allow the shareholder ledger to be administered by CSD was introduced already in 2001.[49] In 2017 CSDR transposition opened the market to multiple CSDs.[50] The goal of the CSD was to ensure that there would be unity and truthfulness of data. CSD data serves as a source of positive and negative trust. Positive trust means that a person in good faith can trust the data on the securities account is correct, while negative trust means that a person in good faith can trust that the rights that are not represented on the securities account do not exist.[51] In case shares of an OÜ are registered at CSD no shareholder ledger is maintained by the management board.[52] The registration, which is subject to multiple fees, is voluntary and very rarely used.

The ledger maintained by the CSD is a public ledger and falls under the definition of a "database" under the Public Information Act[53] (IPA).

---

[45] Ministry of Justice. (2018) *Ühinguõiguse revisjon Analüüs-konseptsioon* (Revision of Company Law), 15 September 2018. [online] Available from: https://www.just.ee/sites/www.just.ee/files/uhinguoiguse_revisjoni_analuus-kontseptsioon.pdf [Accessed 12 January 2019], p. 489.

[46] According to Articles 14 and 16 of the Directive 2017/1132 there is no disclosure obligation regarding shareholders in commercial registries of the Member States. Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law (Text with EEA relevance). *Official Journal of the European Union* 169, 30 June 2017, pp. 46–127. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017L1132 [Accessed 20 May 2019].

[47] Section 144(1) point 31) of CC.

[48] Case no 3-2-1-163-11 (2012), Estonian Supreme Court (Civil Chamber), 22 February 2012, para. 33; Case no 3-2-1-133-11 (2011), Estonian Supreme Court (Civil Chamber), 14 December 2011, para. 24; Saare, K. et al, Ühinguõigus I, Juura, 2015, pp. 53–54.

[49] *Estonian Central Register of Securities Act* (Eesti väärtpaberite keskregistri seadus) 2001. Estonia: Riigi Teataja (State Gazette). RT 2000, 57, 373, in Estonian.

[50] *Securities Register Maintenance Act* (SRMA) (Väärtpaberite registri pidamise seadus) 2017. Estonia: Riigi Teataja (State Gazette). RT I, 26.06.2017, 1 in Estonian.

[51] Case no. 3-4-1-3-12 (2012) Estonian Supreme Court (Constitutional Review Chamber), 6 July 2012, para. 52.

[52] § 2(3) of SRMA.

The data therein must be more accessible than data maintained by management boards. According to IPA § 43[3]

> *"before the establishment of a database [...] the technical documentation of the database shall be approved by the Estonian Information System's Authority, the Data Protection Inspectorate and the Statistics Estonia".*

This means the IPA requires CSD maintained ledger to go through vigorous checks and certification by various authorities. Any CSD wishing to use a DLT-based ledger application would have to go through the same checks and verifications.

Under the SRMA § 1[2] (2) the CSD is a database belonging to the state information system. In essence the CSD ledger must comply with the three--level IT baseline security system.[54] The CSD ledger needs to be centrally controlled as the obligated subject must enter into an agreement with the state to maintain the ledger. Similarly, any DLT-based ledger application the CSD wishes to use needs to be operated also centrally and meet the IT baseline security system requirements.

Further from the technical requirements, the registration of shares in CSD requires the existence of a securities account with the CSD for every shareholder, which presumes the opening of a bank and securities account by an account operator[55] such as a bank. As of 1 January 2019 as a solution to the overall difficulty of opening the necessary accounts due to AML concerns there is also an option for the OÜ to open a deposit account with the CSD for an additional fee in the name of the shareholder. In addition, professional participants have the right to open a nominee account for holding the shares for and on behalf of another person.[56] Therefore, the CSD's role is to merely aggregate the data recorded on the securities, deposit and nominee accounts to represent this on the centralised shareholder ledger and also send the data to CR.

---

[53] *Public Information Act* (Avaliku teabe seadus) 2001. Estonia: Riigi Teataja (State Gazette). RT I 2000, 92, 597, in Estonian.

[54] State Information System Website. Available from: https://www.ria.ee/en/cyber-security/it-baseline-security-system-iske.html [Accessed 02 June 2019].

[55] Account operator is a professional participant in the Estonian securities market, *Eesti Pank* (Central Bank of Estonia), an investment firm, credit institution, operator of the regulated market or operator of a securities settlement system registered in a Member State or in a third country in case of further pre-conditions. SRMA § 11(1), SRMA § 11(1).

[56] SRMA § 6(1) and (2).

Similar aggregation of data into CR could be also done with ledgers operating on DLT. Yet, the DLT-based ledgers would most likely be able to offer more flexibility in opening wallets or accounts to users as these DLT-applications would not have as strict AML requirements as banks on which the CSD system depends upon.

3.4. LEDGERS MAINTAINED BY MANAGEMENT BOARDS

The shareholder ledger maintained by the management board is not a public ledger. The regulation on the management board-administered ledger does not prescribe that it must be in any particular media or form and therefore, it can be in any media or form and using any technology applications chosen by the management board.

According to notaries and legal practitioners, standard practice demonstrates that management boards do not actually administer shareholder ledgers at all or do it in oral form.[57] As non-CSD-registered share transfer transactions need to be authenticated by the notary, the practise shows that prior to authentication of the transaction the notaries merely copy shareholder data off the CR and ask the management board to confirm it with signature. This is a somewhat risky practice as the CR also updates its data based on annual reports and that could make CR data incorrect.[58]

To mitigate this risk there is common, yet, unnecessary[59] practice among notaries to verify the CR data by requiring the seller to submit a copy of the share acquisition transaction document.[60] The only plausible risk the notary actually needs to mitigate is that there has not been another transaction that has not yet been reported to the CR as according to the law the notaries have to report transactions within two working days. However,

---

[57] Alekand A. (2015) Osaühingu osanikeregistri pidamine. *Juridica* I 2015, p. 10. Available from: https://www.juridica.ee/article_full.php?uri=2015_1_osa_hingu_osanikeregistri_pidamine&pdf=1 [Accessed 04 January 2019].

[58] The data will be entered on the basis of share transfer notice, share capital increase or decrease resolution by shareholders or on the basis of the shareholder ledger appended to annual report. Ibid, p. 13. See also Decree of the Minister of Justice no 60 (2012), Statute of the registry department of the court (*Kohtu registriosakonna kodukord*), 19 December 2012, RT I, 28. 12. 2012, 10.

[59] It is unnecessary as notaries themselves can check the source of the entry into CR and do not have to double-check the previous transaction documents.

[60] The system is even more bureaucratic due to the practice that if the same notary who is about to authenticate the planned transaction has authenticated also the previous transaction reported to the Commercial Register then the notary will demand the seller to still submit the copy of the previous transaction document and not check it themselves from their notarial register of documents.

this risk is not mitigated by requesting the acquisition document from the seller, but would rather be mitigated in case transactions would be recorded in the ledger instantaneously with a technological application such as for example DLT.

3.5. DIFFERENCES IN SHARE TRANSFERS

There are differences in share transfer rules depending on whether the shares are registered or not registered at CSD.

3.5.1. LEDGER ADMINISTERED BY MANAGEMENT BOARD

For the transfer of non-CSD registered shares there is a limitation of the principle of freedom of form[61] as notary authenticated transactions are required for both the obligations constituting contract and the real right contract.[62] The required notarial authentication can only be done by an Estonian notary practicing in Estonia and not by a notary in any other jurisdiction of the world.[63] The primary aim of establishing the authentication requirement for share transfer transactions of OÜs was to guarantee legal certainty.[64] Should the parties to a transaction fail to comply with the statutory notarial authentication form requirement, the transaction is void.[65]

The notarial authentication requirement was not in the CC from the adoption of the CC as it was introduced in 1998.[66] Its initial absence was named as the *"single biggest minus of the Commercial Code"*[67] as entries of the shareholder ledger lacked credibility. According to the case-law of the Estonian Supreme Court, the aim of the notarial authentication requirement is not merely documenting a transaction (*evidentiary function*[68])

---

[61] Sein, K. Tehingu vorminõuded ja nende järgimata jätmise tagajärjed, *Juridica* VII 2010, p. 509; Section 77 (1) of the GPCCA. *General Part of the Civil Code Act* (Tsiviilseadustiku üldosa seadus) 2002. Estonia: Riigi Teataja (State Gazette), RT 2002, 35, 216, in Estonian (GPCCA); § 8(1) and § 11(1) of the *Law of Obligations Act* (Võlaõigusseadus) 2001. Estonia: Riigi Teataja (State Gazette) RT I 2001, 81, 487, in Estonian.

[62] Section 149(4) of CC.

[63] Section 82 of GPCCA, Section 56(4) of the Notarisation Act. *Notarisation Act* (Notariaadiseadus) 2001. Estonia: Riigi Teataja (State Gazette) RT I 2000, 104, 684, in Estonian.

[64] Sein, K. (2010) Op. cit., p. 509.

[65] § 83(1) of GPCCA.

[66] Explanatory memorandum (744 SE) to the Act amending Commercial Code, Non-Profit Associations Act, Foundations Act and acts related to the above *Äriseadustiku, mittetulundusühingute seaduse, sihtasutuste seaduse ning nendega seotud seaduste muutmise seaduse eelnõu 744 SE seletuskiri*, 15 December 1997 (Explanatory memorandum (744 SE)).

[67] Explanatory memorandum (744 SE), op. cit.

[68] Sein, K. (2010) Op. cit., p. 509.

and identifying the parties thereto (*identification function*), but also the protection of the parties (*warning function*[69]) themselves against rushed and hastily made transactions. The court has explained that the form requirement is there also to warn the parties and explain the legal consequences of the transactions to the parties (*consulting function*[70]).

Last but not least, notaries tasked to authenticate share transfer transactions can refuse to authenticate the transaction in case sufficient data of user´s marital status, consent of spouse, property regime, acquisition document originals or any verified data on seller and buyer (in case of legal entities – registry card, certificate of good standing and incorporation) required by the notary are unavailable. This seriously hampers the liquidity of the shares and creates a subjective judgement linked obstacle to share transfer transactions that the type of transactions should already be able to overcome.

Any ledger operated on DLT certainly fulfils the *evidentiary function* as it reflects the execution of any transaction. The use of the DLT-based ledger could also enable the *identification function* on the basis of similar KYC requirements as applicable to custodial wallet and virtual currency exchange service providers under the 5th AML Directive.[71] The *warning functionality* could be also built in the form of "click-the-box" if you understand the consequences of the transaction, but it is not comparable to warning function of the notary. However, the only function that would not be enabled at all with DLT-based system is the *consulting function*.

3.5.2. LEDGERS ADMINISTERED BY CSD

In the case of CSD-registered shares there is no form requirement for share tranfer transaction and freedom of form prevails.

---

[69] Case no 3-2-1-49-03, Case no 3-2-1-85-04 (2004), Estonian Supreme Court (Civil Chamber) 6 September 2004.

[70] According to Section 18(1) of the Notarisation Act *"the notary shall also explain to parties the meaning and legal consequences of the transaction and the different possibilities for entry into the transaction"* and *"the notary shall ensure that errors and doubts are precluded and the rights of inexperienced or incompetent parties are not damaged"*. See also Case no 3-2-1-49-03 (2003), Estonian Supreme Court (Civil Chamber) 13 May 2003; Case no 3-2-1-127-03 (2003), Estonian Supreme Court (Civil Chamber) 10 November 2003; Case no 3-2-1-141-14 (2015), Estonian Supreme Court (Civil Chamber), 28 January 2015, paras. 34–35.

[71] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU. *Official Journal of the European Union* 156, 19 June 2018, pp. 43–74 (5th AML Directive). Available from:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L0843 [Accessed 30 May 2019].

The primary requirements for CSD-registered share transfers come from the SRMA and its implementation acts regarding securities transfers. The order to transfer the share is given either in writing[72] or electronically[73]. When an order is given to a securities account administrator, it must perform the following tasks: (i) identification of client (*identification function*) and (ii) AML checks (e.g. inquiry into buyer´s source of funds). The securities account operator does not check the existence of the transaction constituting the obligation or the real right contract and therefore, fulfils the *evidentiary function* only to a limited extent, as similarly to DLT-application based ledger, it merely sees the execution transaction intermediated by the account operator.

Similarly to any DLT-based ledger the account operator[74] in case of CSD--registered shares is not obligated to perform any *consulting* or *warning function*.[75] Hence, if the legislature did not see it necessary to require the fulfillment of these functions for CSD-registered share transactions, it should also be acceptable for the legislature that the DLT-based ledger solution fails to fulfil these functions.

3.5.3. CONSTITUTIVE VALUE OF THE LEDGER ENTRY

It is important to note that under the CC neither the entry in the shareholder ledger maintained by the management board nor the replication of data at CR have constitutive value. Only the entry into CSD has constitutive value and is the basis for good faith acquisition of a share.[76]

Under the CC, the transfer of a share is deemed effected and a share is deemed to have transferred with respect to the OÜ in case the management board has been notified of the transfer of the share and received evidence thereof.[77] Thus, even if the management board never amends the shareholder ledger according to the new *status quo*, from the company´s perspective the share still has already transferred and the ledger reflects the shareholder status incorrectly.

---

[72] GPCCA § 78(1).
[73] GPCCA § 80(2).
[74] Sein, K. (2010) Op.cit., p. 513.
[75] Alekand, A. (2015) Op. cit., p. 14.
[76] § 9(2) of SRMA.
[77] § 150(1) of CC.

Secondly, there is no constitutive value also in the entry of the shareholder data in the CR. This fact, however, decreases the value of the rest of the data recorded in the CR. If a third party cannot trust one data item in the CR why should it trust another.[78] The *status quo* has created confusion also among courts themselves who have incorrectly relied on the CR shareholder data.[79]

Similarly to entries into CSD, the DLT-based ledger entries could enjoy constitutive value as again similarly to CSD the ledger entry is the result of a verified and immutable record of transaction that is secured by transparency of the ledger and its protocol.

3.6. REFORM IDEAS

In 2014, the Estonian *Ministry of Justice* initiated a company law codification project and by 2018 a working group was established by the Ministry that issued an analysis-concept paper[80] providing an overview of identified shortcomings, relevant regulation in comparative jurisdictions and their suggestions for revision.

Coinciding with proposals made by the Estonian start-up community[81] and the *Estonian Bar Association*[82], the company law revision included a suggestion to ease the obligatory notarial authentication form requirement for non-CSD-registered share transfer transactions (both the obligation-constituting and the real right contract).[83]

The working group stated that most of the jurisdictions they looked at in their analysis for the purposes of comparison (i.e. Finland, Sweden, Latvia, Lithuania and Delaware) did not have an obligatory share transfer form requirement at all or there was merely written form for a real right

---

[78] Kõve, V. (2013) Kas kinnistusraamatu ja teiste kohtulike registrite korraldus vajab reformi? (*Does the Public Title Book and other court register organization demand a reform?*). *Juridica* VII 2013, p. 461 Available from: https://www.juridica.ee/article_full.php?uri=2013_7_kas_kinnistusraamatu_ja_teiste_kohtulike_registrite_korraldus_vajab_reformi_&pdf=1 [Accessed 10 January 2018].

[79] Ibid., p. 461. See also Case no 3-2-1-133-11, Estonian Supreme Court (Civil Chamber), 14 December 2011, para. 24; Case no 3-2-1-163-11, Estonian Supreme Court (Civil Chamber), 22 February 2012, para. 33.

[80] Ministry of Justice. (2018) Op. cit.

[81] Äripäev. (2019) Õiguskomisjon tahab välisinvesteeringute kaasamist lihtsustada. *Äripäev*, 9 September 2019. [online] Available from: https://www.aripaev.ee/uudised/2019/09/09/oiguskomisjon-tahab-valisinvesteeringute-kaasamist-lihtsustada?fbclid=IwAR1XjLS2xr96vXKvdP6B-IF7hl1e11atM9zVxHmGR52GhBHWf4uMYj4xjTw [Accessed 20 September 2019]

[82] Ibid.

[83] Ibid, pp. 13–14.

contract (in the UK and Denmark).[84] Of the compared jurisdictions Germany was the only one that had the obligatory notarial authentication requirement for obligation-constituting contracts and real right contracts, while the Netherlands and Luxembourg had the same requirement only for real right contracts. The working group is not suggesting to entirely abolish the obligatory form requirement, but does propose a more flexible solution. The obligation constituting transaction could be form-neutral while the prescribed form for real right contract should either be notarial certification[85] or the electronic form[86] instead of notarial authentication.

This idea of the working group should, however, be viewed together with a more stringent solution suggested for the shareholder ledgers. The idea of easing the form requirement for share transactions is linked to the suggestion of replacing the format-neutral shareholder ledger system with a notaries´ monopoly to administer shareholder ledgers.[87] The reasoning is understandable – reliability of the shareholder ledger entries. In summary, the idea of the working group is either to replace both of the current shareholder ledger administration alternatives – the CSD and management board – or merely to replace the latter with a notary--administered ledger solution.

In this context the legislature should also consider innovative technology solution (e.g. DLT) based ledger operators as possible gatekeepers in addition to notaries and CSDs. The legislature could introduce standards the ledger administrators would have to meet in order to maintain the ledger. This means the legislature does not have to necessarily introduce DLT-specific amendments like Delaware or France did, but instead should assess how to secure competition of ledger administrators for the benefit of the market and how to support innovation of the ledger maintenance practise without compromising on values and needed functions.

---

[84] Ibid, p. 485.

[85] According to Section 80(2) of GPCCA – the notarial certification means that the transaction documents shall be prepared in writing and the signature of the person entering into the transaction shall be certified by a notary (identification function).

[86] Electronic form under Estonian law means the transaction is digitally signed and parties are identified under the electronic ID linked to the certificate of the digital signature (identification function).

[87] Ministry of Justice (2018) Op. cit., p. 119. Similar systems exist in Austria and Switzerland.

3.7. CONCLUSION

As a summary of this theoretical application of the DLT-based ledger to the concerns identified above, it is noteworthy to state that assuming the DLT-based ledger application used would not lose its core characteristics the entries in the ledger would be instantaneous, verified and immutable transactions which would ensure the reliability of the ledger data. There would be no need to duplicate the ledger data into CR, yet, it would be possible to continue it for the sake of one source for all shareholder data. There would be no need for the notaries to ask for previous transaction documents or distrust the chain of control as due to linked timestamping and cryptography employed in the technology, the application would ensure transparency and immutability. The DLT--based ledger operator could also fulfil identification obligations under 5th AML Directive as virtual currency exchange service providers do.

Generally speaking DLT's attractiveness lies in that (i) it allows for operating a transparent public ledger, (ii) the ledger is accessible globally and easily, (iii) the ledger is resistant to tampering and employs a consensus mechanism, (iv) the protocol underlying the ledger is also tamper-proof as everyone can constantly verify it, and (v) the transactions amending the status of the ledger are verified by nodes. A DLT-based shareholder ledger can either be using the infrastructure of permissioned or permissionless network. The application layer can be built on the core protocol of the network using its infrastructure, yet, its own private rules of accessibility. The network could include – on the basis of the Delaware example – CR (or any other state authority) as one of the nodes verifying the transactions.

4. TECHNOLOGY-NEUTRALITY IN LEDGER MAINTENANCE RULES

After a brief introduction of the technology-neutrality principle, the regulation portrayed in section 3 is analysed on the basis of the said principle in order to address the research question of the article.

4.1. TECHNOLOGY-NEUTRALITY PRINCIPLE

The technology-neutrality principle is a classical non-discrimination principle, which initially required offline and online world to be treated

equally.[88] The principle was adopted more widely in the nineties with the advent of the Internet. In legal acts the principle is included in Article 20 of the *Charter for Fundamental Rights*, defined in Recital 18 and Article 8 of the Framework Directive[89] (stating that regulation should neither impose nor discriminate in favour of the use of a particular type of technology) and supported by Recital 51 of NIS Directive[90], which forbids to require certain product

"to be designed, developed or manufactured in a particular manner".

The assessment model to check the compliance of regulation with the principle of technology-neutrality can be separated into the following components:

1. *Functional equivalence* – the legislature should not discriminate between different technology (e.g. offline and online modes) in case these technologies have the same or similar functions;
2. *Effects equivalence* – regulation must have in majority an equivalent effect across different technologies even if it requires to have technology-specific legislation in place.

The aim of the principle is also to future-proof regulation – so that regulation does not hinder or create obstacles to innovation, but also would not need constant amendment.[91]

Technology-neutrality includes also media-neutrality, which means that the rules per different media or format should have a similar effect on the media used for a similar function or aim.

---

[88] Reed, C. (2007) Taking Sides on Technology Neutrality. *SCRIPTed* 263 4(3) September 2007, pp. 263–284. [online] Available from: http://heinonline.org/HOL/P?h=hein.journals/scripted 4&i=281 [Accessed 01 June 2019].

[89] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive). *Official Journal of the European Union*, L 108, 24. 4. 2002, pp. 33–50.

[90] 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 (NIS Directive). *Official Journal of the European Union*, L 194, 19. 7. 2016, pp. 1–30.

[91] Koops, B.-J. (2006) Should ICT Regulation be Technology-Neutral? In: Bert-Jaap Koops et al. *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*. IT & Law Series. 9, pp. 77–108, The Hague: T.M.C. Asser Press 2006, p. 100.

4.2. IS THE CURRENT REGULATION TECHNOLOGY-NEUTRAL?

4.2.1. TECHNICAL REQUIREMENTS FOR THE LEDGERS

Although majority of ledgers are maintained by management boards, these ledgers are not trusted by third parties. Ledgers administered by management boards are decentralised ledgers, maintained by individual companies themselves in any form they see fit. The CSD and the CR are centrally administered ledgers with the registrar under the supervision of an authority and regarded as public databases.

The regulation on the management board-administered ledger is technology-neutral as the CC does not prescribe that it must be in any particular media or form and therefore, it can be in any media or form or using any technology applications chosen by the management board. Consequently, any technology – DLT or other – can be used to administer the ledger as the regulation does not prefer a technology over another. The regulation has a similar effect on any technology and treats equally technology that functions similarly. Such approach makes the regulation actually technology-independent as it does not consider technology at all and even presumes the non-existence of technology being primarily focused on the subject who maintains and not the mechanism how it is maintained.

The ledger maintained by the CSD has technical standards applicable to it, requirements stemming from the law and public procurement terms. For the purposes of this article it is clear that any technological application the CSD wishes to use that is based on DLT needs to be separately assessed based on the applicable requirements. Due to the low usage of the CSD alternative in Estonia, it is not within the scope of this article to assess whether these requirements applicable to CSD are technology-neutral.

4.2.2. SHARE TRANSFER REGULATION

The differences of share transfer formalities on the basis of shareholder ledger maintenance begs the question: *Why is there different treatment of shares and shareholders depending on the administrators they use?* This question is based on the logic that CSD-registered share transfer transactions are form-neutral, while non-CSD transactions are not. In case of CSD-registered shares the transfer transaction form does not secure the fulfilment of any *consulting* or *warning function*. Also the *evidentiary function* is fulfilled only to a limited extent. Consequently, shareholders receive different protection by the regulation as it depends on the choice

of administrator of the legal entity´s shareholder ledger. It can be concluded that the form requirement differences are discriminatory towards non-CSD--registered shares and it is fair to conclude that the legislature simply does not consider *consultation* and *warning function* a necessary aspect of share transfer transactions for all shareholders across the board but requires these to be fulfilled only in case of non-CSD-registered share transfer transactions.

The irony in all this is that shareholder data ends up in the CSD on the basis of an application of the management board – the same management board who according to notary´s practise cannot be trusted to submit correct data about shareholders and shares. Therefore, the claim that the CSD ledger data is in any way more trustworthy than management board ledger data is incorrectly based on the assumption that the data is somehow checked by the CSD when the management board registers the shares at the CSD. In truth, the shareholder data is not checked against any reliable source in any way by the CSD when the registration application is submitted by the management board. The mere fact that the shares are registered at the CSD does not make the data submitted there more reliable. However, any transactions executed that follow from the moment of registration are verified and parties of the transaction identified by the account operators.

It is fair to conclude that the differences of the share transfer requirements are administrator-specific and technology-independent, meaning that the rules do not care about how but rather about who. This means there exists a prejudice against ledgers maintained by management board irrelevant of the functions the ledger enables. On the one hand, the CSD ledger solution is carefully vetted by the state as part of a public procurement tender process for ledger maintenance, but on the other hand, the solutions used by the management boards for the same aim are not differentiated at all.

This is where the technology-independence actually works against the management boards as they should also be able to vet the solution they use for ledger maintenance. In short, this means that in case management boards would maintain shareholder ledgers using a technology that could at least fulfil *identification function* and up to a level *evidentiary function* similar to CSD – the share transfer transaction requirements applicable should be differentiated so that there would be effects equivalence among

the alternative share ledger maintenance models (CSD and management board).

The effect of the existing regulation is discriminatory towards any technological solution used by the management board for ledger maintenance that enables the same functions as the CSD as such solution would not enjoy the same benefits of ease of liquidity as the CSD solution (form-neutral share transactions).

On the basis of principle of technology-neutrality the regulation should have the same or similar effect if there is functional equivalence of technology used. The fair application of this principle would demand the regulator to allow the management board to vet the solution used by it in order to establish whether its functionalities would make it possible for it to forgo the obligatory share transfer form of notarial authentication.

4.2.3. ARE THE REFORM IDEAS TECHNOLOGY-NEUTRAL?

The working group addressing the codification challenge has suggested that the shareholder ledger should be maintained solely by notaries. However, they would not operate as a separate ledger, but instead the notaries would be the gatekeepers of ledger data entered into the CR. Ledger data would be accessible through CR (through entries by notaries) or quite possibly also by CSD as the voluntary alternative, which would be also duplicated in the CR.

The suggested solution would centralise the administration of all shareholder ledger data into the hands of human intermediaries (i.e. notaries) and would, therefore, have a monopolising effect. In that case no technology use, however rich in functions, would be sufficient for ledger maintenance. Any such amendment of company law would have a negative effect on technology-neutrality and the use of any new technology, incl. DLT, for shareholder ledger administration as it would not allow any decentralized ledgers or gatekeepers at all.

A technology-neutral solution would be to enlist the functionalities the ledger needs to enable, the data categories it needs to collect and enable or even require these ledgers to send (or allow aggregation) of the ledger data into CR irrelevant of who is maintaining it (company itself or outsourcing the service). This would allow the management boards (by using market-developed and -led solutions), the CSDs (national or cross-border service providers) and notaries (hopefully not only

Estonian) to function as gatekeepers of trustworthy, reliable and constituent shareholder ledger data that could be all aggregated into the CR in order to ease the consumption of the shareholder data by using one comprehensive data source.

This solution does not necessarily require that the solution used by management boards needs to be DLT-based, but it can be. It also does not mean the CR needs to duplicate the ledger data, but if the concern is the loss of unity of data as it is scattered around multiple sources, then this concern can be also addressed. All in all it means the regulator should think of ways to implement minimum technical standards set out in technology--neutral guidelines rather than centralizing the privilege to operate as an administrator with measures that support technology-independency and in effect do not grant technology a fair chance to prove that it is ready to replace some functions of humans (in this case notaries) without jeopardizing any of the functions the regulator wished to enable.

5. CONCLUSIONS

The article examined whether one could make use of new technological solutions, such as DLT, for administering a shareholder ledger of an OÜ in Estonia by applying technology-neutrality principle on the current regulation. Regarding the question of whether the use of DLT is allowed in ledger administration, the answer is at least partly affirmative. The legal rules in force regarding ledger administration by management boards are technology-neutral and do not give preference to or discriminate against any technology or medium.

The current technical requirements for ledger maintenance by management board are very light, yet the share transfer requirements are very strict. Even if the management board would voluntarily meet higher technical standards in ledger maintenance, this would not ease the strict share transfer form requirements. This means that the law does not recognize any technological solution the management board may use as fulfilling similar functions met by the technical solution used by CSD. The management board administered ledger is suffering a substantial disadvantage in comparison to CSD ledger due to share transfer form requirements (notarial authentication rule) and without any change in regulation a DLT-based ledger would suffer the same disadvantage. The codification working group suggestions aggravate the situation even

further as accepting these would mean there is no decentralized ledger alternative anymore.

The effect of the current regulation is that there can be no alternative to CSD that could enjoy the ease of transfer and liquidity similar or even more advanced than CSD enjoys. All alternatives to CSD would have the same hindrances and obstacles to liquidity as the ledgers maintained by management boards under current regulation. The core separation between CSD and all alternatives is that CSD is a centralized ledger and management boards maintain decentralized ledgers. In order to comply with the technology-neutrality principle, the legal rules should be unified and made non-discriminatory from the point of view of decentralised and centralized ledger systems plus irrespective of the administrator of these systems. Such a change would allow the use of DLT for ledger maintenance purposes enjoying both access to and liquidity of the DLT-based networks and assets listed there enjoy. Consequently, amendments in regulation are needed to ensure technology-neutrality by implementing technical standardisation requirements and whichever ledger solution meets these can enjoy the same share transfer form freedom as CSD-registered shares. Alternative solution would be to introduce DLT-specific amendments to give DLT-based ledger maintenance applications that meet certain technical standards (similar to Delaware, US example) equal status with CSD-ledgers (as granted by the French DLT Order). Yet, it is not necessary to construct DLT-specific legislation as in the State of Delaware and France as also a more general approach could be introduced with either market-led or state-instituted technology-neutral standards or guidelines for all gatekeepers of shareholder ledgers.

The law should grant share transfer form freedom to any technological or human solution that through testing or validation process proves it fulfils the same functions as required for CSD share transfers. This could of course also mean that IT baseline security system requirements could be applied to these technological solutions, but these requirements should apply in a technology-neutral way.

In responding to the research questions the author also recognises that the pace of technological innovation is accelerating immensely. The way legislature has coped with technological innovation thus far has been through introducing technology-neutral regulation that would not create hindrances or obstacles to new technologies or their use cases. However,

the pace of innovation makes it difficult for any legislature to cope with technology-neutrality principle as any change of technological innovation could challenge the neutrality of the regulation all over again. This is because technology-neutrality sometimes requires the introduction of amendments to *ex ante* laws in order not to exclude innovative business models or technology uses the same treatment as granted to as existing technology. Exactly this aspect of the principle of technology-neutrality is ever more difficult to address due to a "pacing problem" which means that

> *"technological innovation is increasingly outpacing the ability of laws and regulations to keep up"*.[92]

The pacing problem is further intensified by the "knowledge problem",[93] which in the 21st century is no longer linked to insufficiency of information, but rather to overflow of information and the difficult task of understanding what information about technology is relevant for the legislature understand in order to create technology-neutral regulation.

The Estonian company law revision working group did not examine DLT as part of their analysis, which indicates the existence of a "pacing problem". Although any new technology could be a solution to the concerns of the current ledger administration system, the legislature and the working group procured with the codification task was not yet ready to assess the nascent technology´s possible effects on the current practice. This means it is up to legal scholars to identify the problems the current regulation has in the context of technology-neutrality and suggest solutions in order to allow also new technology – DLT or any other – to be used in administrating shareholder ledgers in a meaningful way.

LIST OF REFERENCES

[1] Alekand A. Osaühingu osanikeregistri pidamine, *Juridica* I 2015. [online] Available from: https://www.juridica.ee/article_full.php?uri=2015_1_osa_hingu_osanikeregistri_pidamine&pdf=1 [Accessed 04 January 2019].

[92] Thierer, A. (2018) The Pacing Problem, the Collingridge Dilemma & Technological Determinism. [blog entry] *The Technology Liberation Front blog* (16 August 2018). Available from: https://techliberation.com/2018/08/16/the-pacing-problem-the-collingridge-dilemma-technological-determinism/ [Accessed 27 January 2019].

[93] Ibid, p. 37.

[2] Allison, I. Smart securities issuer Symbiont fires shots in the private blockchain arms race. *International Business Times*, 28 September 2015. Available from: https://www.ibtimes.co.uk/smart-securities-issuer-symbiont-fires-shots-private-blockchain-arms-race-1521449 [Accessed 08 May 2018].

[3] Case no 3-2-1-133-11 (2011), Estonian Supreme Court (Civil Chamber), 14 December 2011.

[4] Case no 3-2-1-141-14 (2015), Estonian Supreme Court (Civil Chamber), 28 January 2015.

[5] Case no 3-2-1-163-11 (2012), Estonian Supreme Court (Civil Chamber), 22 February 2012.

[6] Case no 3-4-1-3-12 (2012), Estonian Supreme Court (Constitutional Review Chamber), 6 July 2012.

[7] Chamber of Notaries. (2018) Notarite Koja arvamus ühinguõiguse revisjoni muudatusettepanekute kohta (*Opinion to the analysis-concept paper of company law revision working group*), 17th December 2018. [online] Available from: https://www.just.ee/sites/www.just.ee/files/notarite_koja_arvamus_18.12.2018.pdf [Accessed 12 January 2019].

[8] Clifford Chance (2017). France pioneers blockchain legal framework for unlisted Securities, Briefing Note. [online] Available from: https://www.cliffordchance.com/content/dam/cliffordchance/PDFDocuments/Client%20Briefing%20-%20France%20-%20Blockchain%20for%20unlisted%20securities%20180750-4-2....pdf [Accessed 08 May 2018].

[9] Collingridge, D. (1981) *The Social Control of Technology*. Open University Press.

[10] *Commercial Code* (Äriseadustik) 1995. Estonia: Riigi Teataja (State Gazette). RT I 1995, 26, 355, in Estonian. English translation available from: https://www.riigiteataja.ee/en/eli/507012019006/consolide [Accessed 09 February 2019].

[11] ConsenSys. (2018) Wyoming Passes 5 Pro-Blockchain Laws, Points the Way in Digital Asset Regulation (15 March 2018). Available from: https://media.consensys.net/wyoming-passes-5-pro-blockchain-laws-points-the-way-in-digital-asset-regulation-6fae9e07d129 [Accessed 27 January 2019].

[12] Cuccuru, P. (2017) Beyond bitcoin: An early overview on smart contracts. *International Journal of Law and Information Technology*, 25 (3). [online] Available from: https://doi.org/10.1093/ijlit/eax003 [Accessed 30 May 2018].

[13] De Filippi, P., Wright A. (2018) *Blockchain and the Law: The rule of code*. Harvard University Press.

[14] Decree of the Minister of Justice no 60. (2012) Statute of the registry department of the court (*Kohtu registriosakonna kodukord*), 19 December 2012, RT I, 28. 12. 2012, 10.

[15] Delaware State Senate 149th General Assembly Senate Bill No. 69. An act to amend title 8 of the Delaware Code Relating To The General Corporation Law. [online] Available

from: https://legis.delaware.gov/json/BillDetail/GenerateHtmlDocument?legislationId=25730&legislationTypeId=1&docTypeId=2&legislationName=SB69 [Accessed 07 May 2018].

[16] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive). *Official Journal of the European Union*, L 108, 24. 4. 2002.

[17] Directive 2009/101/EC of the European Parliament and of the Council of 16 September 2009 on coordination of safeguards which, for the protection of the interests of members and third parties, are required by Member States of companies within the meaning of the second paragraph of Article 48 of the Treaty, with a view to making such safeguards equivalent (Text with EEA relevance). OJ L 258, 1. 10. 2009.

[18] 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 (NIS Directive). *Official Journal of the European Union*, L 194, 19. 7. 2016.

[19] Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law (Text with EEA relevance). OJ L 169, 30. 6. 2017.

[20] *Estonian Central Register of Securities Act* (Eesti väärtpaberite keskregistri seadus) 2001. Estonia: Riigi Teataja (State Gazette). RT 2000, 57, 373, in Estonian. English translation available from: https://www.riigiteataja.ee/en/eli/ee/519112013006/consolide [Accessed 09 February 2019].

[21] European Commission (2019). Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions FinTech Action plan: For a more competitive and innovative European financial sector. Brussels, 8. 3. 2018 COM(2018) 109 final (9 January 2019). Available from: https://eur-lex.europa.eu/resource.html?uri=cellar:6793c578-22e6-11e8-ac73-01aa75ed71a1.0001.02/DOC_1&format=PDF [Accessed 23 January 2019].

[22] Explanatory memorandum (744 SE) to the Act amending Commercial Code, Non-Profit Associations Act, Foundations Act and acts related to the above *Äriseadustiku, mittetulundusühingute seaduse, sihtasutuste seaduse ning nendega seotud seaduste muutmise seaduse eelnõu 744 SE seletuskiri*, 15 December 1997. Available from: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/cf759bd3-97aa-310b-bb84-4bc734d83249/%C3%84riseadustiku,%20mittetulundus%C3%BChingute%20seaduse,%20sihtasutuste%20

seaduse%20ning%20nendega%20seotud%20seaduste%20muutmise%20seadus [Accessed 07 January 2019].

[23] *Family Law Act* (Perekonnaseadus). 2009 Estonia: Riigi Teataja (State Gazette) RT I 2009, 60, 395, in Estonian. English translation available from: https://www.riigiteataja.ee/en/eli/507022018005/consolide [Accessed 09 February 2019].

[24] *General Part of the Civil Code Act* (Tsiviilseadustiku üldosa seadus) 2002. Estonia: Riigi Teataja (State Gazette), RT 2002, 35, 216, in Estonian. English translation available from: https://www.riigiteataja.ee/en/eli/502012019003/consolide [Accessed 09 February 2019].

[25] Guardtime (2019). [online] Available from: https://guardtime.com/technology [Accessed 14 January 2019].

[26] Koops, B.-J. (2006) Should ICT Regulation be Technology-Neutral? In Bert-Jaap Koops et al. *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*. IT & Law Series, 9. The Hague: T.M.C. Asser Press, 2006.

[27] Korjus, K. (2017) *Welcome to the blockchain nation*. [blog entry] Medium Blog (7 July 2017). Available from: https://medium.com/e-residency-blog/welcome-to-the-blockchain-nation-5d9b46c06fd4 [Accessed 20 January 2019].

[28] Kõve V. (2013) Kas kinnistusraamatu ja teiste kohtulike registrite korraldus vajab reformi? *Juridica* VII 2013. Available from: https://www.juridica.ee/article_full.php?uri=2013_7_kas_kinnistusraamatu_ja_teiste_kohtulike_registrite_korraldus_vajab_reformi_&pdf=1 [Accessed 01 January 2018].

[29] *Law of Obligations Act* (Võlaõigusseadus) 2001. Estonia: Riigi Teataja (State Gazette) RT I 2001, 81, 487, in Estonian. English translation available from: https://www.riigiteataja.ee/en/eli/508082018001/consolide [Accessed 09 February 2019].

[30] *Law of Property Act* (Asjaõigusseadus) 1993. Estonia: Riigi Teataja (State Gazette) RT I 1993, 39, 590, in Estonian. English translation available from: https://www.riigiteataja.ee/en/eli/502012019009/consolide [Accessed 09 February 2019].

[31] Long, C. (2018) *Blockchain crosses the Delaware*. [blog entry] Mediamarkets blog, 31 July 2018. Available from: https://www.marketsmedia.com/blockchain-crosses-delaware/ [Accessed 07 May 2018].

[32] Lucking, D. (2017) *Delaware Passes Law Permitting Companies to Use Blockchain Technology to Issue and Track Shares*. Allen & Overy publications, 26 September 2017. [online] Available from: http://www.allenovery.com/publications/en-gb/Pages/Delaware-Passes-Law-Permitting-Companies-to-Use-Blockchain-Technology-to-Issue-and-Track-Shares-.aspx [Accessed 05 May 2019].

[33] McCorry, P., Hicks, A., and Meikeljohn, S. (2018) Smart contracts for bribing miners. *Conference Proceedings The 5th Workshop on Bitcoin and Blockchain Research,* 2nd March 2018. Available from: https://fc18.ifca.ai/bitcoin/schedule.html [Accessed 03 May 2018].

[34] Ministry of Justice. The Draft Core Assignment of the Codification of Company Law (*Ühinguõiguse kodifitseerimise lähteülesande projekt*), 2014. Available from: https://www.just.ee/sites/www.just.ee/files/uhinguoiguse_kodifitseerimise_lahteulesande_projekt_0.pdf [Accessed 12 January 2019]

[35] Ministry of Justice. (2018) Revision of Company Law, Analysis-Concept Paper (*Ühinguõiguse revisjon Analüüs-konseptsioon*), 15 September 2018. [online] Available from: https://www.just.ee/sites/www.just.ee/files/uhinguoiguse_revisjoni_analuus-kontseptsioon.pdf [Accessed 12 January 2019].

[36] Nakamoto, S. (2008) *Bitcoin: Peer-to-peer Electronic Cash System*. [online] Available from: https://bitcoin.org/bitcoin.pdf [Accessed 12 April 2018].

[37] Nicholson, G. (2019) Wyoming Proposes Bill for Issuance of Tokenised Certificates with Stocks. *TokenMarket* (17 January 2019). Available from: https://tokenmarket.net/news/regulation/wyoming-proposes-bill-issuance-tokenised-certificates-stocks/ [Accessed 23 January 2019].

[38] O'Toole, M. J., Reilly, M. K. (2017) The First Block in the Chain: Proposed Amendments to the DGCL Pave the Way for Distributed Ledgers and Beyond. *Harvard Law School Forum on Corporate Governance and Financial Regulation*, 16 March 2017. Available from: https://corpgov.law.harvard.edu/2017/03/16/the-first-block-in-the-chain-proposed-amendments-to-the-dgcl-pave-the-way-for-distributed-ledgers-and-beyond/#3 [Accessed 30 April 2017].

[39] Polner, G. et al. (2017) Delaware Approves Use of Blockchain in New DGCL Amendments. *Gibson Dunn Securities Regulation and Corporate Governance Monitor*. 31 July 2017. [online] Available from: http://securitiesregulationmonitor.com/Lists/Posts/Post.aspx?ID=299 [Accessed 07 May 2018].

[40] Proposal HB0185 Corporate stock-certificate tokens. [online] Available from: https://www.wyoleg.gov/Legislation/2019/HB0185 [Accessed 23 January 2019].

[41] *Public Information Act* (Avaliku teabe seadus) 2001. Estonia: Riigi Teataja (State Gazette). RT I 2000, 92, 597, in Estonian.

[42] Reed, C. (2007) Taking Sides on Technology Neutrality. *SCRIPTed* 263 4 (3), September. [online] Available from: http://heinonline.org/HOL/P?h=hein.journals/scripted4&i=281 [Accessed 11 April 2018].

[43] Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012 Text with EEA relevance. OJ L 257, 28. 8. 2014 (CSDR).

[44] Report to the President of the Republic relating to Ordinance No. 2017-1674 of 8 December 2017 on the use of a shared electronic registration device for the representation and transmission of financial securities, *Rapport au Président de la République relatif à l'ordonnance n° 2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers*. Published in JORF n°0287 du 9 décembre 2017 texte n° 23. [online] Available from: https://www.legifrance.gouv.fr/eli/rapport/2017/12/9/ECOT1729053P/jo/texte [Accessed 01 May 2018].

[45] Saare K. et al, *Ühinguõigus* I, Juura, 2015.

[46] Securities Register Maintenance Act (Väärtpaberite registri pidamise seadus) 2017. Estonia: Riigi Teataja (State Gazette). RT I, 26. 06. 2017, 1, in Estonian. English translation available from: https://www.riigiteataja.ee/en/eli/511012018001/consolide [Accessed 10 February 2019].

[47] Sein, K. Tehingu vorminõuded ja nende järgimata jätmise tagajärjed, *Juridica* VII/2010.

[48] Shaan, R. *The Difference Between Blockchains & Distributed Ledger Technology*. [blog entry] Medium Blog Towards Data Science. Available from: https://towardsdatascience.com/the-difference-between-blockchains-distributed-ledger-technology-42715a0fa92 [Accessed 01 May 2018].

[49] Song, W. (2018) Bullish on blockchain: examining Delaware's approach to distributed ledger technology in corporate governance law and beyond. *Harvard Law Review*. Available from: http://www.hblr.org/2018/01/bullish-on-blockchain-examining-delawares-approach-to-distributed-ledger-technology-in-corporate-governance-law-and-beyond/ [Accessed 07 May 2018].

[50] State Information System Website. [online] Available from: https://www.ria.ee/en/cyber-security/it-baseline-security-system-iske.html [Accessed 02 June 2019].

[51] Stromberg G. T. et al. (2018) Are Headwinds Hampering Delaware's Blockchain Initiative? *Law 360*, 23 March 2018. Available from: https://jenner.com/system/assets/publications/17844/original/stromberg%20Law360%20March%2023%202018.pdf?1521837416 [Accessed 14 January 2019].

[52] Thierer, A. (2018) The Pacing Problem, the Collingridge Dilemma & Technological Determinism. [blog entry] *The Technology Liberation Front blog* (16 August 2018). Available from: https://techliberation.com/2018/08/16/the-pacing-problem-the-collingridge-dilemma-technological-determinism/ [Accessed 27 January 2019].

[53] Veerpalu, A. (2018) Decentralised Technology and Technology Neutrality in Legal Rules: An Analysis of De Voogd and Hedqvist. *Baltic Journal of Law & Politics*, 11 (2). [online] doi: https://doi.org/10.2478/bjlp-2018-0011

[54] Wikipedia. (2018) *Corda.* [online] Available from: https://en.wikipedia.org/wiki/R3_(company)#Corda [Accessed 14 January 2018].

[55] Wikipedia. (2019) *Ethereum.* [online] Available from: https://en.wikipedia.org/wiki/Ethereum [Accessed 14 January 2019].

[56] Vocabulary of Computing (list terms, expressions and definitions adopted). *Vocabulaire de l'informatique (liste de termes, expressions et définitions adoptés)* published in JORF n°0121 du 23 mai 2017 texte n° 20. Available from: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000034795042&categorieLien=id [Accessed 01 May 2018].

[57] Äripäev. (2019) *Õiguskomisjon tahab välisinvesteeringute kaasamist lihtsustada*. Äripäev, 9 September 2019 [online]. Available from: https://www.aripaev.ee/uudised/2019/09/09/oiguskomisjon-tahab-valisinvesteeringute-kaasamist-lihtsustada?fbclid=IwAR1XjLS2xr96vXKvdP6B-IF7hl1e11atM9zVxHmGR52GhBHWf4uMYj4xjTw [Accessed 20 September 2019].

DOI 10.5817/MUJLT2019-2-7

IN THE PROCEDURAL SURROUNDINGS OF CONSUMER PROTECTION: ONLINE DISPUTE RESOLUTION, THE ADVERSARIAL PRINCIPLE, AND TENDENCIES TOWARD SETTLEMENT[*]

by

ERIK BJÖRLING[**]

The article builds on a pluralistic perspective on law and the understanding that legal research must take into account the procedural and institutional landscape where legal rights are enforced. In relation to online dispute resolution (ODR), two procedural mechanisms, namely the adversarial principle and the tendency toward settlements, are studied and discussed. The adversarial principle (argued to be integral to most ODR procedures) and tendencies toward settlements (also argued to be integral to most ODR procedures) are considered in relation to the overarching (and possibly contradictory) objectives of protecting individual consumer rights and the interest of increasing economic efficiency within the EU's internal market.

KEY WORDS

ADR, Adversarial Principle, Consumer Litigation, ODR, Procedural Law, Settlements

1. INTRODUCTION

Within European consumer law, the *European Commission* has been working actively for a number of years to resolve disputes in consumer cases through alternative dispute resolution formats. The efforts have been based on the key words simplicity, proportionality, justice, and efficiency, and

[*] The author would like to thank *Ragnars Söderbergs stiftelse* for making this article possible.

[**] erik.bjorling@law.gu.se, *Erik Björling* (LLD) is a researcher and teacher in the fields of procedural law and legal theory at the Department of Law, University of Gothenburg, Sweden.

the method is *alternative dispute resolution (ADR)*, and in a digital setting *online dispute resolution (ODR)*.[1] The sector in which ODR is expected to have an impact is immense. In the EU, consumer transactions account for more than 50 percent of the total gross domestic product.[2] About half of all EU consumers regularly shop over the Internet, and online sales are also the fastest growing type of sales in the EU.[3]

The most common legal conflicts related to consumer trade are what most people consider everyday legal types of conflicts such as delivery delays, damaged products, and products that do not arrive at all.[4] Dispute resolution in consumer-related disputes, both through court and alternative processes, however, is anything but an everyday issue. Rather, consumer processes are unusual and only two percent of all EU consumers who believe they have a reason to target a business continue on to some type of dispute resolution procedure. Studies show that even companies are cautious about using the court as a forum for consumer disputes.[5] Thus, there is a widespread reluctance to take conflicts that arise as a result of consumer consumption to judicial institutions. For disputes of lesser value, procedures that require the parties to meet face to face are simply not an option, especially in cross-border situations.[6] In addition, the methods of ordinary dispute resolution are quite varied and, in most cases, very cumbersome.[7]

Consumer protection within the EU is ensured by means of mandatory rules that strengthen the position of the consumer. Signals from among others the *Court of Justice of the European Union (CJEU)* indicate that these

---

1 Cortés, P. (2017a) *The Law of Consumer Redress in an Evolving Digital Market: Upgrading from Alternative to Online Dispute Resolution*. Cambridge: Cambridge University Press, p. viii.

2 European Commission. (2012) Communication from the commission to the European Parliament, The Council, The Economic and Social Committee and the Committee of the Regions: A European consumer agenda – Boosting confidence and growth. COM(2012) 225 final, p. 1.

3 Cortés, P. (2017a) *The Law of Consumer Redress in an Evolving Digital Market: Uppgrading from Alternative to Online Dispute Resolution*. Cambridge: Cambridge University Press, p. 4–5.

4 Ibid.

5 European Commission. (2011) Commission Staff Working Paper Impact Assessment Accompanying the document Proposal for a Directive of the European Parliament and of the Council on Alternative Dispute Resolution for consumer disputes (Directive on consumer ADR) and Proposal for a Regulation of the European Parliament and of the Council on Online Dispute Resolution for consumer disputes (Regulation on consumer ODR). SEC(2011) 1408 final, p. 13.

6 Cortés, P. (2017a) *The Law of Consumer Redress in an Evolving Digital Market: Upgrading from Alternative to Online Dispute Resolution.* Cambridge: Cambridge University Press, p. 2–4.

7 Commission staff working paper, p. 13.

rights are to be upheld *ex officio* by court officials across the EU.[8] However, since a very low number of conflicts between consumers and companies reach court proceedings, there is no forum, i.e. no institutional context, for actual enforcement of consumer protection. This is where the ADR and ODR initiatives are supposed to present an option. To enable easily accessible and efficient out-of-court redress for consumer disputes, including disputes arising from cross-border e-commerce, an extensive legal framework on ADR and ODR was adopted at EU level in 2013 and has been in place since 2016. The ODR as an initiative has its origin in the notion that civil courts for many years have failed to provide access to justice for ordinary individuals.[9] The idea behind the initiative is to give consumers access to a comprehensive landscape of ADR bodies. By doing this the *Commission* is hopeful that consumers will be able to solve disputes with companies that arise from online transactions in a simple, fast, and inexpensive way, while companies avoid costly litigation procedures and maintain good customer relations. In addition to this, it is also outspoken that ODR considers the interest of increasing economic efficiency within the internal market.[10] The importance of the ODR framework as a contributor to economic growth has been manifestly held forth by the *Commission*.[11]

The two legislative instruments comprising the described framework, the ADR Directive and the ODR Regulation, are interlinked and complementary.[12] The online dispute resolution platform (the *ODR*

---

[8] See, e.g. Judgement of 27 June 2000, Joined Cases *Océano Grupo Editorial SA v Roció Murciano Quintero and Salvat Editores SA v José M. Sánchez Alcón Prades and Others*, C-240/98 to C-244/98, ECLI:EU:C:2000:346, and Judgement of 4 June 2009, *Pannon GSM Zrt. v Erzsébet Sustikné Győrfi*, C-243/08, ECLI:EU:C:2009:350.

[9] *Cortés* makes this point referring to *Lord Justice Briggs*. See Cortés, P. (2017b) The Online Court: Filling the Gaps of the Civil Justice System? *Civil Justice Quarterly*, 36, pp. 109–126, p. 109.

[10] Cortés, P. (2017a) *The Law of Consumer Redress in an Evolving Digital Market: Upgrading from Alternative to Online Dispute Resolution.* Cambridge: Cambridge University Press, p. 2. The ODR platform is supposed to contribute to strengthening consumers' and companies' confidence in shopping and trading online both in their country and abroad.

[11] European Commission. (2012) Communication from the commission to the European Parliament, The Council, The Economic and Social Committee and the Committee of the Regions: A European consumer agenda – Boosting confidence and growth. COM(2012) 225 final, p. 1.

[12] Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR), Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR) (2013).

platform) – a website that channels complaints to ADR bodies – is the central node for the out-of-court framework that has been established. These ADR bodies (sometimes ODR entities) have been notified to the *Commission* by national authorities and must pass an assessment of their compliance with the quality requirements mandated in the ADR/ODR legal framework.[13] A large number of ADR bodies have been registered on the ODR platform since its launch. More than 300 ADR bodies from 26 member states can currently be accessed through the platform. The ADR bodies are complemented with designated national ODR contact points where consumers can receive assistance with how to use the platform.[14]

In light of the current reforms, a reasonable question to ask is how the objective of creating *"easily accessible and efficient out-of-court redress"* relates to other important principles and institutional considerations within the field of consumer redress. The present article focuses on procedural considerations regarding ODR. In order to understand the consequences of the ADR and ODR initiatives, there is a need for an assessment that includes the procedural mechanisms that contribute to the enforcement of the legal norms at stake. This article will discuss two such mechanisms, namely the *adversarial principle* and the *tendency toward settlements*. The aim is to address how the adversarial principle (argued to be integral to most ODR procedures) and tendencies toward settlements (also argued to be integral to most ODR procedures) affect the overarching idea of ODR as a tool to enforce consumer legislation. The article does not strive to criticize the system as such or to present ideas for reforms, but rather attempts to explore the procedural landscape where consumer redress is currently prioritized.

The institutional context where ODR takes place could be described as pluralistic. ODR exists in an institutional environment with public and private bodies (some of which are profit driven) that utilize a variety of techniques including meditation, arbitration, and ombudsman.[15] In addition, there are different levels of technology (sometimes including advanced automated and assisted negotiation) involved in the digital

[13] European Commission. (2017) Report from the Commission to the European Parliament and the Council on the functioning of the European Online Dispute Resolution platform established under Regulation (EU) No 524/2013 on online dispute resolution for consumer disputes COM(2017) 744 final, (2017) p. 1.

[14] Op. cit., p. 4.

[15] Schlote, J. A. (2017) Polycentrism and Democracy in Internet Governance. In: Uta Kohl (ed.). *The Net and the Nation State*. Cambridge: Cambridge University Press, pp. 165–184, p. 167.

interfaces available through the ODR platform.[16] Following the by now old idea that pluralism in fact should be followed by pluralism in norm/theory, this article takes its point of departure in pluralistic legal theory, which will be presented below.[17]

Discussions concerning tendencies toward settlements (and critique thereof) as well as discussions on the consequences of the adversarial principle, within different kinds of litigation, are certainly not new. Arguments and concerns about settlements in legal settings have already been put forth within the field of ODR.[18] Also the adversarial principle have been discussed previously, at least considering the broader subject of ADR.[19] However, as already mentioned, the aim of this article is not to critique these concepts, or the ODR platform or different ODR entities, *per se*. Instead, the article is rooted in the idea that in order to understand consumer litigation within the ODR framework, there is a need for theory and research concerning the institutional and procedural context of the ODR platform. The article aims at contributing to this by addressing *how* the adversarial principle and settlements affect the underlying landscape of consumer litigation through ODR.

The overarching aim of the article will be fulfilled by examining two ODR platforms in more detail, the German ODR entity *General Consumer Arbitration Board, Center for Mediation* (*Allgemeine Verbraucher--schlichtungsstelle Zentrum für Schlichtung, AVZS*) and the Swedish ODR entity *National Board for Consumer Disputes* (*Allmänna reklamationsnämnden, ARN*). These ODR entities have been chosen as both of them deal with a large number of cases every year and because they have a quite similar (*prima facie*) internal structure. They will be use in order to illustrate how the adversarial principle (and below, the tendencies toward settlement) forms an integral part of the ODR entities and co-produces the outcome of the proceedings. The two ODR bodies are similar in most regards. However, for ARN, the main rule is that *the Board* gives a proposal

---

[16] Cortés, P. (2017a) *The Law of Consumer Redress in an Evolving Digital Market: Upgrading from Alternative to Online Dispute Resolution*. Cambridge: Cambridge University Press, p. 44–52.

[17] Rosenfeld, M. (1998) *Just interpretations: Law between ethics and politics*. Santa Monica: University of California Press, 1998, p. 200.

[18] See Eidenmüller, H. and Engel, M. (2014) Against False Settlement: Designing Efficient Consumer Rights Enforcement Systems in Europe. *Ohio State Journal on Dispute Resolution*, 29 (2), p. 261–298.

[19] See, e.g. Wagner, G. (2014) Private Law Enforcement Through ADR: Wonder Drug Or Snake Oil. *Common Market Law Review*, 5, p. 165–194.

to the parties and settlement is an exception to this rule. For AVZS, it is the other way around.

2. CONSUMER ODR AND CONSUMER PROTECTION WITHIN THE EU

Before moving on to the theoretical foundation for this article and the substantial discussions on the adversarial principle and settlements, a few words should be said about consumer protection in EU countries. Consumer legislation has been a priority for many decades within the EU. Article 169 (1) and subsection (a) of Article 169 (2) of the *Treaty on the Functioning of the European Union (TFEU)* provide that the Union is to contribute to the attainment of a high level of consumer protection through measures adopted pursuant to Article 114 TFEU. Similarly, Article 38 of the *Charter of Fundamental Rights of the European Union* provides that Union policies are to ensure a high level of consumer protection. In accordance with Article 26 (2) TFEU, the internal market is to comprise an area without internal frontiers in which the free movement of goods and services is ensured. The internal market should provide consumers with added value in the form of better quality, greater variety, reasonable prices, and high safety standards for goods and services, which should promote a high level of consumer protection.[20]

Consumer protection is highlighted in the first paragraphs of the ADR Directive and the ODR Regulation. These provisions state that the purpose of the Directive and the Regulation is to achieve a high level of consumer protection *and* to contribute to the proper functioning of the internal market.[21] According to the preamble of the ADR Directive, resolutions emanating from ADR (including ODR) should not result in a consumer being

[20] European Commission. (2012) Communication from the commission to the European Parliament, The Council, The Economic and Social Committee and the Committee of the Regions: A European consumer agenda – Boosting confidence and growth. COM(2012) 225 final, p. 2.

[21] Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR). And Regulation, 'Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR).

> *"deprived of the protection afforded to him by the provisions that cannot be derogated from by agreement by virtue of the law of the Member State in which the consumer is habitually resident."*[22]

Furthermore, the rights to an effective remedy and to a fair trial are fundamental rights laid down in Article 47 of the *Charter of Fundamental Rights of the European Union*. Therefore, ADR procedures should not be designed to replace court procedures and should not deprive consumers or businesses of their rights to seek redress before the courts. In cases where a dispute could not be resolved through a given ADR procedure whose outcome is not binding, the parties should subsequently not be prevented from initiating judicial proceedings in relation to that dispute.[23]

The protection of consumer rights in relation to national procedural institutions has been discussed by the CJEU in several cases, with the clear signal that national courts should play an active part in protecting consumer rights.[24] The cases are not specifically concerned with ODR entities, but are quite relevant to the field since they deal with the effective protection of consumers redress through national institutions. In cases such as *Océano, Mostaza Claro*, and *Pannon*, the CJEU stated that unfair prorogation clauses must be set aside by the court regardless of whether this is argued by the consumer and that national courts should make *ex officio* efforts to guarantee consumer rights.[25] In *Duarte Hueros,* the CJEU held that a consumer not getting a price reduction constituted an infringement of the principle of effectiveness, even though the consumer had not claimed a price reduction in the court process. [26] In *Pénzügyi Lízing*, the CJEU considered it a responsibility of the national court to take an active part in investigating whether consumer rights have been violated.[27]

---

[22] Directive on consumer ADR, preamble § 44.

[23] Directive on consumer ADR, preamble § 45.

[24] For deeper analysis on this matter see, e.g. [forthcoming] Wallerman, A. (2019) Manoeuvring Procedural Autonomy In Sweden: Is Materielle Prozessleitung the Answer? In: Anna Nylund and Bart Krans (ed.). *Procedural autonomy: Room for manoeuvre?* Cambridge: Intersentia.

[25] Judgement of 27 June 2000, Joined Cases,*Océano Grupo Editorial SA v Roció Murciano Quintero and Salvat Editores SA v José M. Sánchez Alcón Prades and Others,* C-240/98 to C-244/98, ECLI:EU:C:2000:346, Judgement of 26 October 2006, *Mostaza Claro v Centro Móvil Milenium SL*, C-168/05, ECLI:EU:C:2006:675 and Judgement of 4 June 2009, *Pannon GSM Zrt. v Erzsébet Sustikné Győrfi*, C-243/08, ECLI:EU:C:2009:350.

[26] Judgement of 3 October 2013, *Soledad Duarte Hueros v Autociba SA och Automóviles Citroën España SA*, C-32/12, ECLI:EU:C:2013:637.

[27] Judgement of 6 July 2010, *VB Pénzügyi Lízing Zrt. v Ferenc Schneider*, C-137/08, ECLI:EU:C:2010:659.

The case law presented here indicates a strong responsibility for national institutions to act *ex officio*. Nevertheless, the CJEU has also highlighted the importance of ADR. In the *Alassini* case, where Italian legislation demanded that the consumer tried an out-of-court procedure before turning to a court, the CJEU approved of such a legislation, insofar as it ensures that out-of-court procedures are systematically used for settling disputes, and since it is designed to *strengthen* the EU consumer legislation at stake.[28] In sum, the CJEU stresses the importance of national procedural law strengthening the position of the consumer but also seems to be open to this being done through ADR proceedings (e.g. via the ODR platform).

3. PLURALISM AS A THEORETICAL TOOL FOR ODR RESEARCH

Legal pluralism as a theoretical concept has many dimensions, which in turn can be said to target different aspects of ODR.

Firstly, pluralism comes with a theoretical baggage. To get a grasp of the theories behind pluralism, the following words by *Davis* are illustrative:

> *"All normativity is produced by interactions between human agents who are not abstract individuals with unattached free wills, but rather already situated in diverse contexts of social meaning. Normativity (including anything termed "legal") is therefore necessarily constructed and reconstructed across these discursive environments by virtue of the fact that agents circulate between them. Norms and the "systems" attributed to them are therefore not closed and stable but intrinsically open and contingent."*[29]

This entails that in order to understand how ODR might function, the contingent expression of ODR must be studied. Furthermore, all aspects of the institutional context of ODR are potentially legally relevant. This means that a large number of considerations besides the ones discussed

[28] Judgement of 18 March 2010, Joined Cases, *Rosalba Alassini v Telecom Italia SpA (C-317/08), Filomena Califano v Wind SpA (C-318/08), Lucia Anna Giorgia Iacono v Telecom Italia SpA (C-319/08) and Multiservice Srl v Telecom Italia SpA (C-320/08) Par 45,* C-317/08, C-318/08, C-319/08 and C-320/08.

[29] Davies, M. (2010) Legal Pluralism. In: Peter Cane and Herbert Kritzer (ed.). *The Oxford Handbook of Empirical Legal Research*. Oxford: Oxford University Press, p. 805–827, 823.

in this article could (and should) be addressed in order to understand the relevant context for legal studies of ODR.[30]

The pluralistic theoretical view requires the researcher to pay attention to the procedural framework where consumer rights are (supposedly) made efficient. The relationship, and potential discrepancies, between an individual consumer right and a settled ODR procedure then inevitably become a focus of interest; e.g. does an ODR settlement mean that an individual consumer right has been enforced, and do possible transformations occur when a substantive legal act is situated in a specific institutional context?

Secondly, pluralism invites legal scholarship to consider how different disciplines/fields of law work together and how norms from different systems support or counteract each other. In this particular article, the focus of interest connects several fields of law, especially consumer protection law in relation to procedural law. In the examples discussed below, it must be considered that the ODR platform, enacted under Article 169 of TFEU, co--exists with mandatory consumer legislation and general (national) procedural principles.

Thirdly, the general understanding of pluralism strives to take into account all potentially legally relevant institutional factors. This includes the study of potential parallel systems for consumer protection legislation in the absence of a clear path for consumer cases to the supreme court (i.e. the CJEU). It has been argued in the ODR literature that paths to the general court system should not be hindered, but the question is whether there exists a *functional* route in the nitty gritty legal practice. The so-called "individual complaint journey" will in few instances lead to court and, in very few situations, find its way to the CJEU. "Ombudsprudence" has already been coined.[31] Furthermore the institutional environment also invites the well explored discussion on how technology forms and transforms the consumer protection enforcement via various technological tools.[32]

Fourthly, pluralism could also be considered on a more formal level concerning the competence to issue legal norms relevant for ODR. EU member state competence regarding civil procedure, EU initiatives under

[30] Studies concerning the technological dimensions and their consequences of ODR included.

[31] Stüner, M. (2014) ADR and Adjucation by State Courts: Competitors or Complements? *Grundfragen*, 3, pp. 122–128, 127.

Article 169 of the TFEU, guiding procedural principles deriving from the *European Convention of Human Rights (ECHR)*, and Article 47 of the *Charter of Fundamental Rights (ECFR)* are examples of how different legal institutions with different but overlapping competences all have normative influence over ODR.[33]

It is safe to assume that legal research rooted in legal pluralism, as it has been presented here, becomes very complicated. All relevant contexts cannot be addressed at once, and furthermore, the pluralistic perspectives deconstruct the idea that law can, in an exhaustive way, be studied from the position of the so-called legal insider.[34] Instead, different perspectives need to complement each other in order to get a grasp of the complex "discursive elements" where

> *"[n]orms and the 'systems' attributed to them are therefore not closed and stable but intrinsically open and contingent."*[35]

From this theoretical point of departure, the present article continues to the more specific question of the role of the adversarial principle and the tendencies toward settlement.

4. THE ADVERSARIAL PRINCIPLE WITHIN THE ODR FRAMEWORK

It should first be noted that the ODR framework did not emanate from the field of procedural law but from Article 169 TFEU and the aim to promote the interests of consumers and ensure a high level of consumer protection.

Nevertheless, since all ODR schemes should be in accordance with the fundamental rights to an effective remedy and to a fair trial under Article 47 of ECFR, ODRs are also, of course, procedural in their nature.[36]

---

[32] See, e.g. Carnerio, D. et al. (2012) Online dispute resolution: an artificial intelligence perspective. *Artificial Intelligence Review*, 41, pp. 211–240, Zeleznikow, J. (2017) Can Artificial Intelligence and Online Dispute Resolution Enhance Efficiency and Effectivness In Courts. *International Journal For Court Administration*, 8 (2), pp. 30-45 and Lodder, A. R. (2006) The Third Party and Beyond. An Analysis of the Different Parties, in particular the Fifth, Involved in Online Dispute Resolution. *Information & Communications Technology Law*, 15 (2), pp. 143–155.

[33] ODR Directive preamble § 26, ADR Directive preamble § 45.

[34] Davies, M. (2010) Legal Pluralism. In: Peter Cane and Herbert Kritzer (ed.). *The Oxford Handbook of Empirical Legal Research.* Oxford: Oxford University Press, p. 805–827, 823, 816.

[35] Op. cit., p. 823.

[36] Regulation on consumer ODR, preamble § 26, Directive on consumer ADR, preamble § 45.

Article 47 covers the scope of Article 6 and 13 of the ECHR. Although not spelled out in the article, the adversarial principle is held to be part of Article 6 of the ECHR.[37]

Ordinary civil court procedure is rooted in the adversarial principle, which includes the idea of rational negotiations between two parties that have equally strong arms at their disposal. The basic idea is that two parties put forth their interests, evidence, and arguments before a neutral third party in a rational way and also have the opportunity to criticize and debunk the argumentation of the other party. In this way, the parties, in total, have incentives to put forth all facts necessary for the neutral third party to make a ruling in accordance with the relevant substantive law. This, of course, is never the case in real court or ADR settings. The idea of two equal parties is in most situations an illusion, especially within the field of consumer litigation.[38] In turn, this has amounted to political reforms in court systems during the last 40 years where the weaker party is supported in one way or another in order to ensure real equality of arms between the parties. The weaker party is supported by arms such as financial support to afford a legal counsel, substantive case management by the court, a relieved burden of proof, and special courts for consumer disputes in order to level the playing field in the proceedings.

Although reforms try to achieve "real" equality of arms, and thereby efficient adversarial proceedings, the adversarial model remains criticized. The main point of this criticism was summarized by *Menkel-Meadow* in the mid-1990s.[39] *Menkel-Meadow* claimed that the binary positions intrinsic to the adversarial model polarize debate and tort the truth by leaving out information. The idea of oppositional presentation of facts only works when the actors involved in the process exhibit a genuine search for truth, which is something quite different than a genuine will to win a case.[40] The adversarial model, claims *Menkel-Meadow*, also simplifies complexity and obscures rather than clarifies.

It is not controversial to put forth that legal argumentation is situated in a complex contingent discursive environment, as described above. Thus,

[37] Danelius, H. (2012) *Mänskliga rättigheter i europeisk praxis: En kommentar till Europakonventionen om de mänskliga rättigheterna*. Stockholm: Norstedts Juridik, p. 246–247.

[38] See, e.g. Galanter, M. (1975) Afterword: Explaining Litigation, *Law & Society Review*, 9 (2), p. 347–368, 363. See also Lindblom, PH. (2017) *Progressive Procedure.* Uppsala: Iustus, p. 155f.

[39] Menkel-Meadow, C. (1996) The Trouble With the Adversary System in a Postmodern, Multicultural World. *William and Mary Law Review*, 38 (5), pp. 5-44, 13.

[40] Op. cit., p. 13.

the procedural order of formulating short claims and precise facts is delimiting the underlying conflict. To put it bluntly, the adversarial system lacks a genuine search for the complexities of reality.

Furthermore, the adversarial system is built upon the idea of positivist objectivity and neutrality and therefore also assumes the idea of common values among the parties involved.[41] Objectivity and neutrality are furthermore the values that often are put forth as definitions of *"independent and impartial"* (in Article 47 ECFR and Article 6 ECHR). The idea of a positivist objectivity (in a legal context) has been widely criticized.[42] Also the idea of a neutral third party has been heavily scrutinized,[43] and add to this the diverse legal and societal conditions within the EU. In sum, there are several epistemological problems associated with the adversarial principle (as the best tool for finding the facts of a complex reality).

The idea of an "illusionary balance" between the parties is non--controversial to put forth, especially in a consumer litigation context. In fact, the illusionary balance can be regarded as the reason for this specific field of law to exist in the first place. The imbalance between the parties has led to different kinds of reforms in different kinds of proceedings in recent decades. It is common to call out the need for competent legal expertise (human or non-human) in order to bring equality of arms to the parties.[44] However, it has been claimed by *Menkel-Meadow* that support via legal expertise brings *skills* concerning the procedure *per se*, and not arguments concerning the facts of the case. You win a case as a skilled lawyer and not as a lawyer who brings the relevant facts. But it should not be *skill* but *argument*, say the criticism here put forth. In sum, the idea of equality of arms misses the target, as it does not necessarily focus on the underlying conflict and therefore does not necessarily bring stronger enforcement of consumer rights to the table.[45]

---

[41] Op. cit., p. 8.

[42] From e.g. both legal realists and from the *Critical Legal Studies* movement. See, e.g. Bladini, M. (2013) *I objektivitetens sken: en kritisk granskning av objektivitetsideal, objektivitetsanspråk och legitimeringsstrategier i diskurser om dömande i brottmål.* Göteborg: Makadam, p. 89ff.

[43] See footnote 16 in Menkel-Meadow, C. (1996) The Trouble With the Adversary System in a Postmodern, Multicultural World. *William and Mary Law Review*, 38 (5), p. 5–44.

[44] See Article 47 of the ECFR.

[45] See also *Lewis* concerning small case litigants without counsel and their difficulties in understanding what kind of evidence is needed, Lewis, P. (2007) Litigants in Person and Their Difficulties in Adducing Evidence: A Study of Small Claims in an English County Court. *International Journal of Evidence & Proof*, 11, p. 24–48.

With this said, the present article does not advocate the abolishment of the adversarial principle, not least due to the lack of better options.[46] Nevertheless, in line with the theoretical understanding presented above, the effects of the adversarial model must be taken into account when assessing how consumer legislation is made efficient through consumer litigation.

The institutional consequences of the adversarial principles within ODR schemes will now be discussed in more detail in relation to the two ODR entities mentioned above, i.e. the Swedish *National Board for Consumer Disputes (Allmänna reklamationsnämnden, ARN)* and the German *General Consumer Arbitration Board, Center for Mediation (Allgemeine Verbraucher--schlichtungsstell. Zentrum für Schlichtung, AVZS)*.

4.1. NATIONAL BOARD FOR CONSUMER DISPUTES (ARN)

The Swedish ODR entity *National Board for Consumer Disputes (ARN)* has the manifest task of trying disputes that arise between consumers and business operators. ARN submits recommendations on how disputes should be resolved, e.g. it may decide/recommend that a product should be repaired by the company. ARN's recommendations are not binding, but a majority of Swedish companies follow them.[47] The inquiry is free of charge for both the consumer and the business involved.

The activities of ARN are governed through legislation ("Instruction for ARN"), where it is stated that ARN is an ADR entity according to the ADR Directive.[48] The instruction also proclaims that ARN should fulfil the obligations that follow from the ODR regulation. However, so far, few cases are brought to ARN via the ODR platform. In 2017, 13 cases were initiated at ARN through the ODR platform (which can be compared with the 14,000 cases assessed yearly by ARN when national cases are included).[49]

---

[46] Although there are voices claiming that *"EU is not, at heart, an adversarial culture, but seeks to build society based upon compromise and consensus"* Hodges, C. (2016) Consumer Redress: Implementing the Vision. In: Pablo Cortés (ed.). *The New Regulatory Framework for Consumer Dispute Resolution*. Oxford: Oxford University Press, pp. 351–368, 367.

[47] National Board for Consumer Disputes (Allmänna Reklamationsnämnden). (2017) *Årsredovisning (Annual Report) 2017*, pp. 7, 11 and 21.

[48] Förordning (2015:739) med instruktion för Allmänna reklamationsnämnden'. (2015) (Instruction for ARN).

[49] National Board for Consumer Disputes (Allmänna Reklamationsnämnden). (2017) *Årsredovisning (Annual Report) 2017*, pp. 7 and 11.

At first sight, it seems as if ARN is neither adversarial nor friendly toward settlements. However, when looking closer, it becomes evident that the procedure of preparing the case before *the Board* follows a clear adversarial model. The procedure (that is always a written procedure) is initiated by a letter or an online form. If the matter is not rejected for formal reasons, ARN asks the company to comment on the consumer's claims. The consumer in turn has an opportunity to see and comment on the company's response. Both parties have the right to submit written evidence in the form of e.g. contracts or certificates of inspection.

The registration form instructs the consumer to describe a specific claim and in a clear way motivate the claim (and also provide evidence). After a formal review, the company is invited to respond. When the company has responded, the consumer has the opportunity to complement the case. At this stage, ARN could initiate a discussion in order to reach a settlement between the parties. If needed, there are also options for further written argumentation from the parties.[50] If no settlement is reached, the case is assessed by *the Board* (at a meeting at which the parties are not present).[51]

The Board consists of a chairperson, who is a lawyer and has court experience, and two or four other members, who come from various consumer and trade organizations. The decisions of *the Board* are not formally binding for the company, but are nevertheless accepted in a majority of cases. For example, in 2017, 79 percent of the decisions were accepted by the company involved.[52] The parties have no legal counsel but are advised to seek support from the public advisors in consumer disputes available online via the Swedish single point of *Contents for Consumers*.

4.2. GENERAL CONSUMER ARBITRATION BOARD, CENTER FOR MEDIATION (AVZS)

The German *General Consumer Arbitration Board Center for Mediation (AVZS)* is officially recognized by the *Federal Office of Justice* and is supported by the extrajudicial dispute resolution for consumers and entrepreneurs association. The task of the *Arbitration Board* is to mediate and settle disputes between companies and consumers in order to reach out-of-court

[50] Instruction for ARN §§ 20–22.

[51] National Board for Consumer Disputes (Allmänna Reklamationsnämnden). (2017) *Årsredovisning (Annual Report) 2017*, p. 5.

[52] Op. cit., p. 21.

solutions.[53] AVZS is governed by the German *Act on Alternative Dispute Resolution in Consumer Matters*, which implements the ADR Directive. [54] The German legislation applies to both private and public ADR entities recognized under this Act.[55] The AVZS received 2,125 applications in 2017, 101 of which came via the ODR platform.[56]

Even though AVZS is more focused on settlements compared with ARN, it nevertheless also follows an adversarial model. The procedure should only take into account the outspoken interests of the parties.[57] It also follows from the AVZS rules of procedure that prior to the intervention by the arbitration board, the applicant must clearly formulate the contested claim against the respondent.[58] According to § 4 of the same document, it follows that the procedure is initiated by one of the parties which needs to describe the subject and interests at stake, and that the defendant thereafter is given an opportunity to respond. This phase can be conducted in writing, online, by telephone, or through direct personal conversation. The dispute resolution procedure ends by either a successful agreement or a declaration that the procedure has failed.[59]

The mediations are performed by certified mediators according to mediation law or by full-time lawyers with judge qualifications. The mediators have the objective of working *"impartially and independently"*,[60] and may submit a settlement proposal to the consumers if there are no results in the initial negotiations for a settlement, yet the proposal is not binding on the parties. Following the ADR Directive and ODR Regulation, the *AVZS Rules of Procedure* state that the proposal must be based on the situation arising from the dispute settlement procedure, and that it should be aligned with applicable law and comply with the mandatory consumer protection laws.[61]

---

53 AVZS website (2019). [online] Available from: https://www.streitbeilegungsstelle.org/ueber-uns/streitbeilegungsstelle/ [Accessed 11 mars 2019].

54 AVZS Rules of Procedure (Verfahrensordnung) § 8.

55 Gesetz über die alternative Streitbeilegung in Verbrauchersachen – Verbraucher--streitbeilegungsgesetz (Act on Alternative Dispute Resolution in Consumer Matters), § 1.

56 General Consumer Arbitration Board Center For Mediation Activity Report 2018, pp. 2, 4.

57 Op. cit., § 3 (3).

58 Op. cit., § 4 (2).

59 AVZS website (2019). [online] Available from https://www.streitbeilegungsstelle.org/das-verfahren/verfahrensordnung-ablauf/ [Accessed 11 March 2019]

60 AVZS website (2019). [online] Available from https://www.streitbeilegungsstelle.org/ueber-uns/streitmittler/ [Accessed 11 March 2019].

61 AVZS Rules of Procedure (Verfahrensordnung) § 8.

4.3. INITIAL REMARKS ON THE ROLE OF THE ADVERSARIAL PRINCIPLE FOR ARN AND AVZS

Both ARN and AVZS comprise the features that the criticism of the adversarial model targets, namely that the situation is framed by the claim presented by the consumer, and that the process of formulating the facts of the case is done through a back-and-forth written proceeding where the third party (competent in consumer legislation) is passive. *The Board*, which represents the third neutral party, but also the party with the competence to safeguard consumer rights, becomes involved when the dispute has already been framed by the parties. An interesting question to ask is whether it is possible to safeguard consumer rights without safeguarding which facts enter the proceedings. The case law from the CJEU seems to, at least to some extent, point in the direction that national courts should be active also in, *ex officio*, investigating relevant facts in consumer cases.[62]

Compared with ARN, AVZS is more focused on finding a friendly resolution, and no decision is given by the ODR entity without consent from both parties. Nevertheless, if the dispute mediator has made a proposal to the parties to resolve the dispute under the rules of procedure, this proposal must be based on the facts resulting from the dispute resolution procedure. Furthermore, both ARN's and AVZS's websites inform the parties that the ODR entities are not consumer protection organizations and do not unilaterally represent interests. They offer no legal advice and therefore represent neither companies nor consumers.[63] Instead, they serve as a neutral mediator between the parties. The paradoxical pluralistic mission, integral to ODR, here becomes obvious. ARN and AVZS are supposedly neutral third parties (adversarial model) and at the same time actors obligated to uphold consumer protection (ADR Directive, § 1). In the light of the ODR schemes described above, the view put forth by *Menkel-Meadow* that the adversarial principle tends to find its way into all kinds of legal procedure rings true, also for consumer redress ADR, online or not. The role of both acting as a neutral third party and defender of individual consumer rights is indeed challenging. And the situation will

[62] See Section 2 above.

[63] AVZS website (2019). [online] Available from https://www.verbraucher-schlichter.de/ueber-uns/verbraucherschlichtungsstelle [Accessed 11 March 2019]. The same principle is noted on the ARN's website: https://www.arn.se/ [Accessed 11 March 2019].

become even more complex when we add the tendencies toward settlements.

5. TENDENCIES TOWARD SETTLEMENT

The trend toward an increasing number of settlements is not only a trend within ADR (including ODR), but also within all kinds of civil procedure.[64] Settlements promise possibilities to achieve quick solutions, which is held as a value on its own regard.[65] Nevertheless, similar to the adversarial principle, settlements, too, have institutional and procedural consequences that have been highlighted in the legal literature.

Already in the 1980s, *Owen Fiss* formulated a quite elegant critique of settlements. The critique implicates that settlements are counterproductive in relation to the substantial law that the case concerns. The parties bypass the consumer litigation and instead agree on a sum of money to be paid in compensation, an agreement that replaces concrete application of the law. Of course, the settlement negotiations are not unrelated to the substantial law, but the point is that the process becomes more about assessment of e.g. risks, time delay, procedural costs etc. and less about finding facts in the case and matching them with substantive consumer rights.[66]

Within the field of ODR, *Eidenmüller and Engel* have warned against "false settlements". They argue that

> *"mandatory consumer protection rights attempt to correct market failure. Hence, enforcing these rights should not be returned to the market."*[67]

---

[64] "Settlement euphoria". Eidenmüller, H. and Engel, M. (2014) Against False Settlement: Designing Efficient Consumer Rights Enforcement Systems in Europe. *Ohio State Journal on Dispute Resolution*, 29 (2), pp. 261–298, 263.

[65] Cortés, P. (2014) Online Dispute Resolutions Services: A Selected Number of Case Studies. *Computer and Telecommunications Law Review*, 6, pp. 172–178, 172 and Cortés, P. (2016) The New Landscape of Consumer Redress: The European Directive on Consumer Alternative Dispute Resolution and the Regulation on Online Dispute Resolution. In: Pablo Cortés (ed.). *The New Regulatory Framework for Consumer Dispute Resolution*. Oxford: Oxford University Press, pp. 17–41, 35.

[66] See Wagner, G. (2014) Private Law Enforcement Through ADR: Wonder Drug Or Snake Oil. *Common Market Law Review,* 51, pp. 165–194, 176. See also Eidenmüller, H. and Engel, M. (2014) Against False Settlement: Designing Efficient Consumer Rights Enforcement Systems in Europe. *Ohio State Journal on Dispute Resolution*, 29 (2), pp. 261–298, 281 and Weiss, R. (2006) Some Economic Musings on Cybersettle. *University of Toledo Law Review*, 38, pp. 89–99, 95ff.

[67] Eidenmüller, H. and Engel, M. (2014) Against False Settlement: Designing Efficient Consumer Rights Enforcement Systems in Europe. *Ohio State Journal on Dispute Resolution*, 29 (2), pp. 261–298, 263.

In addition to this, there are concerns that 300 ODR entities will result in a fragmentation of decisions, which will make it difficult to uphold consistent consumer law application throughout the EU.[68] *De Paolo and Canessa* highlight that lawyers and parties tend to take the path of least resistance.[69] If consumer rights are to be protected, they need to be accompanied with smooth institutional structures. However, dealing with cross-border cases, the situation is often quite the opposite. Few consumers will consider suing a company for a faulty object worth 100 euro in their own city, and even less so if the company is seated in another country.[70] Furthermore, very few consumers will risk a proposed 50/50 settlement when faced with the risk of having to engage in a lengthy process with the potential outcome of getting nothing. The ADR Directive and ODR Regulation are clear on the point that ODR should not deny the consumer's right of access to court. However, *Eidenmüller and Engel* point out that it is very unlikely that a consumer will continue to court if an "expert" (the *ADR Board*/mediator) already has stated that the consumer has no case. The formal right of "access to court" is one thing; the institutional potential to make that right effective is another.[71]

Consumer legislation, formulated as individual rights, is often mandatory in the sense that the consumer is prohibited to refrain from the exercising the right. The logic behind this is that consumer protection legislation is in place in order to defend consumers from the influence of business owners. Opening up for individuals to refrain from their right would reduce the level of protection. In relation to this logic within the substantive law, it is a bit paradoxical that individual consumers, taking part of the ODR procedure, are trusted to accept settlements and decide which facts and arguments to bring to the table, when they at the same time are not, in many regards, deemed suitable to negotiate the terms of a consumer purchase.[72] With this being said, consumer rights are not

[68] See Wagner, G. (2014) Private Law Enforcement Through ADR: Wonder Drug Or Snake Oil. *Common Market Law Review*, 51, pp. 165–194, 171ff.

[69] De Paolo, G. and Canessa, R. (2016) New Trends for ADR in the European Union. In: Pablo Cortés (ed.). *The New Regulatory Framework For Consumer Dispute Resolution*. Oxford: Oxford University Press, pp. 407–426, 425.

[70] Eidenmüller, H. and Engel, M. (2014) Against False Settlement: Designing Efficient Consumer Rights Enforcement Systems in Europe. *Ohio State Journal on Dispute Resolution*, 29 (2), pp. 261–298, 268.

[71] Op. cit., p. 293.

[72] Although this is exactly the point made by CJEU in the case law cited above, namely that the court *ex officio* should provide consumers with information on which facts to bring to the case.

the only dimensions of conflict of importance to consumers.[73] The point being made here is merely that the paradoxical dimension of consumer redress, where consumers are autonomous and not autonomous at the same time, is part of the institutional landscape.

So far, a very small share of consumer-company conflict reaches the ODR framework. The *European Commission* has been monitoring and gathering information on ODR entities since the launch in 2016. In a report from 2017, an analysis was made of a complete dataset related to all complaints logged on the platform from 15 February 2016 to 15 February 2017. The analysis focused solely on complaints that were generated within the platform's workflow and did not take into consideration complaints received by ADR entities directly, i.e. outside the platform.[74]

During the 12 months monitored by the *Commission*, some 1.9 million people visited the platform and more than 24,000 complaints were submitted on the platform in its first year of operation.[75] However, 85 percent of the complaints were automatically closed within 30 days of submission due to the deadline for the consumer and business to agree on a competent ADR body. In order to understand the significance of these data and evaluate the interest of companies in ADR procedures, the *Commission* carried out a specific survey to get feedback from consumers whose cases were automatically closed. The survey revealed that, although a large number of businesses did not follow through using the ODR platform, 40 percent of consumers who submitted a complaint on the ODR platform that was automatically closed after 30 days had been contacted directly by the company to solve the problem without any further progression of the complaint on the platform. Hence, the ODR framework may lead to more case resolutions than the statistics show.[76] Nine percent of the complaints submitted via the ODR platform were not automatically

[73] See Hodges, C. (2016) Consumer Redress: Implementing the Vision. In: Pablo Cortés (ed.). *The New Regulatory Framework for Consumer Dispute Resolution*. Oxford: Oxford University Press, pp. 351–368, 358.

[74] European Commission. (2017) Report from the Commission to the European Parliament and the Council on the functioning of the European Online Dispute Resolution platform established under Regulation (EU) No 524/2013 on online dispute resolution for consumer disputes COM(2017) 744 final', (2017).

[75] Op. cit., p. 4.

[76] There are also technical reasons for the businesses' lack of responsiveness on the platform. For example, when a complaint is against a business is submitted for the first time and the business is not yet registered on the platform, the automatic notification may reach an incorrect email address. Other reasons could be that the origin of the notification message is unclear to the business or that the notification ends up in the businesses' email spam folder and remains unread. Op. cit., p. 6.

closed by the system but were refused by the company. Furthermore, in many of these cases, the respective businesses indicated that they made direct contact with the consumer and solved the issue or were planning to do so. For 4 percent of the submitted complaints, the data showed that both parties had used the possibility to withdraw from the procedure before their agreement to use a specific ADR body.[77]

Only 2 percent of the complaints were submitted to a specific ADR body. In around half of these cases, the ADR bodies refused to deal with the case on procedural grounds such as lack of competence or the consumer's failure to attempt to contact the business first. In some instances, either consumers or businesses withdrew from the procedure before it was completed. In the end, ADR procedure reached a final outcome in less than 1 percent of the 24,000 cases submitted via the platform, i.e. a couple of hundred cases.[78]

On the other hand, the *Commission* states that 44 percent of the submitted cases were settled bilaterally outside the platform.[79] All in all, this means that a large part of the cases processed via the ODR platform reach settlements. This also means that a very limited share of consumer--company conflicts result in the application of consumer legislation on facts of the case, in a court application sense.

Let us now consider settlement more closely in relation to the two ODR entity examples.

5.1. THE NATIONAL BOARD FOR CONSUMER DISPUTES (ARN)

ARN is not an ODR designed to settle cases. Instead, as mentioned above, the main route of the procedure is for *the Board* to finalize a written recommendation. Nevertheless, current trends toward efficiency have led to reforms, and since 2016 ARN has been obliged to make efforts in order for the parties to reach a settlement. According to § 3 and § 22 of the instruction for ARN, *the Board* should try to encourage a settlement between the parties.[80]

A report from the parliamentary ombudsmen in Sweden (JO) states that ARN, during a trial period conducted conciliation talks by telephone

[77] Ibid.

[78] Op. cit., p. 7.

[79] Ibid.

[80] Förordning (2015:739) med instruktion för Allmänna reklamationsnämnden'. (2015) (Instruction for ARN) 3 § and 22 §.

(in order to reach settlements) and measured among other things the time they spent on the conversation. During the evaluation, it was found that the ARN staff had managed to reconcile the parties in a majority of cases, but that the conciliation talks took a lot of time. The staff were therefore advised not to raise the issue of conciliation in all cases, but only in cases where time could be saved.[81] The reason for considering a settlement could therefore be said to concern cost efficiency for ARN, not other normative values connected to consumer protection.[82] Hence, the reason for settlements concerns the efficiency of ARN as an organization trying to increase its efficiency in achieving resolutions. The possible distinction between a settlement and an assessment of facts under relevant (mandatory) consumer legislation was not discussed in the report. In 2017, 22 percent of the cases brought to ARN reached a settlement and therefore did not end up in a written decision from *the Board*. This should be compared with the 37 percent of the cases that actually resulted in a decision by *the Board*.[83]

In sum, although the basic design of ARN points toward a decision by *the Board*, a fifth of the cases are resolved through settlements. This is a relatively high number considering that only 37 percent of the cases end up with a substantive decision.

5.2. GENERAL CONSUMER ARBITRATION BOARD, CENTER FOR MEDIATION (AVZS)

As mentioned above, it follows from the AVZS website that it is not a consumer protection organization. Furthermore, AVZS offers no legal advice and therefore represents neither companies nor consumers. Instead, it serves as a neutral mediator between the parties. Nevertheless, if the mediation does not lead to an amicable solution, *the Board* submits an arbitration proposal accompanied with reasons for the proposal.

---

[81] Justitieombudsmannen, 'Dnr 6398-2017 – Inspektion av Allmänna reklamations nämnden (ARN) den 23–24 oktober 2017 (Parlimentary Ombudsmen, Inspection of ARN 23–24 oktober 2017), p. 4.

[82] See National Board for Consumer Disputes (Allmänna Reklamationsnämnden). (2017) *Årsredovisning (Annual Report) 2017*, p. 10.

[83] Förordning (2015:739) med instruktion för Allmänna reklamationsnämnden' (2015). (Instruction for ARN) 3 § and 22 §. National Board for Consumer Disputes (Allmänna Reklamationsnämnden). (2017) *Årsredovisning (Annual Report) 2017*, p. 6 (when cases where the company has not responded are included, this number rises to 47 percent for the year 2017, p. 15).

The Board must also inform the parties of the possibility of not accepting the deal and instead having the option to turn to a court.[84]

According to the activity report for 2018, 1,993 of 2,125 cases were finished at AVZS.[85] All of these cases were not settled since also cases that were withdrawn were counted as finished. Overall, 1,376 cases were unsuccessful in the sense that no agreement was reached between the parties. Of these, 1,171 were unsuccessful in this way because the defendant did not get involved in the procedure. Furthermore, 197 applications were withdrawn by the applicant.[86] When excluding the number of rejected cases (396), the agreement rate for 2017 ends up being 13.84 percent, which means that 221 cases were settled. [87] There is no information in the report concerning the underlying reasons in order for the parties to reach a settlement.

5.3. GENERAL CONSIDERATIONS CONCERNING THE TENDENCIES TOWARD SETTLEMENT

The statistics from the *Commission* report and the figures from ARN and AVZS paint a picture of settlements being very common. Also for ARN, a body where the main path of procedure does not lead to settlements, they are still very common. Although there are no statistics from ARN, AVZS, and the *Commission*, it is not very farfetched to assume, following *Weiss*, *Wagner*, *Eidenmüller and Engel*, that a large share of the settlements are not based on consumer regulation considerations, but rather on considerations of costs, risks, and quick resolutions to the conflicts at hand.[88] The examples from ARN also indicate that the ODR entity involves a cost benefit analysis concerning when to pursue a settlement and when not to. The normative difference between a settlement and an assessment of the facts in a case does not seem to be an issue of concern. The two types of resolutions are treated as interchangeable. The lack of discussion or distinction between a settlement, a reasoned proposal, and an assessment of the facts in a case,

---

[84] AVZS Rules of Procedure (Verfahrensordnung) § 8 (3).

[85] General Consumer Arbitration Board Center For Mediation Activity Report 2018, p. 2.

[86] Op. cit., p. 7.

[87] Op. cit., p. 8.

[88] Weiss, R. (2006) Some Economic Musings on Cybersettle, *University of Toledo Law Review*, 38, p. 89–99, Wagner, G. (2014) Private Law Enforcement Through ADR: Wonder Drug Or Snake Oil. *Common Market Law Review*, 51, pp. 165–194 and Eidenmüller, H. & Engel, M. (2014) Against False Settlement: Designing Efficient Consumer Rights Enforcement Systems in Europe. *Ohio State Journal on Dispute Resolution*, 29 (2), pp. 261–298.

in the *Commission* report, and in the information provided by ARN or AVZS is interesting considering that resolving a conflict to avoid time-delay or to avert risks is something quite different than applying a legal right.

6. PROCEDURAL TRANSFORMATION WITHIN ODR SCHEMES

This article has focused on two specific procedural considerations regarding ODR: the adversarial principle and tendencies toward settlements. The reasoning is rooted in the idea that in order to understand the consequences of the ADR and ODR initiatives, we need to understand the procedural mechanisms that contribute to the enforcement of the legal norms at stake.

An obvious starting point for this discussion is to put forth that to settle is to do something other than enforce a consumer right. There is quite a different normative process involved. Instead of matching substantive norms to facts, the parties are involved in a negotiation based on economic rationale. However, the distinction between different kinds of resolutions is not visible in the official reports concerning ODR. As already mentioned, the ODR platform has the twofold objective of promoting both consumer protection and the internal market. A distinction between resolving a case based on the application of legal rights, and resolving a case based on the broader considerations involved in settlements is central to the objective of promoting consumer protection, but it is not as relevant in relation the growth of the EU economy. Since consumer transactions add up to a large part of the EU's gross domestic product, there is considerable economic interest in making the consumer market as efficient as possible. The lack of distinction between applications of norms and resolutions on other grounds makes sense only in relation the objective of the ODR framework to promote cross-border trade. Conflicts need to be resolved for the market to function, but the normative basis for such resolutions is not that important. The economic efficiency is calculated at an aggregated level, which is quite an opposite starting point compared with individual legal rights, and the prime aim is resolutions. From this perspective, the consumers become a mass, a collective, that is weighed against an abstract economic interest of the companies to strike a balance with positive effects on the internal market. The possibilities to find efficient consideration toward consumers, on an aggregated scale, is further

strengthened by the possibilities to access data due to the digital dimension of ODR.[89] Or as expressed by *Eidenmüller and Engel*:

> *"mandatory consumer protection rights attempt to correct market failure."*[90]

In other words, the focus on settlements (and the adversarial model) could be said to build a system around economic rationale in order to support the system as such making the objective of economic growth primary and the objective of enforcing (individual) consumer rights secondary. From what seems (at least at a first glance) to be the opposite perspective, the signals from the CJEU, i.e. that court officials around EU should take active steps to ensure individual consumer rights, paint quite a different picture.

Furthermore, the ADR Directive Article 11 stresses that there must be no infringements of mandatory consumer law. These concerns have led to raised voices for the need for individual assessments based on an adversarial model that ensures access to courts in a fair trial where the parties have equal arms.[91] Nevertheless, if ODR is seen as something that becomes when legal decisions are made (rather than as a fixed field of law open to doctrinal studies), then it should be considered that in many cases, no resolutions seem to take place at all. After all, the statistics show that less than 1 percent of the cases submitted to an ODR platform reach some sort of a substantive assessment. In this institutional landscape (a landscape of an almost non-existent formal consumer redress), there are calls for quick and flexible routes to ensure just conflict resolutions to consumers. This is where settlements enter the stage. But once again, quite interestingly, the potential problems arising from too many settlements are leading to a renewed call for more strict adversarial models of conflict resolution, as the adversarial process is seen as strengthening access to justice.[92] Therefore, considering the risk for settlements on non--legitimate grounds, adversarial models are called for to safeguard

[89] Concerning this, see Weiss, R. (2006) Some Economic Musings on Cybersettle. *University of Toledo Law Review,* 38, p. 89–99, 96 and Cortés, P. (2017b) The Online Court: Filling the Gaps of the Civil Justice System? *Civil Justice Quarterly,* 36 (1), pp. 109–126, 173.

[90] Eidenmüller, H. & Engel, M. (2014) Against False Settlement: Designing Efficient Consumer Rights Enforcement Systems in Europe. *Ohio State Journal on Dispute Resolution*, 29 (2), pp. 261–298, 263.

[91] See, e.g. Eidenmüller, H. & Engel, M. (2014) Against False Settlement: Designing Efficient Consumer Rights Enforcement Systems in Europe. *Ohio State Journal on Dispute Resolution*, 29 (2), pp. 261–298, 269.

[92] Ibid.

individual rights. And, *vice versa*, when the adversarial model makes processes slow and complicated, settlements offer the necessary quick and flexible routes to ensure just conflict resolutions to consumers.[93] In this way, the adversarial model and settlements promise solutions to each other's problems in a paradoxical manner.

This article concludes in this contradictory notion with no clear answers on how to strike the best balance for ODR schemes. Taking a pluralistic approach, it is clear that the complex reality of consumer redress gives rise to different kinds of problems at different levels depending on how we go about conflict resolution. Consumer redress through the ODR platform will transform consumer conflicts (as all legal institutions do). This transformation is an integral part of law. "Resolution" is not the same in a settlement compared to an application of norms to facts. Furthermore, a settlement based on an individual assessment is not the same as a settlement where the mediator has access to aggregated data on typical consumer behavior. Lastly, a presentation of a case channeled through an adversarial model is not the same as a presentation of a case channeled through *ex officio* action by an investigating authority. Further research in this field is called for in order to understand the special and varying implications of procedural principles surrounding consumer protection within ODR.

LIST OF REFERENCES

[1] ARN. (2019) [online] Available from: https://www.arn.se/ [Accessed 11 March 2019].

[2] AVZS. (2019) [online] Available from: https://www.verbraucher-schlichter.de/ueber-uns/verbraucherschlichtungsstelle [Accessed 11 March 2019].

[3] Bladini, M. (2013) *I objektivitetens sken: en kritisk granskning av objektivitetsideal, objektivitetsanspråk och legitimeringsstrategier i diskurser om dömande i brottmål*. Göteborg: Makadam.

[4] Carnerio, D. et al. (2012) Online dispute resolution: an artificial intelligence perspective. *Artificial Intelligence Review*, 41.

[5] Cortés, P. (2014) Online Dispute Resolutions Services: A Selected Number of Case Studies. *Computer and Telecommunications Law Review*, 6.

[93] Cortés, P. (2016) The New Landscape of Consumer Redress: The European Directive on Consumer Alternative Dispute Resolution and the Regulation on Online Dispute Resolution. In: Pablo Cortés (ed.). *The New Regulatory Framework for Consumer Dispute Resolution*. Oxford: Oxford University Press, pp. 17–41, 3.

[6] Cortés, P. (2016) The New Landscape of Consumer Redress: The European Directive on Consumer Alternative Dispute Resolution and the Regulation on Online Dispute Resolution. In: Pablo Cortés (ed.). *The New Regulatory Framework for Consumer Dispute Resolution*. Oxford: Oxford University Press.

[7] Cortés, P. (2017a) *The Law of Consumer Redress in an Evolving Digital Market: Upgrading from Alternative to Online Dispute Resolution*. Cambridge: Cambridge University Press.

[8] Cortés, P. (2017b) The Online Court: Filling the Gaps of the Civil Justice System? *Civil Justice Quarterly*, 36 (1).

[9] Danelius, H. (2012) *Mänskliga rättigheter i europeisk praxis: En kommentar till Europakonventionen om de mänskliga rättigheterna*. Stockholm: Norstedts Juridik.

[10] Davies, M. (2010) Legal Pluralism. In: Peter Cane and Herbert Kritzer (ed.). *The Oxford Handbook of Empirical Legal Research*. Oxford: Oxford University Press.

[11] De Paolo, G. and Canessa, R. (2016) New Trends for ADR in the European Union. In: Pablo Cortés (ed.). *The New Regulatory Framework For Consumer Dispute Resolution*. Oxford: Oxford University Press.

[12] Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC.

[13] Eidenmüller, H. & Engel, M. (2014) Against False Settlement: Designing Efficient Consumer Rights Enforcement Systems in Europe. *Ohio State Journal on Dispute Resolution*, 29 (2).

[14] European Commission. (2011) Commission Staff Working Paper Impact Assessment Accompanying the document Proposal for a Directive of the European Parliament and of the Council on Alternative Dispute Resolution for consumer disputes (Directive on consumer ADR) and Proposal for a Regulation of the European Parliament and of the Council on Online Dispute Resolution for consumer disputes (Regulation on consumer ODR). SEC(2011) 1408 final.

[15] European Commission. (2012) Communication From The Commission To The European Parliament, The Council, The Economic and Social Committee and the Committee of the Regions: A European Consumer Agenda – Boosting confidence and growth. COM(2012) 225 final.

[16] European Commission. (2017) Report From The Commission to The European Parliament and The Council on the functioning of the European Online Dispute

Resolution platform established under Regulation (EU) No 524/2013 on online dispute resolution for consumer disputes. COM(2017) 744 final.

[17] Förordning (2015:739) med instruktion för Allmänna reklamationsnämnden'. (2015) (Instruction for ARN).

[18] Galanter, M. (1975) Afterword: Explaining Litigation. *Law & Society Review*, 9 (2).

[19] General Consumer Arbitration Board Center for Mediation (Allgemeine Verbraucher--schlichtungsstelle Zentrum für Schlichtung) Activity report (2018).

[20] Gesetz über die alternative Streitbeilegung in Verbrauchersachen – Verbraucher--streitbeilegungsgesetz (Act on Alternative Dispute Resolution in Consumer Matters).

[21] Hodges, C. (2016) Consumer Redress: Implementing the Vision. In: Cortés, Pablo (ed.). *The New Regulatory Framework for Consumer Dispute Resolution*. Oxford: Oxford University Press.

[22] Judgement of 18 March 2010, Joined Cases, *Rosalba Alassini v Telecom Italia SpA (C-317/08), Filomena Califano v Wind SpA (C-318/08), Lucia Anna Giorgia Iacono v Telecom Italia SpA (C 319/08) and Multiservice Srl v Telecom Italia SpA (C-320/08)* Par 45, C-317/08, C-318/08, C 319/08 and C-320/08.

[23] Judgement of 26 October 2006, *Mostaza Claro v Centro Móvil Milenium SL*, C-168/05, ECLI:EU:C:2006:675.

[24] Judgement of 27 June 2000, Joined Cases, *Océano Grupo Editorial SA v Roció Murciano Quintero and Salvat Editores SA v José M. Sánchez Alcón Prades and Others*, C 240/98 to C-244/98, ECLI:EU:C:2000:346.

[25] Judgement of 4 June 2009, *Pannon GSM Zrt. v Erzsébet Sustikné Győrfi*, C-243/08, ECLI:EU:C:2009:350.

[26] Judgement of 3 October 2013, *Soledad Duarte Hueros v Autociba SA och Automóviles Citroën España SA*, C-32/12, ECLI:EU:C:2013:637.

[27] Judgement of 6 July 2010, *VB Pénzügyi Lízing Zrt. v Ferenc Schneider*, C-137/08, ECLI:EU:C:2010:659.

[28] Justitieombudsmannen (Parlimentary Ombudsmen). (2017) 'Dnr 6398-2017 – Inspektion av Allmänna reklamationsnämnden (ARN) den 23–24 oktober 2017 (Inspection of ARN 23–24 oktober 2017).

[29] Lewis, P. (2007) Litigants in Person and Their Difficulties in Adducing Evidence: A Study of Small Claims in an English County Court. *International Journal of Evidence & Proof*, 11.

[30] Lindblom, PH. (2017) *Progressive Procedure*. Uppsala: Iustus.

[31] Lodder, A. R. (2006) The Third Party and Beyond. An Analysis of the Different Parties, in particular the Fifth, Involved in Online Dispute Resolution. *Information & Communications Technology Law*, 15 (2).

[32] Menkel-Meadow, C. (1996) The Trouble With the Adversary System in a Postmodern, Multicultural World. *William and Mary Law Review*, 38 (5).

[33] National Board for Consumer Disputes (Allmänna Reklamationsnämnden). (2017) *Årsredovisning (Annual Report) 2017*.

[34] Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC.

[35] Rosenfeld, M. (1998) *Just interpretations: Law between ethics and politics*. Santa Monica: University of California Press, 1998.

[36] Schlote, J. A. (2017) Polycentrism and Democracy in Internet Governance. In: Uta Kohl (ed.). *The Net and the Nation State*. Cambridge: Cambridge University Press.

[37] Stüner, M. (2014) ADR and Adjucation by State Courts: Competitors or Complements? *Grundfragen*, 3.

[38] Wagner, G. (2014) Private Law Enforcement Through ADR: Wonder Drug Or Snake Oil. *Common Market Law Review*, 51.

[39] Wallerman, A. (2019) Manoeuvring Procedural Autonomy In Sweden: Is Materielle Prozessleitung the Answer? In: Anna Nylund and Bart Krans (ed.). *Procedural autonomy: Room for manoeuvre?* Cambridge: Intersentia [forthcoming].

[40] Weiss, R. (2006) Some Economic Musings on Cybersettle. *University of Toledo Law Review*, 38.

[41] Zeleznikow, J. (2017) Can Artificial Intelligence And Online Dispute Resolution Enhance Efficiency And Effectivness In Courts. *International Journal For Court Administration*, 8 (2).

DOI 10.5817/MUJLT2019-2-8

BLOCKCHAIN-BASED LAND REGISTRATION: POSSIBILITIES AND CHALLENGES*

by

MARIA KACZOROWSKA**

In recent decades land registration systems operating in Europe and worldwide have been subject to modernisation processes consisting in implementation of information and communication technologies. Such reforms have gradually led to facilitating access to land information, improving effectiveness of land registration proceedings and even introducing possibilities to dispose of the ownership of land electronically by developing electronic conveyancing mechanisms. Another innovative concept much discussed nowadays is the application of blockchain technology in the land registration sector. This solution is currently being tested in a number of countries.

Distributed ledger technology underlying blockchain is expected to revolutionise land registration by offering a secure architecture to store land transactions with the use of cryptographic protocol. This shall bring advantages of increased trust and processing efficiency as well as reduction of costs. However, the above idea raises concerns given that, under the assumptions of the "original" blockchain model, transactions are irreversible and are carried out without intermediaries, which means the lack of any external control and independent verification of the transactions to be recorded.

The article examines potential benefits and risks of automatisation of land transactions as well as practical experiences of selected countries in implementing blockchain in the area of land registration. On this basis, an assessment will be

* This article has been prepared within the research project *Informatisation of land and mortgage registers* supported financially by the Polish National Science Centre (No. 2015/17/B/HS5/00460). It is an extended version of a paper presented at the *16th International Conference Cyberspace* held in Brno, 1 December 2018.

** maria.kaczorowska@uwr.edu.pl, assistant professor, Research Centre for Legal and Economic Issues of Electronic Communication, Faculty of Law, Administration and Economics, University of Wrocław, Poland.

made as to whether blockchain-based registration could indeed replace the existing methodology of registering rights to land.

KEY WORDS

Blockchain Technology, Informatisation, Land Registration, Real Estate Transactions

1. INTRODUCTION

The common use of information and communication technologies transforms progressively the way in which market transactions are carried out and public services are performed by the authorities. This can be illustrated by the example of real estate transactions and land registration which are subject to advanced informatisation processes. Technological improvements being implemented in this area are intended to facilitate the transfer of immovables and increase the functionality of land registers by providing rapid and easy access to reliable information regarding the legal status of land as well as ensuring effective land registration proceedings. Considerable achievements in modernisation of land registration systems have been made recently in European countries, including Poland, which is demonstrated by guaranteeing public online access to land registers and introducing an infrastructure to initiate land registration proceedings electronically, with the use of qualified electronic signatures (for the time being under Polish law applications for entry in the land register are submitted solely via the IT data transmission system by notaries, court executive officers and heads of tax offices, however it is planned that in the future this method of communication be used by other entitled entities as well). In case of an electronic application an automatic notice is made in the land register in real time so that any movements on the property are blocked until completion of the registration procedure.[1] Moreover, in some jurisdictions systems of electronic conveyancing are

[1] See e.g.: Gołaczyński, J. and Klich, A. (2016) Informatyzacja ksiąg wieczystych. Uwagi ogólne. In: Andrzej Marciniak (ed.). *Elektronizacja postępowania wieczystoksięgowego. Komentarz praktyczny. Akty wykonawcze,* Warszawa: C.H. Beck, pp. 31–58; Gryszczyńska, A. (2011) *Nowa Księga Wieczysta. Informatyzacja rejestru publicznego.* Warszawa: LexisNexis, pp. 182 ff.; Wudarski, A. (2016) Das Grundbuch in der Registerwelt. Eine rechtsvergleichende Untersuchung zum deutschen und polnischen Grundbuch im europäischen Kontext. In: Arkadiusz Wudarski (ed.). *Das Grundbuch im Europa des 21. Jahrhunderts.* Berlin: Duncker & Humblot, pp. 23–82; Kaczorowska, M. (2019) Informatisation of Land Registers in Poland and Other Member States of the European Union: A Comparative Overview. *Law and Forensic Science*, 17 (1), pp. 30–48.

being developed. For example, in Finland the parties can conclude the contract of conveyance in a closed electronic system once they have undergone the identification and authorisation procedures and the registration begins automatically after the transaction text has been checked by the registrar.[2]

Currently, it is expected that the future stage of development of land registers will be the application of blockchain technology which shall revolutionise the land registration process. As highlighted by the promoters of blockchain-based land registration systems, distributed ledger technology underlying blockchain provides a secure architecture to store land transactions, characterised by enhanced transparency and processing efficiency as well as reduced transaction costs resulting from the lack of intermediaries. What is more, actions aimed at testing the possibilities to use blockchain technology in the field of land registration or even introducing blockchain land registers have been undertaken in some countries around the world. At the same time, however, the above idea deserves a thorough analysis because of the concerns that arise given, on one hand, the nature of blockchain and, on the other hand, essential functions of land registers, connected with the specificity of transactions whose object is land. Indeed, it is characterised by high value compared to other assets as well as particular importance from the socio-economic point of view, which is reflected in strict formal requirements envisaged in law, relating to transfer or establishment of real property rights. What needs a particular emphasis is that due to a complex character of real estate transfer, parties to the contracts are commonly assisted by legal professionals and the effect of land registration proceedings is to ensure not only publicity but also certainty of the transaction. It should be therefore considered what role can be played by blockchain in the area of land registration and, above all, whether it can constitute an alternative to the land registration systems functioning nowadays.

[2] Niemi, M. I. (2017) Electronic Conveyancing of Real Property in Europe: Two Models. The English and the Finnish One. In: Luz M. Martínez Velencoso, Saki Bailey and Andrea Pradi (eds.). *Transfer of Immovables in European Private Law.* Cambridge: Cambridge University Press, pp. 32 ff. See also: Brennan, G. (2015) *The Impact of eConveyancing on Title Registration: A Risk Assessment.* Cham: Springer, pp. 74 ff.; Cooke, E. (2003) E-conveyancing in England: Enthusiasms and Reluctance. In: David Grinlinton (ed.). *Torrens in the Twenty--first Century.* Wellington: LexisNexis, pp. 277–293.

2. ASSUMPTIONS AND POSSIBLE IMPACT OF BLOCKCHAIN ON IMPROVING LAND REGISTRATION

The features attributed to blockchain technology are deemed to predestine it to be used in the public services sector, especially for the purpose of maintaining public registers, and among them land registers.[3] The potential of blockchain for enhancing the quality of recordkeeping is recognised in particular as regards developing countries in which the land registration systems are inefficient and unreliable.[4] The reason is that blockchain is a method of recording data in a digital ledger. It operates as a distributed database using cryptographic techniques to store a continuously growing list of records of transactions, i.e. blocks, accessible to all computers running the same protocol. The first and the most famous example of application of blockchain is a cryptocurrency called *Bitcoin*. The *Bitcoin* system offers a possibility to carry out online payments directly from one party to another without going through financial institutions serving as trusted third parties.[5]

Under the blockchain concept blocks are grouped together in such a way that the first block (genesis block) is followed by a sequence of time--stamped blocks, each of which contains a unique identifier (a digital fingerprint) called *hash*, being a reference to the previous block. As a consequence, an unbreakable chain of blocks is created because any change of a single transaction is impossible without modifying subsequent

---

[3] See further e.g.: Boucher, P., Nascimento, S. and Kritikos, M. (2017) *How Blockchain Technology Could Change Our Lives: In-depth Analysis.* Brussels: European Parliament Research Service, pp. 18 ff.; Arruñada, B. (2018) Blockchain's Struggle to Deliver Impersonal Exchange. *Minnesota Journal of Law, Science & Technology*, 19, pp. 55 ff.; Young, S. (2018) Changing Governance Models by Applying Blockchain Computing. *The Catholic University Journal of Law & Technology*, 26 (2), pp. 1 ff.; Graglia, J. M. and Mellon, C. (2018) Blockchain and Property in 2018: At the End of the Beginning. In: *2018 World Bank Conference on Land and Poverty*, Washington DC, USA, 19–23 March. pp. 8 ff. [online] Available from: https://www.conftool.com/landandpoverty2018/index.php?page=downloadPaper&ismobile=true&filename=02-11-Graglia-864_paper.pdf&form_id=864&form_version=final [Accessed 22 December 2018]; Lemieux, V. L. (2017) Blockchain Recordkeeping: A SWOT Analysis. *Information Management*, 51 (6), pp. 22 ff.; Anand, A., McKibbin, M. and Pichel, F. (2017) Colored Coins: Bitcoin, Blockchain, and Land Administration. In: *2017 World Bank Conference on Land and Poverty*, Washington DC, USA, 20–24 March. Available from: https://cadasta.org/resources/white-papers/bitcoin-blockchain-land/ [Accessed 12 December 2018]; Tapscott, D. and Tapscott, A. (2016) *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World.* New York: Portfolio/Penguin, pp 6 ff.

[4] These issues will be expanded in the following sections of the article.

[5] Nakamoto, S. (2008) *A Peer-to-Peer Electronic Cash System.* [online] Available from: https://bitcoin.org/bitcoin.pdf [Accessed 12 December 2018]; Sklaroff, J. M. (2017) Smart Contracts and the Cost of Inflexibility. *University of Pennsylvania Law Review*, 166 (1), pp. 268 ff.

blocks. Before being recorded on the blockchain, transactions are subject to verification performed by users called *miners*, who act within a distributed peer-to-peer network, without the intervention of a central authority, specialised or trusted third parties. Blockchain is based on the consensus mechanism which means that transactions need to obtain approval of the network participants and they are communicated transparently across the entire network. A consensus is reached when the majority of active miners (holding at least 51 % of the computing power) agree to an update in the digital register. Each node, i.e. any computer connected to the system, retains a copy of the history of transactions and the copies should match exactly so that no single user is able to manipulate the data. In order to ensure the integrity and authenticity of records a system of asymmetric cryptography is applied. It is based on digital signatures using public and private keys.[6]

It should be noted that blockchains may be designed as either public or private registers. These two models are correlated with the distinction of permissioned and permissionless types of blockchains.[7] The description presented above refers generally to public blockchain, which is the basic and best known type. Characteristic to a public blockchain is that any user can join the network and participate in verifying transactions thanks to the use of open source software. Public blockchains are often permissionless as no authorisation or authentication of the participants is required and thus they remain anonymous. In case of private blockchain, in turn, the access is restricted to a specific number of authorised users (including either parties who have been privy to the creation of the register, or parties invited to participate according to the system's rules).[8] Blockchains of the latter type correspond to the idea of permissioned ones in which participants are identified and can access the system on condition they are authorised and authenticated. Permissioned blockchains are intended rather to be used within corporations (e.g. in the banking sector).[9] Moreover, a type of blockchain being a combination of private and public

[6] On how blockchain works see e.g.: Lemieux, V. L. (2017) Op. cit., p. 21; Nogueroles Peiró, N. and Martinez García, E. J. (2017) Blockchain and Land Registration Systems. *European Property Law Journal,* 6 (3), p. 300; Spielman, A. (2016) *Blockchain: Digitally Rebuilding the Real Estate Industry.* [online] pp. 42 ff. Ph.D. Massachusetts Institute of Technology. Available from: https://dspace.mit.edu/bitstream/handle/1721.1/106753/969450770-MIT.pdf?sequence =1 [Accessed 14 December 2018].

[7] Lemieux, V. L. (2017) Op. cit., p. 22.

[8] Thomas, R. (2017) Blockchain's Incompatibility for Use as a Land Registry: Issues of Definition, Feasibility and Risk. *European Property Law Journal*, 6 (3), p. 364.

ones is defined as hybrid blockchain. In this case only specific entities or persons can be part of the blockchain network and participate in the consensus process but at the same time public blockchain is utilised for accounting purposes and as a proof of existence.[10] It is observed, however, that the differences among particular blockchain models are reducing.[11]

Taking into account the above characteristics of blockchain, in line with arguments put forward by its proponents, predicted benefits resulting from the application of this technology in the field of land registration consist mainly in the lack of intermediaries, a distributed character of the system, transparency and immutability.

Blockchain in its "original" or "pure" form (i.e. the public variant) is defined as a trustless system because it enables the parties to enter into peer-to-peer online transactions without the participation of professional facilitators such as registries, banks, notaries, conveyancers or real estate agents. The only players involved are parties to the transactions assisted by miners whose role is to validate blocks.[12] Under the mechanism governing the blockchain network the recordation of a transaction is considered to be final and is irreversible, any independent verification of the record to be registered being excluded. Once an entry in the register is made, it cannot be altered or deleted without the consent of the miners which provides security from manipulation. It is therefore assumed that no trust is needed anymore. As expected, the elimination of intermediaries from the transaction process shall lead to reduction of costs, savings in time and increased processing efficiency.[13]

The second key advantage of blockchain is considered to lie in the distribution of information in different nodes. Thanks to the fact that

---

[9] Lemieux, V. L. (2017) Op. cit., p. 22; Gabison, G. (2016) Policy Considerations for the Blockchain Technology Public and Private Applications. *SMU Science & Technology Law Review*, 189, pp. 330 ff.

[10] Szostek, D. (2018) *Blockchain a prawo.* Warszawa: C.H. Beck, pp. 49, 103 ff.; Vos, J. (2015) Blockchain-based Land Registry: Panacea, Illusion or Something in Between?. *7th ELRA Annual Publication*, pp. 16–19. [online] Available from: https://www.elra.eu/wp-content/uploads/2017/02/10.-Jacques-Vos-Blockchain-based-Land-Registry.pdf [Accessed 12 December 2018].

[11] Jeżak, Ł. (2019) *Blockchain Prywatny VS Blockchain Publiczny.* [online] Available from: https://bithub.pl/artykuly/blockchain-prywatny-vs-blockchain-publiczny/ [Accessed 14 April 2019].

[12] Thomas, R. (2017) Op. cit., p. 365.

[13] Thomas, R. (2017) Op. cit., pp. 365–366; Nogueroles Peiró, N. and Martinez García, E. J. (2017) Op. cit., p. 319; Lemieux, V. L. (2017) Op. cit., p. 23; Vos, J. (2015) Op. cit., p. 3.

the digital register, being a shared database, is replicated in each node, the system becomes more secure because any attack is more difficult.[14] Since a large number of users participate in the blockchain network, there is no single point of control. Consequently, even if a part of the network fails, the other parts continue to operate.[15] The idea of broadcasting the transactions to the blockchain network and the application of consensus mechanism shall contribute to solving the problem of double spending (this refers to a situation in which an owner of a digital currency file can easily make a copy of that file and send it to more than one person) or rather double selling (when considering the possibility to dispose of property simultaneously more than once).[16] As opposed to the above model, the existing land registries commonly use one central database.

It is also highlighted that all entries in the distributed database are public and can be viewed by the authorised users of the blockchain system (as indicated above, the access may be limited when dealing with a private blockchain). Therefore, the level of transparency shall be increased, given that every new block, once added to a public blockchain, is available for anyone to verify its authenticity.[17]

Finally, a positive attribute of blockchain is that the integrity of the system is ensured through the application of cryptographic techniques so that any attempt to change the information recorded can be easily detected. It is suggested that this solution ensures protection against potential frauds.[18]

3. INCONSISTENCIES AND CONTROVERSIES ABOUT THE IDEA OF A BLOCKCHAIN LAND REGISTRY

Notwithstanding the abovementioned potential advantages resulting from the use of blockchain technology in the land registration domain, there is a need to further analyse the blockchain construct in order to verify whether such a solution is indeed suitable for real estate transactions. Before examining in more detail some questionable issues in this regard, account

[14] Nogueroles Peiró, N. and Martinez García, E. J. (2017) Op. cit., pp. 300, 319.

[15] Thomas, R. (2017) Op. cit., p. 366.

[16] Vos, J. (2015) Op. cit., p. 5; Sklaroff, J. M. (2017) Op. cit., p. 269.

[17] Thomas, R. (2017) Op. cit., p. 366; Vos, J. (2015) Op. cit., p. 11; Spielman, A. (2016) Op. cit., p. 42.

[18] Thomas, R. (2017) Op. cit., p. 367; Lemieux, V. L. (2017) Op. cit., p. 22; Nogueroles Peiró, N. and Martinez García, E. J. (2017) Op. cit., p. 319.

must be taken of the complexity of rules governing land transfer and land registration as well as considerable socio-economic relevance of purchase of real estate given that the subject of such transactions are unique high--value assets.[19] This is demonstrated particularly by the role notaries and other specialised lawyers commonly play in the conveyancing and registration process. In most European countries, following the Latin model of notariat, notaries act as persons of public trust vested with competences to draw up agreements of transfer of immovable property and the form of notarial deed is required to complete the registration.[20] It should also be underlined that a common characteristics of land registration systems is that registers are maintained by public authorities, being either courts or administrative bodies, but at the same time further significant differences exist among registration regimes adopted in particular countries.[21]

For instance, in terms of the subject of registration a distinction is made between registers of titles and registers of deeds. With respect to title registration, rights on land are inscribed in the register upon prior examination of their legality. This system is characteristic e.g. for Poland, England and Wales, Germany, Spain and Sweden, to mention just a few European countries. By contrast, in case of deeds registration documents regarding land transactions are registered, basically without

---

[19] See e.g.: Barbieri, M. and Gassen, D. (2017) Blockchain – Can This New Technology Revolutionize the Land Registry System? In: *2017 World Bank Conference on Land and Poverty*, Washington DC, USA, 20–24 March, pp. 8, 11. Available from: http://www.notartel.it/export/contenuti_notartel/pdf/Land_Poverty_Conference_Blockchain.pdf [Accessed 12 December 2018]; Arruñada, B. (2018) Op. cit., p. 78; Méndez, F. P. (2018) *Smart Contracts, Blockchain and Land Registry.* [speech] European Land Registry Association (ELRA) General Assembly. Brussels, 30 November, pp. 7–8. Available from: https://www.elra.eu/wp-content/uploads/2018/12/Smart-Contracts-Blockchain-and-Land-Registry-by-F-Mendez.pdf [Accessed 18 December 2018].

[20] See e.g.: Blajer, P. (2018) *Rejestry nieruchomości – studium prawnoporównawcze.* Warszawa: C.H. Beck, pp. 183 ff.; Bertrand du Marais and David Marrani (eds.). (2016) *Legal Certainty in Real Estate Transactions: A Comparison of England and France.* Cambridge: Intersentia, passim. See also: Méndez, F. P. (2018) The Land Registrar as a Legal Professional. *7th ELRA Annual Publication*, pp. 1 ff. Available from: https://www.elra.eu/wp-content/uploads/2017/02/6.-Fernando-P.-Mendez-The-Land-Registrar-as-a-Legal-Professional.pdf [Accessed 7 January 2019].

[21] See e.g.: Blajer, P. (2018) Op. cit., pp. 337 ff.; Stawecki, T. (2002) Rejestry nieruchomości, księgi hipoteczne i księgi wieczyste od czasów najdawniejszych do XXI wieku. *Studia Iuridica*, 40, pp. 167–208; Martínez Velencoso, L. M. (2017) The Land Register in European Law: A Comparative and Economic Analysis. In: Luz M. Martínez Velencoso, Saki Bailey and Andrea Pradi (eds.). *Transfer of Immovables in European Private Law.* Cambridge: Cambridge University Press, pp. 3 ff.; Cámara Lapuente, S. (2005) Registration of Interests as a Formality of Contracts: Comparative Remarks on Land Registers within the Frame of European Private Law. *European Review of Private Law*, 6, pp. 798 ff.; Lodde, A. (2016) The European Systems of Real Estate Registration: An Overview. *Territorio Italia*, 1, pp. 23–42; Zevenbergen, J. (2002) *Systems of Land Registration: Aspects and Effects.* Delft: Netherlands Geodetic Commission (NCG), pp. 47 ff.

the identification of the last genuine title-holder. Thus, the land register is merely a collection of documents which only have to comply with formal requirements. However, modern registers of documents are often improved and well-organised. Examples of registers of that type can be found in Belgium, France, Italy and the Netherlands.[22] In addition, depending on particular system, registration may be of a constitutive or a declaratory character. Constitutive registration is necessary and decisive to create or transfer a right on real estate and is applied e.g. in Germany. Under the latter system registration is aimed only to disclose the legal status of real estate and make the transfer of a right opposable to third parties. Declaratory registration is a rule e.g. in France. In some legal orders (e.g. in Poland and Italy) the registration of the transfer of ownership is declaratory, while in case of the creation of limited real rights constitutive registration is required.[23] Other exemplary criteria include the format of registration (real folium or personal folium), public faith attributed to the content of the register (basically good faith in the land register is protected in case of constitutive registration) and the publicity of registered information (public access for everyone or access restricted to persons with a legitimate interest).[24]

Considering specific rules adopted in different land registration models, it can be argued that the precepts of the blockchain concept followed by the "original" – public blockchain are incompatible with main functions performed by the land registry in the title registration systems. These include principally: the information function, which consists in reducing uncertainty as to the legal status of land by providing detailed and complete land information; the protective function, relating to ensuring accuracy of information that can be relied on by persons acting in trust to the content of the land register, and the control function, connected with the power of the registration authority to check the correctness of the basis for entry in the register.[25] It is therefore clear that under the regime of title

[22] Blajer, P. (2018) Op. cit., pp. 226 ff.; Martínez Velencoso, L. M. (2017) Op. cit., pp. 9–12; Cámara Lapuente, S. (2005) Op. cit., pp. 831 ff. See also: Blajer, P. (2013) 'Deeds recordation' a 'title registration'. Rozwiązania modelowe w zakresie rejestrów nieruchomości w systemie 'common law'. *Zeszyty Prawnicze*, 13 (4), pp. 53–90.

[23] Lodde, A. (2016) Op. cit., pp. 37–38; Cámara Lapuente, S. (2005) Op. cit., pp. 809–812.

[24] Blajer, P. (2018) Op. cit., pp. 257 ff., 293 ff., 643 ff.; Lodde, A. (2016) Op. cit., pp. 36, 38, 40; Cámara Lapuente, S. (2005) Op. cit., pp. 832–833.

[25] Stawecki, T. (2005) *Rejestry publiczne. Funkcje instytucji.* Warszawa: Wydawnictwo Prawnicze LexisNexis, pp. 36 ff.; Gryszczyńska, A. (2011) Op. cit., pp. 41 ff.

registration the control of substantive aspects of a land transaction is essential, whereas blockchain registration basically excludes any intervention of a specialised authority and thus any external verification of the data submitted to the land register. In contrast to the rule of legality underlying registration of titles, in case of deeds registration systems the examination of documents carried out by registrars is limited to formal aspects. For this reason the latter model seems to correspond with the way the blockchain system is designed as it amounts to no more than a recordation of information.[26] Nevertheless, other specific aspects of land registration procedure need to be explored as well to determine whether a register of deeds could really follow the blockchain mechanism. Some of these issues will be addressed below.

Disintermediation, cited as one of main strengths of blockchain technology in the context of streamlining land registration, in fact raises many doubts. It should be pointed out that a consequence of how blockchain in its "hard" ("pure") form operates is that it cannot offer a legal presumption of accuracy of an entry, i.e. a presumption of validity of a transaction regarding land, nor a proof of ownership (in the sense of indicating the legitimate owner), which is the case of title registration systems. This is because validation of a transaction performed by miners may be considered in a technical sense but not in a legal sense so it cannot be treated as an equivalent of examination of the title carried out by the registrar. Instead, the only presumption that can be provided for is a factual presumption of authenticity which refers to the date of the transaction, the identity of the parties, the declarations made by them and the time the new block has been added to the chain.[27] In consequence, the information stored in the land register cannot be regarded as reliable.

What is more, the idea of blockchain infrastructure poses problems related to conferring priority which is the effect of both title registration and deeds registration. According to the existing rules governing land registration priority assigned to titles or deeds is dependent mainly on the time of application. Therefore, the moment a relevant document

[26] Cf. Nogueroles Peiró, N. and Martinez García, E. J. (2017) Op. cit., pp. 301 ff.; Arruñada, B. (2018) Op. cit., pp. 95–96; Méndez, F. P. (2018) Op. cit., p. 19.

[27] On this matter, it is justified to share the view of: Nogueroles Peiró, N. and Martinez García, E. J. (2017) Op. cit., pp. 315–316, 319. See also: Szczerbowski, J. J. (2018) *Lex cryptographia. Znaczenie prawne umów i jednostek rozliczeniowych opartych na technologii blockchain.* Warszawa: Wydawnictwo Naukowe PWN, pp. 42 ff.

arrives to the land registry is decisive to determine the rank in case of a conflict of rights to be registered. In this respect, instruments such as notices of submitted applications are of importance as they prevent the risk connected with the registration gap, i.e. the period between the completion of a transaction and the registration. The warning function of notices is enhanced if the applications are sent to the register electronically. When it comes to the blockchain system, there is no guarantee that the order in which transactions are received by the nodes is the same order in which new blocks are added, the reason being that the order is not based on chronology of applications and depends on a random act.[28] In such case the registration gap cannot be eliminated and it becomes difficult to prevent double selling.[29] The above risk is even greater in view of the fact that miners are rewarded for validating new transactions and receive fees for obtaining priority. Furthermore, in practice groups of miners, so-called mining pools or mining farms, are created in order to control most of the processing power so that the decentralisation of the blockchain system and the democratic nature of consensus must be put into question. Hypothetically, in such a situation a threat arises not only of manipulating the priority but also of depriving the legitimate owners of their property.[30] On this basis, it should be stated that the blockchain's operating methods do not prove appropriate even for deeds registration. After all, under this system priority is not conferred in a mechanical manner, taking into account the applicable rules on good faith and notices.

Another problematic issue connected with the way blockchain is structured regards legal liability in case of errors affecting the transactions to be recorded. This is because blockchain is based on the assumption that there is no single point of failure[31]. As for traditional land registration systems, normally the state liability is envisaged and a compensation is paid in case of a loss suffered due to mistakes from the land registry. When determining who shall bear the risk of mistakes or responsibility for blockchain system abuses we can consider the system administrator, the users of the system (collectively) as well as a person who has derived

[28] Nogueroles Peiró, N. and Martinez García, E. J. (2017) Op. cit., pp. 302–305.

[29] Méndez, F. P. (2018) Op. cit., pp. 15–16, 19–20.

[30] Barbieri, M. and Gassen, D. (2017) Op. cit., pp. 5, 11–12. See also: Gallego, L. (2016) Blockchain and Title Registration. *IPRA-CINDER International Review*, 1, pp. 49–50.

[31] Gabison, G. (2016) Op. cit., pp. 343 ff.

a benefit as a result of irregular transactions.[32] This matter is however more complicated due to the anonymity of the participants of the network which is one of the basic features of blockchain in its "original" form. Although the participating users are connected to digital certificates, their identity is not revealed. This also may entail a difficulty to establish the law applicable to liability in case miners represent different nationalities.[33] Again, the above problems can affect both title registration and deeds registration systems.

In this context the question concerning the anonymous character of blockchain should be developed. A situation in which the identity of the parties involved in the blockchain is not disclosed to the other users is incompatible with the very idea of land registers as one of their core functions is to ensure publicity. Overall, in conditions of anonymity real estate transactions would be hardly conceivable. In order to resolve these difficulties it is postulated that electronic IDs connected to the public keys could be used.[34] However, another problem arises – to determine who could receive a public key in the blockchain and under which procedure.[35] Moreover, the issue of privacy should be taken into account here.[36]

There are reasonable grounds to observe that due to the lack of an independent verification, the lack of disclosure of the network participants' identity and the risk of irregularities resulting therefrom, when dealing with a blockchain-based land registration – contrary to the arguments advanced by its advocates – the conveyancing costs can increase instead of decreasing. It can be assumed that the financial institutions providing services to parties may require the involvement of specialised intermediaries in the transactions as a means of hedging their risk; furthermore, extended due diligence exercises and title insurances may be needed.[37] Above all, one should consider the perspective of legal recourse as an indispensability. This also applies to situations in which an encryption key is lost or stolen and it is necessary to recover the property

---

[32] See further: Thomas, R. (2017) Op. cit., pp. 387 ff.; Gallego, L. (2016) Op. cit., pp. 30–31.

[33] Nogueroles Peiró, N. and Martinez García, E. J. (2017) Op. cit., pp. 313–314. Cf. Vos, J. (2015) Op. cit., p. 7.

[34] Verheye, B. (2017) Real Estate Publicity in a Blockchain World: A Critical Assessment. *European Property Law Journal*, 6 (3), pp. 458–459. See also: Vos, J. (2015) Op. cit., p. 14.

[35] Verheye, B. (2017) Op. cit., p. 459.

[36] Lemieux, V. L. (2017a) Op. cit., pp. 22–23.

[37] This is sensibly suggested by: Thomas, R. (2017) Op. cit., pp. 386–387.

associated with it.[38] These issues can become particularly problematic if we consider the use of blockchain in cross-border conveyancing, in view of the noticeable diversity of land registration systems.

In contrast to public blockchain, it can be assumed that the features of private or hybrid blockchains would allow some of the above problems to be overcome. Nevertheless, in such case the distributed nature of blockchain, promoted as one of its main advantages, is frustrated[39]. What is more, there is still a need for trust, which, indeed, shall be supposed to be unnecessary under the blockchain concept.[40]

4. PRACTICAL APPLICATION OF BLOCKCHAIN IN THE AREA OF LAND REGISTRATION – EXAMPLES

As mentioned above, the idea to convert land registers to blockchain databases is already being implemented in practice as shown by initiatives undertaken by governments in such countries as the Republic of Georgia, Sweden, Ukraine, Ghana, Brazil, Honduras, India and Japan. This proves that blockchain-based land registration is of interest to both developing and advanced economies. Recently, a debate on possibilities to use blockchain technology in the real estate market has also been launched in Poland with setting up the *Working Group on Distributed Ledgers and Blockchain* at the *Ministry of Digital Affairs*.[41] In order to illustrate potential solutions in this regard, experiences of Georgia, Sweden and Brazil will be outlined.

The Republic of Georgia is the first country that has started registering land titles using blockchain, with the aim to increase the level of trust. Georgia has developed a blockchain-based registration system as a result of cooperation between the *National Agency of Public Registry (NAPR)* and a bitcoin mining company *Bitfury*. It should be emphasised that before introducing blockchain technology the Georgian land registration system has been reformed for decades so that it has become relatively efficient and corruption-free.[42] The land register is based on a private permissioned blockchain, administered by *NAPR*, acting as a third party enforcer.

[38] Szczerbowski, J. J. (2018b) Transaction Costs of Blockchain Smart Contracts. *Law and Forensic Science*, 16 (2), pp. 1–6; Barbieri, M. and Gassen, D. (2017) Op. cit., p. 12; Graglia, J. M. and Mellon, C. (2018) Op. cit., p. 12.

[39] Vos, J. (2015) Op. cit., pp. 16 ff.

[40] Lemieux, V. L. (2017) Op. cit., p. 23.

[41] Ministerstwo Cyfryzacji. (2018) *Grupa robocza ds. rejestrów rozproszonych i blockchain.* Available from: https://www.gov.pl/web/cyfryzacja/grupa-robocza-ds-rejestrow-rozproszonych-i-blockchain [Accessed 4 January 2019].

The scope of the implemented project covers sale of land titles, registration of new titles, mortgages, rentals and notary services.[43] It is assessed that the above initiative has brought positive effects of increased trust and transparency and there are plans to introduce blockchain technology in other sectors of the administration as well.[44]

Another example of jurisdiction experimenting with blockchain is Sweden. In 2016 the Swedish land registration authority, *Lantmäteriet*, together with a group of partners (including a blockchain startup *ChromaWay*, a consulting company *Kairos Future* and a telecommunications company *Telia*) launched a pilot project to evaluate potential blockchain applications for real estate transactions. According to the assumptions blockchain could be used as a technical solution intended to make the well--functioning land register more efficient. Currently the process from signing the contract of sale until the registration of the property takes approximately 4 months, although the register is digitised and most real estate contracts are submitted to the registry in digital form.[45] The project has already undergone three stages. After two initial phases, including the proof of concept and building a testbed with working technology, the third stage, aimed at conducting a real-world property transfer using the blockchain system, was completed in June 2018.[46] The testbed created for the project is based on a private blockchain network. It is accessible only to authorised parties using a smart contract application that manages the transactions. It is designed to store verification records of documents

---

[42] Santiso, C. (2018) Will Blockchain Disrupt Government Corruption? *Stanford Social Innovation Review,* (March). [online] Available from: https://ssir.org/articles/entry/will_blockchain_disrupt_government_corruption [Accessed 21 December 2018].

[43] Graglia, J. M. and Mellon, C. (2018) Op. cit., pp. 33–34; Higgins, S. (2017) *Republic of Georgia to Develop Blockchain Land Registry.* [online] Available from: https://www.coindesk.com/bitfury-working-with-georgian-government-on-blockchain-land-registry [Accessed 21 December 2018]; Shin, L. (2017) The First Government to Secure Land Titles on the Bitcoin Blockchain Expands Project. *Forbes*, 7 February. Available from: https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/#2ae7c5184dcd [Accessed 21 December 2018]; Nimfuehr, M. (2017) *Blockchain Application Land Register: Georgia and Sweden Leading.* [online] Available from: https://medium.com/bitcoinblase/blockchain-application-land-register-georgia-and-sweden-leading-e7fa9800170c [Accessed 21 December 2018]; Nogueroles Peiró, N. and Martinez García, E. J. (2017) Op. cit., p. 317.

[44] Verheye, B. (2017) Op. cit., p. 448; Graglia, J. M. and Mellon, C. (2018) Op. cit., p. 34.

[45] McMurren, J., Young, A. and Verhults, S. (2018) *Addressing Transaction Costs Through Blockchain and Identity in Swedish Land Transfers.* [case study] pp. 4 ff. Available from: https://blockchan.ge/blockchange-land-registry.pdf [Accessed 14 November 2018]; Lemieux, V. L. (2017) Evaluating the Use of Blockchain in Land Transactions. *European Property Law Journal*, 6 (3), pp. 410 ff.; Graglia, J. M. and Mellon, C. (2018) Op. cit., p. 38; Nogueroles Peiró, N. and Martinez García, E. J. (2017) Op. cit., pp. 316–317; Verheye, B. (2017) Op. cit., pp. 447–448; Nimfuehr, M. (2017) Op. cit.

and not documents themselves, which shall be held by each party to the agreement. Moreover, verification records are summarised in an external blockchain that is transparent to the public. Professional users, such as banks, real estate agents and *Lantmäteriet*, access the contract in a professional interface, which can be integrated with their own systems. Administrators at the land registry and its technical partners administer the contract through a third interface, with changes overseen by all partners running the blockchain. The project also envisages the application of a digital ID system.[47]

Unlike Georgia and Sweden, Brazil lacks a modern integrated land registration system and faces challenges connected with corruption and frauds. The major part of the territory is untitled, there is no electronic database for examining encumbrances and the registration procedure is a complex one. In 19th century the *Torrens* system, based on registration of titles, was adopted in Brazil but it is not much used in practice.[48] A blockchain pilot project was launched in 2017 by the real estate registry office, *Cartório de Registro de Imóveis*, in cooperation with a blockchain technology company *Ubitquity* in the *State of Rio Grande do Sul*, *Municipalities of Pelotas* and *Morro Redondo*. It is expected that this initiative will improve accuracy, security and transparency of the land registration process as well as lower costs. The purpose of the project is to introduce a parallel blockchain platform to replicate the existing legal structure of property recording and transfer processes, with the use of the Software as a Service business model to record land transactions on behalf of companies and government agencies. The system architecture

---

[46] ChromaWay. (2018) *Blockchain and Future House Purchases: Third Phase to Be Completed in April 2018.* [online] Available from: https://chromaway.com/landregistry/ [Accessed 27 December 2018]; Kempe, M. (2016) *The Land Registry in the Blockchain: A Development Project with Lantmäteriet (The Swedish Mapping, Cadastre and Land Registration Authority), Telia Company, ChromaWay and Kairos Future.* [online] Available from: http://ica-it.org/pdf/Blockchain_Landregistry_Report.pdf [Accessed 27 December 2018]; Kempe, M. (2017) *The Land Registry in the Blockchain – Testbed. A Development Project with Lantmäteriet, Landshypotek Bank, SBAB, Telia Company, ChromaWay and Kairos Future.* [online] Available from: https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf [Accessed 27 December 2018]; Kim, C. (2018) *Sweden's Land Registry Demos Live Transaction on a Blockchain.* [online] Available from: https://www.coindesk.com/sweden-demos-live-land-registry-transaction-on-a-blockchain/ [Accessed 27 December 2018].

[47] McMurren, J., Young, A. and Verhults, S. (2018) Op. cit., p. 5; Kempe, M. (2017) Op. cit., pp. 59 ff. See also: Verheye, B. (2017) Op. cit., p. 458; Nogueroles Peiró, N. and Martinez García, E. J. (2017) Op. cit., p. 317.

[48] Blajer, P. (2013) Op. cit., p. 73; Cash, A. (2016) *Land Registration in Brazil: An Interview with Alex Ferreira Magalhães.* [online] Available from: http://www.rioonwatch.org/?p=29200 [Accessed 29 December 2018].

encompasses web frontend that captures information taken from the general real estate registry as well as a web server and backend storage. Additionally, *Colu Colored Coins* protocol is applied to record transactions on the *Bitcoin* blockchain. *Colored Coins* is a group of protocols and methods for representing and managing real world assets, such as real estate, as a data layer on top of a blockchain. In the longer term it is planned to create a system that would incorporate the features of blockchain technology to transform the existing recording and land transfer.[49]

5. CONCLUSION

Concerns raised in the course of the analysis show that blockchain technology in the "classic" form (the public type) is not suitable for the specificity of real estate transfer and land registration. The reason is that the idea behind the blockchain mechanism excludes the possibility to guarantee legal certainty and this applies not only to land registration systems based on title registration, in particular of constitutive character, but also to deeds registration systems under which land registration is not necessary to complete the transfer of ownership. Certainly, a land register cannot be equated to a simple database and land transfer is far more complex than the purchase of low-value consumer goods.

In consequence, blockchain could be applied provided it is adapted to the existing land registration architecture. Conditions to be met in this respect regard primarily limiting the access to the blockchain system and reducing the number of miners to persons fulfilling particular qualifications as well as ensuring proper identification of the users and defining liability rules. As an institutional infrastructure is indispensable to guarantee real property rights, only the use of a private or a hybrid blockchain, administered by the land registry and used by the current stakeholders of real estate transactions (like notaries and conveyancers) could be taken into consideration.[50]

---

[49] Lemieux, V. L. (2017b) Op. cit., pp. 403 ff.; Lemieux, V. L., Flores, D. and Lacombe, C. (2017) *Real Estate Transaction Recording in the Blockchain in Brazil (RCPLAC-01).* [case study] pp. 7 ff. Available from: http://blogs.ubc.ca/recordsinthechain/files/2018/01/RCPLM-01-Case-Study-1_v14_English_Final.pdf [Accessed 27 December 2018]; Graglia, J. M. and Mellon, C. (2018) Op. cit., p. 56; Keirns, G. (2017) *Blockchain Land Registry Tech Gets Test in Brazil.* [online] Available from: https://www.coindesk.com/blockchain-land-registry-tech-gets-test-brazil [Accessed 27 December 2018].

[50] In this regard, I concur with the arguments put forward by: Thomas, R. (2017) Op. cit., p. 390; Nogueroles Peiró, N. and Martinez García, E. J. (2017) Op. cit., p. 319; Verheye, B. (2017) Op. cit., pp. 465 ff.; Vos, J. (2015) Op. cit., p. 19.

This is also confirmed by the examples provided above (including systems representing the title registration model). In Sweden and Georgia, whose land registers are quite developed and have been digitised, public intervention is maintained and a private blockchain is used as a complementary technology supporting the existing registration systems. The Brazilian conveyancing system, in turn, is unsafe and therefore at the first stage of the pilot project blockchain is supposed to play a role of preserving the archive and facilitating its recovery in case of attack or loss. On this basis, it is reasonably recommended that applying blockchain technology should be preceded by digitisation of land registers.[51] At the same time, blockchain is rightly considered to have a potential in terms of storage of information.[52]

Furthermore, it should be observed that currently available technological solutions applied in the area of land registration prove to be sufficient to obtain effects considered as main blockchain's advantages, i.e. security, integrity and transparency. Particular reference should be made here to advanced methods of identification, based on digital signatures, as well as electronic time-stamping.[53] This shall call into question the justification for transforming land registers in blockchain databases as, indeed, the core novelty of blockchain consists in the distribution of information.

The above remarks lead to a conclusion that blockchain can be effectively used as a tool serving to improve the efficiency of the existing land registration systems, after an appropriate adjustment. It is therefore advisable to continue the discussion on optimal legal and technical ways of taking advantage of the possibilities offered by blockchain technology, in accordance with the principal functions of land registers.

LIST OF REFERENCES

[1] Anand, A., McKibbin, M. and Pichel, F. (2017) Colored Coins: Bitcoin, Blockchain, and Land Administration. In: *2017 World Bank Conference on Land and Poverty*, Washington DC, USA, 20–24 March. Available from: https://cadasta.org/resources/white-papers/bitcoin-blockchain-land/ [Accessed 12 December 2018].

[51] Graglia, J. M. and Mellon, C. (2018) Op. cit., p. 11.

[52] Nogueroles Peiró, N. and Martinez García, E. J. (2017) Op. cit., p. 318.

[53] This is also accurately pointed out by: Nogueroles Peiró, N. and Martinez García, E. J. (2017) Op. cit., p. 319.

[2] Arruñada, B. (2018) Blockchain's Struggle to Deliver Impersonal Exchange. *Minnesota Journal of Law, Science & Technology*, 19.

[3] Barbieri, M. and Gassen, D. (2017) Blockchain – Can This New Technology Revolutionize the Land Registry System? In: *2017 World Bank Conference on Land and Poverty*, Washington DC, USA, 20–24 March. Available from: http://www.notartel.it/export/contenuti_notartel/pdf/Land_Poverty_Conference_Blockchain.pdf [Accessed 12 December 2018].

[4] Blajer, P. (2013) 'Deeds recordation' a 'title registration'. Rozwiązania modelowe w zakresie rejestrów nieruchomości w systemie 'common law'. *Zeszyty Prawnicze*, 13 (4).

[5] Blajer, P. (2018) *Rejestry nieruchomości – studium prawnoporównawcze.* Warszawa: C.H. Beck.

[6] Brennan, G. (2015) *The Impact of eConveyancing on Title Registration: A Risk Assessment.* Cham: Springer.

[7] Cámara Lapuente, S. (2005) Registration of Interests as a Formality of Contracts: Comparative Remarks on Land Registers within the Frame of European Private Law. *European Review of Private Law*, 6.

[8] Cash, A. (2016) *Land Registration in Brazil: An Interview with Alex Ferreira Magalhães.* [online] Available from: http://www.rioonwatch.org/?p=29200 [Accessed 29 December 2018].

[9] ChromaWay. (2018) *Blockchain and Future House Purchases: Third Phase to Be Completed in April 2018.* [online] Available from: https://chromaway.com/landregistry/ [Accessed 27 December 2018].

[10] Cooke, E. (2003) E-conveyancing in England: Enthusiasms and Reluctance. In: David Grinlinton (ed.). *Torrens in the Twenty-first Century.* Wellington: LexisNexis.

[11] Gabison, G. (2016) Policy Considerations for the Blockchain Technology Public and Private Applications. *SMU Science & Technology Law Review*, 189.

[12] Gallego, L. (2016) Blockchain and Title Registration. *IPRA-CINDER International Review*, 1.

[13] Gołaczyński, J. and Klich, A. (2016) Informatyzacja ksiąg wieczystych. Uwagi ogólne. In: Andrzej Marciniak (ed.). *Elektronizacja postępowania wieczystoksięgowego. Komentarz praktyczny. Akty wykonawcze*. Warszawa: C.H. Beck.

[14] Graglia, J. M. and Mellon, C. (2018) Blockchain and Property in 2018: At the End of the Beginning. In: *2018 World Bank Conference on Land and Poverty*, Washington DC, USA, 19–23 March. [online] Available from: https://www.conftool.com/landandpoverty

2018/index.php?page=downloadPaper&ismobile=true&filename=02-11-Graglia-864_paper.pdf&form_id=864&form_version=final [Accessed 22 December 2018].

[15] Gryszczyńska, A. (2011) *Nowa Księga Wieczysta. Informatyzacja rejestru publicznego.* Warszawa: LexisNexis.

[16] Higgins, S. (2017) *Republic of Georgia to Develop Blockchain Land Registry.* [online] Available from: https://www.coindesk.com/bitfury-working-with-georgian-government-on-blockchain-land-registry [Accessed 21 December 2018].

[17] Jeżak, Ł. (2019) *Blockchain Prywatny VS Blockchain Publiczny.* [online] Available from: https://bithub.pl/artykuly/blockchain-prywatny-vs-blockchain-publiczny/ [Accessed 14 April 2019].

[18] Kaczorowska, M. (2019) Informatisation of Land Registers in Poland and Other Member States of the European Union: A Comparative Overview. *Law and Forensic Science*, 17 (1).

[19] Keirns, G. (2017) *Blockchain Land Registry Tech Gets Test in Brazil.* [online] Available from: https://www.coindesk.com/blockchain-land-registry-tech-gets-test-brazil [Accessed 27 December 2018].

[20] Kempe, M. (2016) *The Land Registry in the Blockchain: A Development Project with Lantmäteriet (The Swedish Mapping, Cadastre and Land Registration Authority), Telia Company, ChromaWay and Kairos Future.* [online] Available from: http://ica-it.org/pdf/Blockchain_Landregistry_Report.pdf [Accessed 27 December 2018].

[21] Kempe, M. (2017) *The Land Registry in the Blockchain – Testbed. A Development Project with Lantmäteriet, Landshypotek Bank, SBAB, Telia Company, ChromaWay and Kairos Future.* [online] Available from: https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf [Accessed 27 December 2018].

[22] Kim, C. (2018) *Sweden's Land Registry Demos Live Transaction on a Blockchain.* [online] Available from: https://www.coindesk.com/sweden-demos-live-land-registry-transaction-on-a-blockchain/ [Accessed 27 December 2018].

[23] Lemieux, V. L. (2017) Blockchain Recordkeeping: A SWOT Analysis. *Information Management*, 51 (6).

[24] Lemieux, V. L. (2017) Evaluating the Use of Blockchain in Land Transactions. *European Property Law Journal*, 6 (3).

[25] Lemieux, V. L., Flores, D. and Lacombe, C. (2017) *Real Estate Transaction Recording in the Blockchain in Brazil (RCPLAC-01).* [case study] Available from: http://blogs.ubc.ca/recordsinthechain/files/2018/01/RCPLM-01-Case-Study-1_v14_English_Final.pdf [Accessed 27 December 2018].

[26] Lodde, A. (2016) The European Systems of Real Estate Registration: An Overview. *Territorio Italia*, 1.

[27] Bertrand du Marais and David Marrani (eds.). (2016) *Legal Certainty in Real Estate Transactions: A Comparison of England and France.* Cambridge: Intersentia.

[28] Martínez Velencoso, L. M. (2017) The Land Register in European Law: A Comparative and Economic Analysis. In: Luz M. Martínez Velencoso, Saki Bailey and Andrea Pradi (eds.). *Transfer of Immovables in European Private Law.* Cambridge: Cambridge University Press.

[29] McMurren, J., Young, A. and Verhults, S. (2018) *Addressing Transaction Costs Through Blockchain and Identity in Swedish Land Transfers.* [case study] Available from: https://blockchan.ge/blockchange-land-registry.pdf [Accessed 14 November 2018].

[30] Méndez, F. P. (2018) *Smart Contracts, Blockchain and Land Registry.* [speech] European Land Registry Association (ELRA) General Assembly. Brussels, 30 November. Available from: https://www.elra.eu/wp-content/uploads/2018/12/Smart-ontracts-Blockchain-and-Land-Registry-by-F-Mendez.pdf [Accessed 18 December 2018].

[31] Méndez, F. P. (2018) The Land Registrar as a Legal Professional. *7th ELRA Annual Publication.* Available from: https://www.elra.eu/wp-content/uploads/2017/02/6.-Fernando-P.-Mendez-The-Land-Registrar-as-a-Legal-Professional.pdf [Accessed 7 January 2019].

[32] Ministerstwo Cyfryzacji. (2018) *Grupa robocza ds. rejestrów rozproszonych i blockchain.* Available from: https://www.gov.pl/web/cyfryzacja/grupa-robocza-ds-rejestrow-rozproszonych-i-blockchain [Accessed 4 January 2019].

[33] Nakamoto, S. (2008) *A Peer-to-Peer Electronic Cash System.* [online] Available from: https://bitcoin.org/bitcoin.pdf [Accessed 12 December 2018].

[34] Boucher, P., Nascimento, S. and Kritikos, M. (2017) *How Blockchain Technology Could Change Our Lives: In-depth Analysis.* Brussels: European Parliament Research Service.

[35] Niemi, M. I. (2017) Electronic Conveyancing of Real Property in Europe: Two Models. The English and the Finnish One. In: Luz M. Martínez Velencoso, Saki Bailey and Andrea Pradi (eds.). *Transfer of Immovables in European Private Law.* Cambridge: Cambridge University Press.

[36] Nimfuehr, M. (2017) *Blockchain Application Land Register: Georgia and Sweden Leading.* [online] Available from: https://medium.com/bitcoinblase/blockchain-application-land-register-georgia-and-sweden-leading-e7fa9800170c [Accessed 21 December 2018].

[37] Nogueroles Peiró, N. and Martinez García, E. J. (2017) Blockchain and Land Registration Systems. *European Property Law Journal*, 6 (3).

[38] Santiso, C. (2018) Will Blockchain Disrupt Government Corruption? *Stanford Social Innovation Review* (March). [online] Available from: https://ssir.org/articles/entry/will_blockchain_disrupt_government_corruption [Accessed 21 December 2018].

[39] Shin, L. (2017) The First Government to Secure Land Titles on the Bitcoin Blockchain Expands Project. *Forbes*, 7 February. Available from: https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/#2ae7c5184dcd [Accessed 21 December 2018].

[40] Sklaroff, J. M. (2017) Smart Contracts and the Cost of Inflexibility. *University of Pennsylvania Law Review*, 166 (1).

[41] Spielman, A. (2016) *Blockchain: Digitally Rebuilding the Real Estate Industry.* [online] Ph.D. Massachusetts Institute of Technology. Available from: https://dspace.mit.edu/bitstream/handle/1721.1/106753/969450770-MIT.pdf?sequence=1 [Accessed 14 December 2018].

[42] Stawecki, T. (2002) Rejestry nieruchomości, księgi hipoteczne i księgi wieczyste od czasów najdawniejszych do XXI wieku. *Studia Iuridica*, 40.

[43] Stawecki, T. (2005) *Rejestry publiczne. Funkcje instytucji.* Warszawa: Wydawnictwo Prawnicze LexisNexis.

[44] Szczerbowski, J. J. (2018a) *Lex cryptographia. Znaczenie prawne umów i jednostek rozliczeniowych opartych na technologii blockchain.* Warszawa: Wydawnictwo Naukowe PWN.

[45] Szczerbowski, J. J. (2018b) Transaction Costs of Blockchain Smart Contracts. *Law and Forensic Science*, 16 (2).

[46] Szostek, D. (2018) *Blockchain a prawo.* Warszawa: C.H. Beck.

[47] Tapscott, D. and Tapscott, A. (2016) *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World.* New York: Portfolio/Penguin.

[48] Thomas, R. (2017) Blockchain's Incompatibility for Use as a Land Registry: Issues of Definition, Feasibility and Risk. *European Property Law Journal*, 6 (3).

[49] Verheye, B. (2017) Real Estate Publicity in a Blockchain World: A Critical Assessment. *European Property Law Journal*, 6 (3).

[50] Vos, J. (2015) Blockchain-based Land Registry: Panacea, Illusion or Something in Between?. *7th ELRA Annual Publication*. [online] Available from: https://www.elra.eu/wp-content/uploads/2017/02/10.-Jacques-Vos-Blockchain-based-Land-Registry.pdf [Accessed 12 December 2018].

[51] Wudarski, A. (2016) Das Grundbuch in der Registerwelt. Eine rechtsvergleichende Untersuchung zum deutschen und polnischen Grundbuch im europäischen Kontext. In: Arkadiusz Wudarski (ed.). *Das Grundbuch im Europa des 21. Jahrhunderts.* Berlin: Duncker & Humblot.

[52] Young, S. (2018) Changing Governance Models by Applying Blockchain Computing. *The Catholic University Journal of Law & Technology*, 26 (2).

[53] Zevenbergen, J. (2002) *Systems of Land Registration: Aspects and Effects.* Delft: Netherlands Geodetic Commission (NCG).

DOI 10.5817/MUJLT2019-2-9

ALGORITHMIC COPYRIGHT ENFORCEMENT AND AI: ISSUES AND POTENTIAL SOLUTIONS, THROUGH THE LENS OF TEXT AND DATA MINING

by

ANDREA KATALIN TÓTH*

Although digitalization and the emergence of the Internet has caused a long-term crisis for copyright law, technology itself also seems to offer a seemingly ideal solution to the challenges of digital age: copyright has been a major use case for algorithmic enforcement from the early days of digital rights management technologies to the more advanced content recognition algorithms. These technologies identify and filter possibly infringing content automatically, effectively and often in a preventive fashion. These methods have been criticized for their shortcomings, such as the lack of transparency, bias and the possible impairment of fundamental rights. Self-learning machines and semi-autonomous AI have the potential to offer even more sophisticated and expeditious enforcement by code, however, they could also aggravate the aforementioned issues. As the EU legislator envisions to make the use of such technologies essentially obligatory for certain online content sharing service providers (via the infamous Article 17 of the directive on copyright in the digital single market), the assessment of the situation in light of future technological development has become a current topic.

This paper aims to identify the main issues and potential long-term consequences of creating legislation that practically requires the employment of such filtering algorithms as well as their solutions. This paper focuses

* andreakatalin.toth@gmail.com, legal officer at the Department of International Copyright Law, Hungarian Intellectual Property Office; Ph.D. candidate at the Department of Civil Law of Eötvös Loránd University Faculty of Law and Political Science in Budapest, Hungary.

on the potential role a broad copyright exception for text and data mining could play in counterbalancing the issues associated with algorithmic enforcement.

KEY WORDS

AI, Copyright Law, EU Law, Machine Learning, Technology, Text and Data Mining

1. INTRODUCTION: COPYRIGHT, EXCEPTIONS AND TECHNOLOGY

The purpose and aim of copyright law has traditionally been described along two major theoretical views: according to the utilitarian approach, copyright's goal is to promote the advancement of learning and culture by providing certain exclusive rights to authors and creators in order to stimulate the production and dissemination of intellectual works, while the natural rights-based justification argues that the relevant rights need to be afforded to authors and creators as a reward for their intellectual labour, as well as a protection of their personality enshrined in their works.[1] Even though the two main copyright law regimes, the common law based "copyright" system and the *droit d'auteur* (authors' rights) approach prevalent in continental Europe formulate and emphasize these ideas differently,[2] the underlying concept is similar in each jurisdiction. From an economic aspect, these exclusive rights (such as: right of reproduction, right of distribution, public performance, creation of derivative works) incentivize and reward the intellectual labour of copyright holders (who are usually the authors of the work), by giving them the sole authority to license and authorize the use and exploitation of their copyright--protected works to third parties.

However, this power does not create an absolute monopoly for the right holder: for the sake of long-term development, and in order to make

[1] Fisher, W. W. (2001) Theories of Intellectual Property. In: Stephen Munzer (ed.). *New Essays in the Legal and Political Theory of Property.* 1st ed. Cambridge: Cambridge University Press, pp. 169–171.

[2] Although the most obvious example of the embodiment of this idea is Article I. Section 8. Clause 8. of the United States' Constitution, it also appears in Recitals (2), (4) and (10) of the most important European copyright directive, the InfoSoc Directive (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* (2001/L-167/10) 22 June. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001L0029&from=EN [Accessed 10 January 2019]) as well as in the recital of the Hungarian Copyright Act, thus this concept is also deeply embedded in the continental "authors' rights" regimes.

the knowledge incorporated in copyright-protected works more easily accessible, some limitations on these exclusive rights have been put in place. One way to limit copyright is by introducing different exceptions[3] by declaring that certain specific uses that do not conflict with the normal exploitation of works and do not unreasonably prejudice the legitimate interests of the right holder[4] do not necessitate prior authorization and/or payment of royalties. These uses are excepted for different reasons, for instance due to their *de minimis* impact on right holders' rights (e.g. temporary acts of reproduction) or their socially beneficial nature (e.g. teaching illustration, criticism).[5] At the same time, however, exceptions also serve as an important tool for balancing between the legitimate economic interests of copyright holders and the fundamental rights (most importantly the freedom of expression and information) of users.

Another important feature of copyright law for the purposes of this paper is its connection to technology and the way the development of this specific field of law and the advancement of technology have always been closely intertwined: the appearance of the movable type and printing press and their contribution to the technology of dissemination of information proved to be a disruptive technology and resulted in the need for

[3] Even though there is no opportunity to explore the topic in detail in this paper, the distinction between the Anglo-American style of *fair use* or *fair dealing* system and the exhaustive list of exceptions found in continental European *droit d'auteur* regimes should be mentioned in relation to the subject of copyright limitations and exceptions. The former, more flexible scheme relies on the judicial interpretation of certain standards. Judges evaluate the following four factors in relation to the allegedly infringing use: (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work (Sec. 107, Copyright Act of 1976). In contrast, the continental European system accommodates clearly and narrowly defined exceptions implemented by way of legislation (see also InfoSoc Directive, Article 5). For more on the American style fair use see: Leval, P. N. (1990) Toward a Fair Use Standard. *Harvard Law Review*, 103, p. 1105; Fisher, W. W. (1988) Reconstructing the Fair Use Doctrine. *Harvard Law Review*, 101 (8), p. 1659; Thatcher, S. G. (2006) Fair Use in Theory and Practice: Reflections on its History and the Google Case. *Journal of Scholarly Publishing*, 37 (3), pp. 215–229; Richard, K. (2018) Fair Use in the Information Age. *Richmond Journal of Law & Technology*, 25 (1); or the U.S. Copyright Office's information. United States Copyright Office. (2019) *More information on fair use.* [online] Washington, D. C.: USCO. Available from: https://www.copyright.gov/fair-use/more-info.html [Accessed 23 May 2019].

[4] This set of requirements is known as the "three step test" and it ensures that exceptions would not truncate copyright protection to an unjustified extent. The test first appeared in Article 9 of the *Berne Convention for Protection of Literary and Artistic Works* and the concept later became also enshrined in Article 13 of the *Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)*, as well as Article 5 paragraph (5) of the InfoSoc Directive.

[5] Stamatoudi, I. and Torremans, P. (2014) *EU Copyright Law, a Commentary.* 1st ed. Cheltenham: Edward Elgar Publishing Limited, p. 441.

an exclusive right for publishers in order to secure their business. This later developed into an exclusive right for the authors of works,[6] and led to the appearance of copyright as a distinct field of law.[7] Throughout its history, technology and new technological inventions have had the most relevant impact on copyright's evolution: new inventions, such as the *Xerox* machine, the audio cassette or the VCR not only accommodated new forms of uses, but also upset the above-mentioned balance between the interests of right holders and users.[8] The most dramatic change and challenge for copyright law so far has proved to be digitalization and the emergence of the Internet. In this new, digital environment the costs of copying and sharing information and copyright-protected content converge towards zero, which fosters unauthorized mass production and distribution, and thus mass infringement.[9] As digital uses of copyright-protected works usually occur in a cross-border manner (given the globalized nature of the Internet) and under anonymity ensured by the World Wide Web, the proper enforcement of exclusive rights became exponentially more difficult for right holders. Many scholars, commentators, policymakers and legislators sought to find a solution to this "crisis" situation, by legislative or extra-legislative means, however, these efforts did not always bring the desired results.[10] Concerning law making, as the legislative process is and will always be slower than technological development, the application and interpretation of existing laws to new technologies and solutions constitutes another problem in the context of technological neutrality. Though this overarching principle of lawmaking aims to ensure that legal provisions are constructed in a way that is independent from any particular

---

[6] The first copyright act, the Statute of Anne was adopted in 1710 in Great Britain and it deviated from the earlier legislation that gave publishing monopoly to the Stationer's Company (an exclusive group of printers and booksellers) and it vested the rights and protection in the authors themselves. See: Joyce, C. (ed.). (2013) *Copyright Law.* 9th ed. New Providence: LexisNexis, pp. 17–19.

[7] Joyce, C. (ed.). (2013) Op. cit., p. 16.

[8] Latman, A. and Patry, W. F. (1986) *Latman's the Copyright Law.* 6th ed. Washington, D.C.: Bureau of National Affairs.

[9] Joyce, C. (ed.). (2013) Op. cit., pp. 45–47.

[10] For more on this, see: Mills, M. L. (1989) New Technology and the Limitations of Copyright Law: An Argument for Finding Alternatives to Copyright Legislation in an Era of Rapid Technological Change. *Chicago-Kent Law Review*, 65 (1); Geller, P. E. (2008) Beyond the Copyright Crisis: Principles for Change. *Journal of the Copyright Society of the USA*, 55, pp. 165–199; Litman, J. (2002) Revising Copyright Law for the Information Age. In: Adam Thierer and Wayne Crews (eds.). *Copy Fights: The Future of Intellectual Property in the Information Age.* 1st ed. Washington, D. C.: Cato Institute.

technology without any negative or positive discrimination,[11] the different approaches towards its conceptualization can lead to very different results.[12] Thus, even the more flexible and reactive jurisprudence and case law is unable to guarantee an adequate, appropriate and uniform answer to the questions of copyright law brought about by emerging new technologies.

2. ALGORITHMIC COPYRIGHT ENFORCEMENT AND ITS EVOLUTION

The so-called algorithmic enforcement of copyright appeared in light of the aforementioned problem triggered by digitalization and the spread of the Internet. As it became clear that the traditional ways of enforcement were inefficient and costly (individual users behind online infringements became extremely difficult to track down and identify and they are typically judgement-proof against large sums of damages), the idea of using technology itself to solve the issues brought about by technology appeared,[13] and the concept of controlling digital uses by digital means came to light.

In copyright, the first generation of algorithmic enforcement tools comprised of the so-called technological protection measures (TPM) [also known as digital rights management, or DRM technologies in the United States], which operated as digital locks: right holders could technically prevent unauthorized access to and control the subsequent use of the digital formats of their works, by way of encryption.[14] This provided a well--functioning technology for right holders, and ensured that users could only gain access to legally acquired works; the option to make digital copies was either completely disabled or limited to a small number of copies or even

[11] Greenberg, B. A. (2016) Rethinking Technology Neutrality. *Minnesota Law Review*, 100 (4), p. 1513.

[12] A more restrictive understanding of technological neutrality could result in the rigid application of old law to new technology regardless of its potential impact on the development of said technology, while the more laxed views also consider achieving equivalent outcomes and maintaining the purpose of copyright law itself. This can lead to opposing results when assessing whether an act is copyright-relevant or not. See: Craig, C. J. (2017) Technological Neutrality: Recalibrating Copyright in the Information Age. *Theoretical Issues in Law*, 17 (2), pp. 608–615.

[13] About the idea that "code is law" and the role of technology as a means for indirect regulation, see: Lessig, L. (2006) *Code v. 2.0.* [online] New York: Basic Books. Available from: http://codev2.cc/download+remix/Lessig-Codev2.pdf [Accessed 10 January 2019].

[14] Perel, M. and Elkin-Koren, N. (2016) Accountability in Algorithmic Copyright Enforcement. *Stanford Technology Law Review*, 19 (3), p. 484.

a restriction regarding the type and number of the devices used for the enjoyment of the works could be applied.[15] The most known applications of this technology were *CSS (Content Scrambling System)*, *Apple's Fair Play* or *Adobe's DRM*. These technologies suffered from a number of shortcomings: as they were easily hacked, an additional legal protection (in the form of the prohibition of the circumvention of TPM) was needed. In addition, even the introduction of such provisions could not help to remedy other problems, such as TPMs causing security risks and slowing down computers, limiting consumers' ability to enjoy their legally bought products by only letting them to access their content on a limited number of devices or generally overriding copyright exceptions by being overly preventive by design.[16] Although some technological tools to accommodate exceptions existed at the time (such as interoperability, the partitioning and authentication of users), they were not and could not be employed by the majority of TPM technologies.[17]

With the spread of social media and the emergence of platforms such as *Facebook*, *YouTube*, or *Instagram* as well as the proliferation of user--generated content that these new platforms enabled, the second generation of algorithmic enforcement technologies appeared. The main focus of these new tools became the online availability of copyright protected content.[18] *Facebook's Rights Manager*[19] or *YouTube's Content ID*[20] offer right holders a nuanced approach to digital copyright management. The best way to illustrate the functioning of such systems is through the example of *YouTube's ContentID* algorithm. Through this mechanism, right holders provide to *YouTube* information and data about their works that they do not wish to see unauthorized copies of on the video-sharing platform. Based on these data a digital fingerprint for that specific piece of content is generated. Each time a new video is uploaded to *YouTube*, the algorithm

[15] Kerr, I. (2010) Digital Locks and the Automation Virtue. In: Michael Geist (ed.). *From „Radical Extremism" to „Balanced Copyright": Canadian Copyright and the Digital Agenda.* 1st ed. Toronto: Irwin Law, p. 267.

[16] Myška, M. (2009) The True Story of DRM. *Masaryk University Journal of Law and Technology*, 3 (2), pp. 272–277.

[17] Akester, P. (2009) *Technological Accomodation of Conflicts between Freedom of Expression and DRM: The First Empirical Assessment.* Rochester, New York: Social Science Research Network, p. 103.

[18] Perel, M. and Elkin-Koren, N. (2016) Op. cit., pp. 478–481.

[19] Facebook. (2019) *Rights Manager.* [online] Available from: https://rightsmanager.fb.com/ [Accessed 10 January 2019].

[20] YouTube. (2019) *Copyright Management Tools – Content ID.* [online] Available from: https://support.google.com/youtube/answer/9245819 [Accessed 10 January 2019].

checks whether there are any matches between any of the fingerprints in the library and the video in question. In the event of a newly uploaded video matching a fingerprint, it becomes flagged as potentially infringing content. As a consequence, the right holder has a few options to choose from: they can follow the viewership statistics of the flagged video, block access to it, or they can also claim all advertising revenues in case the allegedly infringing video is monetized.[21] According to *YouTube's* statistics, *ContentID* is used by more than 9,000 partners, including television broadcast companies, movie studios as well as record companies, while the reference library contains more than 75 million digital fingerprints.[22] Nevertheless, it also means that the main beneficiaries of the *ContentID* mechanism are high-profile entertainment companies whose protected works are used in large numbers. As the employment of this technology necessitates the ownership of a significant amount of copyright-protected content, the submission of a high number of valid takedown requests and the resources to manage them, *ContentID* and its options mentioned above are mostly available for large and economically significant right holders.[23] Smaller companies owning copyright-protected content can benefit from the *Content Verification Tool*, which only makes it possible for the right holders to search for and request the removal of potentially infringing videos.[24] Creators of smaller scale (typically the authors of user-generated content) are offered the *Copyright Match Tool*, which scans the platform for unauthorized uploads of original videos. However, in case of matching content, the authors are only offered more limited options: they can email the uploader, request the immediate removal of the matched content, request a scheduled removal or archive the match without taking any action.[25] Thus, it is clear that the biggest actors in the industry dispose of the widest array of possibilities and most effective tools for enforcement, while smaller entities and creators of original content (who constitute the basis of *YouTube's* functioning and philosophy) have

[21] YouTube. (2019) *How Content ID works.* [online] Available from: https://support.google.com/youtube/answer/2797370?hl=en&ref_topic=2778544 [Accessed 10 January 2019].

[22] YouTube. (2019) *YouTube in Numbers.* [online] Available from: https://www.youtube.com/yt/about/press/ [Accessed 14 June 2019].

[23] YouTube. (2019) *Copyright Management Tools.* [online] Available from: https://support.google.com/youtube/answer/9245819?hl=en [Accessed 14 June 2019].

[24] YouTube. (2019) *Content Verification Program.* [online] Available from: https://support.google.com/youtube/answer/6005923 [Accessed 14 June 2019].

[25] YouTube. (2019) *Copyright Match Tool.* [online] Available from: https://support.google.com/youtube/answer/7648743 [Accessed 14 June 2019].

more constrained options to enforce their rights. The most striking difference is the lack of the option for monetization, the potential to claim the advertising revenues off the potentially infringing videos.

Even more so that this latter option is what provides the apparent benefit of the second generation systems: contrary to the first generation of enforcement technologies, they enable an *ex post facto* licensing mechanism through the possibility of claiming ad-revenues.[26] However, this solution is not completely in line with copyright law's concept: no prior authorization is granted as the collection of revenues takes place after the actual use has already happened; there is no direct agreement between the right holder and the user, thus there is no enforceable contract in place for the purpose of using the protected work. The punitive nature of the redirecting of revenues is also foreign in the licensing practice. At the same time, the content of the videos at least remain accessible to the public. This scheme accommodates freedom of expression and information better, as the default option is not to completely block the potentially infringing content, but to keep it accessible in order to generate revenue for the right holder. At first glance, this mechanism seems to offer a near to ideal solution to the digital copyright law crisis: videos can still be watched by the passive, consumer public, while right holders receive income after the use of their works. Nevertheless, the uncertainty about the type of content that can actually trigger the algorithm and would be flagged and qualified as infringing carries the potential to create a discouraging environment for active users (especially those producing user-generated content), resulting in self--censorship.

3. THE POTENTIAL ISSUES OF ALGORITHMIC COPYRIGHT ENFORCEMENT

Even though the technologies introduced in the previous chapter cater for an effective and seemingly well-functioning enforcement of digital copyright, the potential drawbacks of and issues caused by these algorithmic measures need to be considered and evaluated as well.

One of the main problems derives from the fact that codes and algorithms used as the basis of these technologies are mostly treated

[26] Perel, M. and Elkin-Koren, N. (2016) Op. cit., p. 512–513.

as trade secrets and as such are kept hidden from the public eye in order to secure competitive advantage as well as to prevent users from "playing the system" by exploiting loopholes in the functioning of the algorithms. The resulting non-transparency can lead to overprotection and abuse of power through a lack of accountability.[27] As a consequence, individuals with the intent to legitimately use these platforms are unable to adjust their behaviour to be compliant due to their unawareness of the boundaries of the rules implied by technology. The uncertainty about the type of content that can actually trigger the algorithm and would be flagged and qualified as infringing carries the potential to create a discouraging environment for active users, especially those producing user-generated content and resulting in self-censorship. Given that social media and content sharing platforms were specifically built on the idea of users creating and sharing their own original content, this issue goes to the core of the functioning of these service providers.

The second identified issue is that right holders can effectively disable copyright exceptions by exercising excessively strict control over their content. The problem with the current content identification technologies (including *YouTube's Content ID*) is that although they are capable of filtering out identical or matching content, they are not sophisticated enough to be able to distinguish infringing use from uses that fall under one of the categories of exceptions.[28] Thus, even excepted uses could be flagged and blocked from public availability. An illustrative example is of a review video about a newly released movie: in order to get the point across and to give a foundation to their arguments, the reviewer has the option to use some footage from the movie, which (also considering the extent of the use) could easily qualify as a copyright exception as comment or criticism.[29] Whether inside or outside of the realm of copyright exceptions, disproportionality may present another issue. The terms of the after-the-fact quasi licence contract (which essentially bears the characteristics of a "compulsory licence") embodied in the demonetization and ad-revenue claims could be highly unfair and disproportionate to the actual use of the protected content.[30] For instance, the use of a few seconds of a song as background music in a vlog or a gaming stream could essentially

[27] Op. cit., p. 483.

[28] Bartholomew, T. B. (2015) The Death of Fair Use in Cyberspace: YouTube and the Problem with Content ID. *Duke Law & Technology Review*, 13 (1), p. 70.

"hijack" the advertising revenue of videos of substantial length and views.[31] Regarding the incidental inclusion exception in EU copyright law and other jurisdictions where *de minimis* use falls outside of the scope of copyright protection, this issue relates back to the limitations of copyright.[32]

Finally, whenever legal provisions are translated into code, private and potentially biased actors analyse and interpret the law. As these entities determine the metes and bounds of specific rules, they have a substantial potential in building bias into the code that would favour their interests and discriminate against certain other individuals or groups.[33] The most possible form of bias in the context of enforcement algorithms is technical bias that originates from trying to make human constructs, such as a judgement on the substance of a legal provision, interpretable for computers.[34] Given that the interpretation of law is traditionally a public function

---

[29] In EU copyright law, Article 5, para. (3) d) of the InfoSoc Directive states that Member States may provide for exceptions or limitations to the rights of reproduction and communication to the public in the case of quotations for purposes of such as criticism or review, provided that they relate to a work or other subject matter which has already been lawfully made available to the public, the use is in accordance with fair practice, and to the extent required for the specific purpose. Similarly, Section 107 of the US Copyright Act (17 U.S. Code) states that criticism and comment are of the specific purposes that might warrant fair use in light of the evaluation of the four factors. For a specific example, a movie review about an infamously "bad" movie was given a copyright strike and blocked by the movie's director three days after its release. For the original review video see: I Hate Everything. (2015) *Cool Cat Saves The Kids – The Search For The Worst.* [online video] Available from: https://www.youtube.com/watch?v=HoTZZYm2HZI&t=42s [Accessed 10 January 2019]; for a comment on the video's removal and fair use, see e.g.: Channel Awesome. (2016) *Where's The Fair Use – Nostalgia Critic.* [online video] Available from: https://www.youtube.com/watch?v=zVqFAMOtwaI&t=53s [Accessed 10 January 2019].

[30] Bartholomew, T. B. (2015) Op. cit., p. 66.

[31] One of the most popular YouTubers with a significant number of subscribers, *Felix Kjellberg* (a.k.a. *PewDiePie*) often complains about record labels and production companies claiming the advertising revenue of his gameplay videos (the length of which can extend up to a few hours) for the use of a few seconds of a copyright protected song (that sometimes appear as part of the video-game itself). See for example: PewDiePie. (2017) *Life is cringe – life is strange – S2E01*. [online video] Available from: https://www.youtube.com/watch?v=PX4zk0G4IjM [Accessed 10 January 2019].

[32] Article 5 (3) (i) states that Member States may provide for exceptions or limitations to the rights of reproduction and communication to the public for the incidental inclusion of a work or other subject-matter in other material. This provision creates a legal basis for the introduction of *de minimis* limitations in EU countries' national laws. In the USA, trivial, or *de minimis* use is often allowed by courts. It means that the unauthorized use in question is so small and irrelevant that it would weigh against the finding of infringement both regarding the substantiality of the portion taken and the possible effect of the use on the potential market of the protected work (the third and fourth factors described above in footnote 2.). This doctrine has been developed by case law, mostly in relation to background objects appearing in movies. See: *Ringgold v. Black Entertainment Television, Inc.* (1997) 126 F.3d70, 16 September; *Sandoval v. New Line Cinema Corp.* (1998) 147 F.3d 215, 24 June; *Newton v. Diamond* (2004) 388 F.3d 1189, 7 April.

[33] Friedman, B. and Nissenbaum, H. (1996) Bias in Computer Systems. *ACM Transactions on Information Systems*, 14 (3), pp. 332–333.

[34] Op. cit., p. 334.

of the judiciary or of the legislator, in instances when it is outsourced to private companies, the public scrutiny that courts, judges and parliaments are otherwise subject to can be easily evaded by these entities.[35]

4. A NEW GENERATION IN ALGORITHMIC ENFORCEMENT?

As artificial intelligence and machine learning[36] is gradually spreading across the world, algorithmic copyright enforcement seems to be an obvious field of application. One of the essential tools and technological manifestations of machine learning is text and data mining, which covers the process of gathering and analysing vast amounts of information in order to be able to forecast certain trends and patterns.[37] For autonomous and semi-autonomous systems, the supply of infinite amount of user-generated content[38] provides an invaluable pool of diverse and unfiltered training data, which ensures their effective and accurate functioning. Text and data mining is generally used to extract and classify data from large sets of information. Based on the *KDD-process*[39] *(Knowledge Discovery in Databases)*, it includes the selection, pre-processing, transformation, the actual mining and finally, the evaluation or interpretation of data. Machine learning algorithms, on the other hand, use these clean and targeted datasets and the trends and patterns drawn from them as training data to learn to predict future occurrences as well as to carry out certain tasks in a supervised or unsupervised fashion.[40] As these algorithms generally work better and produce the most accurate results if they have

[35] Citron, D. K. (2008) Technological Due Process. *Washington University Law Review*, 85 (6), p. 1298.

[36] Although these two terms are used interchangeably in the context of this article, machine learning and artificial intelligence are not exactly the same. Artificial intelligence is the broader concept, while machine learning is the manifestation of the study and learning processes that could be applied in artificial intelligence solutions. See: Ryszard S. Michalski, Jaime G. Carbonell and Tom M. Mitchell (eds.). (1983) *Machine Learning: An Artificial Intelligence Approach.* 1st ed. Berlin: Springer-Verlag, p. 3.

[37] Witten, I. H. and Frank, E. (2005) *Data Mining, Practical Machine Learning Tools and Techniques.* 2nd ed. San Francisco: Morgan Kaufmann Publishers, p. 23.

[38] According to some sources, there are 400 hours worth of videos uploaded to *YouTube* every minute and approximately 95 million pictures shared on *Instagram* daily. See at: DMR. (2019) *160 YouTube Statistics and Facts.* [online] Available from: https://expandedramblings.com/index.php/youtube-statistics/ [Accessed 11 January 2019] and Omnicore. (2019) *Instagram by the Numbers: Stats, Demographics & Fun Facts.* [online] Available from: https://www.omnicoreagency.com/instagram-statistics/ [Accessed 11 January 2019].

[39] Fayyad, U., Piatetsky-Shapiro, G. and Smyth, P. (1996) The KDD Process for Extracting Useful Knowledge from Volumes of Data. *Communications of the ACM*, 39 (11), pp. 30–31.

[40] Murphy, K. P. (2012) *Machine Learning: A Probabilistic Perspective.* 1st ed. Cambridge: Massachusetts Institute of Technology, p. 2.

as much and as diverse data as possible at their disposal,[41] the content managed by these platforms seems ideal for the implementation of machine learning technologies, especially in the field of enforcement.

Considering the issues of algorithmic enforcement discussed above, AI's and machine learning's main contribution towards algorithmic copyright enforcement could be their potential to spot and differentiate clearly infringing use from fair use with the help of their more sophisticated technology than those of TPM and the hashing and search algorithms that are currently employed.[42] Even more so considering that, based on *YouTube's* statement, their content recognition tools do not determine copyright exceptions or fair use.[43] However, in order to make these algorithmic systems more balanced in their functioning, the checks and limitations of the exclusive rights embodied in the exceptions and fair use should be part of their design.[44] Through an adequate flagging and training system, in which the initial enhanced human supervision embodied in marking and flagging infringing and non-infringing content could be later substituted by the algorithm's own assessment facilitated by high--quality and streamlined datasets,[45] the algorithm could be taught to identify cases of fair use or instances of copyright exceptions. Even though the different legal systems and jurisdictions regulate copyright exceptions differently,[46] the problem translated into code is rather uniform. For instance, there are several exceptions that necessitate the evaluation of the creator's intent and purpose as well as the context of the utterance: the relevant question is whether the work was used in relation to social commentary, a parody, teaching illustration or for quotation. AI is already getting better at understanding the intent of the writer or speaker and the context of the specific text through natural language processing.[47] Additionally, it is known that *YouTube* actually uses machine learning

[41] See e.g. Halevy, A., Norvig, P. and Pereira, F. (2009) The Unreasonable Effectiveness of Data. *Intelligent Systems, IEEE*, 24 (2); Banko, M. and Brill, E. (2001) Scaling to Very Very Large Corpora for Natural Language Disambiguation. In: Bonnie Lynn Webber (ed.). *Proceedings of the 39th Annual Meeting on Association for Computational Linguistics*, Toulouse, 6–11 July. USA: Association for Computational Linguistics, pp. 26–33.

[42] Elkin-Koren, N. (2017) Fair Use by Design. *UCLA Law Review*, 64 (5), p. 1097.

[43] See: Google. (2019) *Frequently asked questions about fair use.* [online] Available from: https://support.google.com/youtube/answer/6396261?hl=en [Accessed 15 June 2019].

[44] Elkin-Koren, N. (2017) Op. cit., p. 1085.

[45] Lester, T. and Pachamanova, D. (2017) The Dilemma of False Positives: Making Content ID Algorithms more Conducive to Fostering Innovative Fair Use in Music Creation. *UCLA Entertainment Law Review*, 24 (1), p. 69.

[46] See footnote 3.

in order to distinguish and eliminate extremist content from its platform, and, according to the company, the algorithm seems to function quite well.[48, 49] Based on these assertions, it is not irrational to imagine that the different AI and machine learning applications could be combined together to deal with more complex expressions and issues, such as audio--visual content and copyright exceptions.

Nevertheless, even though the issue relating to fair use and exceptions could be potentially addressed by AI, the other problems already mentioned in relation to algorithmic copyright enforcement have the ability to be magnified through the employment of these novel technologies. Transparency of the decision-making process and the arguments behind its reasoning would essentially disappear: some forms of autonomous systems generate their own code, while deep learning applications and neural networks function effectively as "black boxes" due to their immense complexity, the lack of human intervention as well as the inability to reverse engineer the processes and the reasons behind the machine's actions.[50] As learning algorithms do not only implement the goals of the creator of the code but have the capacity to modify the meaning of the goals

[47] There has been recent developments both regarding sentiment analysis and sarcasm detection through deep learning. See: Sarikaya, R., Geoffrey E. and Deoras, A. (2014) Application of Deep Belief Networks for Natural Language Understanding. *IEEE Transactions on Audio, Speech and Language Processing*, 22 (4) and Zhang, M., Zhang, Y. and Fu, G. (2016) Tweet Sarcasm Detection Using Deep Neural Network. In: Eiichiro Sumita, Takenobu Tokunaga and Sadao Kurohashi (eds.). *Proceedings of COLING 2016, the 26th International Conference on Computational Linguistics: Technical Papers*, Osaka, Japan, 11–16 December. Japan: Japanese Association of Natural Language Processing, pp. 2457–2458.

[48] YouTube. (2017) *An update on our commitment to fight violent extremist content online.* [online] Available from: https://youtube.googleblog.com/2017/10/an-update-on-our-commitment-to-fight.html [Accessed 13 January 2019]. Based on *Google's* recent transparency report, almost 90,000 videos were removed between January and March 2019 due to being of violently extremist nature: Google. (2019) *Featured policies.* [online] Available from: https://transparencyreport.google.com/youtube-policy/featured-policies/violent-extremism [Accessed 14 June 2019].

[49] Although *YouTube* claims that automatization is key in removing content before it could go viral, a *Counter Extremism Project's* report on ISIS content on *YouTube* found that 24 % of the examined 1,348 videos remained online for more than two hours, garnering close to 150,000 views, while 91 % of the extremist videos were later reuploaded. These data are however not completely indicative of the effectiveness of the machine learning algorithms, given that *YouTube* employs human review and hashing as well, while automatization is mainly used to locate extremist videos. Counter Extremism Project. (2018) *The eGlyph Web Crawler: ISIS Content on YouTube.* [online] Available from: https://www.counterextremism.com/sites/default/files/eGLYPH_web_crawler_white_paper_July_2018.pdf [Accessed 14 June 2019].

[50] For further information on this issue, see: Knight, W. (2017) The Dark Secret at the Heart of AI. *MIT Technology Review*, 11 April. [online] Available from: https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/ [Accessed 13 January 2019].

themselves,[51] it would be close to impossible to tell if the machine made justified decisions and used the right criteria for assessing fair use. Similarly, accountability could present a new challenge, as the question of how AI could explain its decisions also touches on the issue of legal personality of artificial intelligence and how and to whom liability for damages and wrongdoings could and should be assessed.[52] Finally, the algorithm-driven pre-adjudication process could lead to biased decision making: even though the formal and public court proceedings would still be available for aggrieved parties, the trust put in algorithmic enforcement and automation bias[53] would discourage people from turning to the traditional judiciary when they feel that their rights as users have been violated by the application of automated enforcement measures, due to humans' tendency to ignore or not search for contradictory information, if a decision is generated by a sophisticated computer and believed to be correct.[54] This could affirm that any sort of bias embedded in the process would remain in the system, unchallenged.

5. THE DIRECTIVE ON COPYRIGHT IN THE DIGITAL SINGLE MARKET AND ITS ARTICLE 17

These concerns as well as the whole idea of automated algorithmic copyright enforcement have become even more relevant recently in Europe, in the context of the EU's recent copyright reform.

The most important part of the copyright reform package of 2016, the directive on copyright in the digital single market[55] (DSM Directive) envisions to modernize European copyright rules to meet the challenges

---

[51] Perel, M. and Elkin-Koren, N. (2017) Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement. *Florida Law Review*, 69 (1), p. 189.

[52] For the extensive literature on the issue of legal personality implications of artificial intelligence see: Solum, L. B. (1991) Legal Personhood for Artificial Intelligences. *North Carolina Law Review*, 70 (4); Čerka, P., Grigienė, J. and Sirbikytė, G. (2017) Is it possible to grant legal personality to artificial intelligence systems? *Computer Law & Security Review*, 33 (5); Allgrove, B. (2004) *Legal Personality for Artificial Intellects: Pragmatic Solution or Science Fiction?* [online] Available from: https://ssrn.com/abstract=926015 [Accessed 15 January 2019].

[53] Bamberger, K. A. (2010) Technologies of Compliance: Risk and Regulation in a Digital Age. *Texas Law Review*, 88 (4), p. 676.

[54] Cummings, M. L. (2006) Automation and Accountability in Decision Support System Interface Design. *The Journal of Technology Studies*, 32, p. 25.

[55] 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* (2019/L-130/92) 17 May. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.130.01.0092.01.ENG&toc=OJ:L:2019:130:TOC [Accessed 15 June 2019].

of the digital world as well as to ensure the proper functioning of the internal market by stimulating innovation, creativity and investment in new content.[56] One of the most debated and controversial provisions, Article 17 aims to regulate the status and liability of certain online platforms. The provision's goal is to clarify and uniformize the *Court of Justice of the European Union (CJEU)* case law and declare online content sharing service providers that store and handle a significant amount of copyright protected work to be primary users of the content when they give the public access to these works or other protected subject matter uploaded by their actual end users.[57] This rule would mainly concern social media and content sharing sites, such as *YouTube*, *Facebook* or *Instagram*, while not-for-profit encyclopaedias, cloud services, educational and scientific repositories, open-source software developing platforms and online marketplaces fall outside the scope of the definition of *"online content sharing service provider"*. As primary users of copyright protected works, it will be necessary for these platforms to obtain licenses, pay licensing fees and to bear the burden of primary liability for copyright infringement. If no such license or authorization is granted, then platforms will be liable for the unauthorized acts of communication to the public, including making available to the public, of the copyright-protected works, unless they demonstrate that they made their best efforts to obtain an authorization and to ensure the unavailability of specific works (for which the right holder has provided the necessary information), and in any case, acted expeditiously upon the receipt of a notice to block or remove those specific works.[58] Nevertheless, the measures to comply with this obligations need to be proportionate to the type, audience, size of the service and the type of the works uploaded, as well as the availability of suitable and effective means.[59] If there is an authorization acquired, it will also have to cover the acts of the users, when they are not acting on a commercial basis or their activities do not generate a significant amount of revenues.[60] Regarding the tools to ensure the unavailability of unlicensed material, the earlier versions of the proposal even made an explicit reference to content

[56] Op. cit., Recital (2).
[57] Op. cit., Article 17 paragraph (1).
[58] Op. cit., Article 17 paragraph (4).
[59] Op. cit., Article 17 paragraph (5).
[60] Op. cit., Article 17 paragraph (2).

recognition technologies.[61] The *European Parliament's* approved report that constituted a basis for the informal trilogue negotiations was even more rigorous in this regard, as it did not even provide for an exemption as described above, thus placing the burden of strict liability for copyright infringement on the platforms concerned.[62]

Even though such measures are currently used by some online platforms voluntarily (as we have seen earlier through the example of *YouTube*), these sites could have still qualified as intermediaries in most cases based on the Ecommerce Directive. As such, they could also have benefited from the harmonized safe harbour provisions[63] shielding them from secondary liability.[64] However, if these platforms are to be considered primary users (meaning that they are going to be regarded as performing the copyright--relevant act of communication to the public themselves as well when their end-users upload a piece of content), the utilisation of content recognition technologies would essentially become obligatory for them to avoid liability for infringement. This creates a strong incentive for these platforms to over filter and block any suspicious and possibly infringing content, in the absence of a relevant authorization. In order to achieve the best results, platforms would also be interested in using the state of the art technology for the application of these preventive measures, which points in the direction of the employment of machine learning and artificial intelligence-based technologies.

Nevertheless, in case these technologies are going to be a ubiquitous part of online content creation and consumption, potential solutions and ways

---

[61] Article 13 paragraph (1), European Commission. (2016) *Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market.* (COM(2016) 593 final) 14 September. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0593 [Accessed 15 January 2019].

[62] The so-called "Voss-report" (named after the rapporteur) was supported by a significant majority of MEPs at the plenary session of the European Parliament on 12 September. See: European Parliament. (2018) *Report on the proposal for a directive of the European Parliament and of the Council on copyright in the Digital Single Market.* (COM(2016)0593 – C8-0383(2016) – 2016/0280(COD)). Available from: http://www.europarl.europa.eu/sides/getDoc.dopubRef=%2F%2FEP%2F%2FTEXT%2BREPORT%2BA8-2018-0245%2B0%2BDOC%2BXM%2BV0%2F%2FEN&language=EN [Accessed 7 February 2019].

[63] Currently secondary liability and its requirements are not harmonized on the European level, however, Articles 12–14. of the Ecommerce Directive do provide for a harmonized liability exemption scheme. See: Nordemann, J. B. (2017) Liability of Online Service Providers for Copyrighted Content – Regulatory Action Needed? In-Depth Analysis for the IMCO Committee. *Directorate-General for Internal Policies, Policy Department A (Economic and Scientific Policy), European Parliament*, p. 19.

[64] The proposal even makes an explicit reference to the inapplicability of the Ecommerce Directive's safe harbour rules to online content sharing platforms that perform a communication to the public. European Commission. (2016) Op. cit., Article 13 para. (3).

to mitigate the drawbacks of the currently employed enforcement systems and the future issues of machine learning-based technology outlined in the previous sections need to be considered.

6. TEXT AND DATA MINING AND ITS POTENTIAL IMPACT ON ALGORITHMIC ENFORCEMENT

Although there is a number of potential tools for such harm-reduction (such as the setting of certain standards of disclosure to ensure transparency and accountability[65] or an effective complaint and redress mechanism to tackle the problems of biased pre-adjudication and to provide human oversight), this chapter focuses on another provision within the DSM Directive, the exception on text and data mining and how it could alleviate the issues associated with algorithmic enforcement.

The essence of text and data mining can be captured through its definition, which denotes the extraction of implicit, previously unknown, and potentially useful information from data, for which machine learning provides the technical basis.[66] A study commissioned by the *European Commission* put text and data mining in the wider context of data analysis, which is the automated processing of digital materials, which may include texts, data, sounds, images or other elements, or a combination of these, in order to uncover new knowledge or insights.[67] Text and data mining is essential in realizing the full potential offered by the accumulation of huge amounts of data, and it is utilized in many different fields, such as commerce, finance, or marketing.[68] Additionally, text and data mining is becoming a useful tool in scientific and academic research[69] and based on the potential uses of machine learning outlined in the previous chapter, it could play an important role in the development of more sophisticated enforcement algorithms, which could differentiate between infringing and

---

[65] Lester, T. and Pachamanova, D. (2017) Op. cit., p. 70; Perel, M. and Elkin-Koren, N. (2016) Op. cit., pp. 529–530.

[66] Witten, I. H. and Frank, E. (2005) Op. cit., p. xxiii.

[67] Triaille, J. P., de Meeus d'Argenteuil, J. and de Francquen, A. (2014) *Study on the legal framework of text and data mining (TDM).* [online] Luxembourg: European Union. p. 17. Available from: https://publications.europa.eu/en/publication-detail/-/publication/074ddf78-01e9-4a1d-9895-65290705e2a5/language-en [Accessed 4 February 2019].

[68] Big Data Made Simple. (2014) *Top 14 useful applications of data mining.* [online] 20 August. Available from: https://bigdata-madesimple.com/14-useful-applications-of-data-mining/ [Accessed 4 February 2019].

[69] Filippov, S. (2014) Mapping Text and Data Mining in Academic and Research Communities in Europe. *The Lisbon Council Special Briefing Issue*, (16), p. 11.

non-infringing uses to a better extent. Text and data mining is closely related to machine learning, as, in general, knowledge extracted from examples of a task through data mining can allow for a better performance of the task, while learning process itself generates more knowledge in the form of data.[70]

As it has been stated earlier, one way to make these algorithms effective is to provide them with as much and as diverse information as possible. However, copyright law itself can constitute an obstacle in this process. The process of text and data mining includes the following stages: the business understanding of the problem, the data-specific understanding of the same problem and task, the preparation of data for analysis (the selection of relevant data and the creation of the final dataset), the modelling (the actual mining, which includes the choice of the proper method and its implementation), the evaluation of the prepared models, and finally, the application of the findings.[71] Text and data mining performed for machine learning purposes thus could potentially include copyright-relevant acts of copying, transforming, or communicating to the public while carrying out the steps above. This means that the analysis of data found within material that is protected by copyright or another right (such as the database right[72]) could necessitate the prior authorization of and additional payment to the right holders. This could be especially true in the case of platforms like *YouTube*, where the vast majority of videos are under copyright law's protection.

Large platforms, such as *YouTube* or *Facebook* operate with terms of service that already provide them with authorization to perform text and data mining on copyright-protected contents uploaded to their servers

---

[70] Calders, T. and Custers, B (2013) What Is Data Mining and How Does It Work? In: Bart Custers et al. (eds.). *Discrinimation and Privacy in the Information Society*. 1st ed. Berlin: Springer, p. 29.

[71] Based on the Cross-industry Standard Process for Data Mining (CRISP-DM). Vorhies, W. (2016) *CRISP-DM – a Standard Methodology to Ensure a Good Outcome.* [online] Data Science Central. Available from: https://www.datasciencecentral.com/profiles/blogs/crisp-dm-a-standard-methodology-to-ensure-a-good-outcome [Accessed 4 February 2019].

[72] The database right is enshrined in Directive 96/9/EC of the European parliament and of the Council of 11 March 1996 on the legal protection of databases. It differentiates between databases protected by copyright law as the own intellectual creation of the author by reason of the selection or arrangement of their content and databases that merit protection due to the fact that the maker of the database has made a qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents of the database. This latter is called the *sui generis* database right. Makers of *sui generis* databases have the right to prevent the extraction and/or re-utilization of the whole or of a substantial part of the database.

through the all-encompassing global licenses.[73] Other actors, such as research or non-profit organizations, however, do not have this luxury of access and they lack one of the most important means to develop their own versions of ID algorithms: a minable database of considerable size.[74] This situation gives large tech-corporations a competitive advantage and essentially a monopoly on algorithmic copyright enforcement. We have seen earlier the problems that algorithmic pre-adjudication such as content filtering by private can pose, as these entities often have their own interests and agenda, which might be contrary to the interests of users as well as the freedom of expression.

A potential way to attenuate these consequences could be to remove the obstacle that copyright and other rights constitute. Although certain countries[75] already have provisions on a copyright exception for text and data mining already in force, there has been no such exception on the EU--level yet. However, a provision in the DSM Directive envisions to remedy this defect: among the rules on new, mandatory exceptions, Article 3 makes it compulsory for member states to introduce a copyright exception providing cultural heritage and research institutions the ability to freely use protected works for text and data mining for scientific research purposes. Another, originally optional provision that turned into a mandatory exception through the course of the negotiations (Article 4) additionally prescribes to member states to introduce a general and broad TDM--exception which would apply regardless of the nature of the beneficiary institutions or the purpose of the activity. This exception would provide an opportunity for other entities to more easily develop alternative methods and algorithms, as they would be free from the burden of authorization and remuneration-payment. In both cases, text and data mining could be carried out freely on works and databases to which they have lawful access to.

[73] See: YouTube. (2019) *Terms of Service, Section 8: Rights you license.* [online] Available from: https://www.youtube.com/static?template=terms [Accessed 7 February 2019] and Facebook. (2019) *Terms of Service, Section 3.3: The permissions you give us.* [online] Available from: https://www.facebook.com/terms.php [Accessed 7 February 2019].

[74] Although there are a number of public datasets that could be used freely for machine learning purposes, they usually do not contain information related to the consumption of copyright-protected content or copyright exceptions. For some lists of datasets see: Stanford, S. (2018) *The Best Public Datasets for Machine Learning and Data Science.* [online] Available from: https://medium.com/towards-artificial-intelligence/the-50-best-public-datasets-for-machine-learning-d80e9f030279 [Accessed 15 June 2019] or DeGroat, T. J. (2018) *19 Free Public Data Sets for Your Data Science Project.* [online] Available from: https://www.springboard.com/blog/free-public-data-sets-data-science-project/ [Accessed 15 June 2019].

[75] These countries include the UK, Ireland, Germany and Japan. See: Triaille, J. P., de Meeus d'Argenteuil, J. and de Francquen, A. (2014) Op. cit.

As a further limitation, right holders could expressly reserve the use of their works and protected subject-matter, thus retaining control over excluding TDM.

In any case, the exception on text and data mining could create competition that could cater for a more fair and transparent algorithmic enforcement. The possibility to be able to analyse and train semi--autonomous and autonomous systems is essential for the effective development of copyright enforcement algorithms. By ensuring that more and better data could be freely processed, the environment would be more adequate for the development of fair algorithms. If more non-profit and research organizations could create their own enforcement algorithms, it would not only ensure a more balanced competition through the possibility of choice for emerging platforms, but the aforementioned issues, such as transparency and bias could also be mitigated: if there are more actors, especially not-for-profit organizations, then trade secrecy becomes less of an issue and with a higher level of transparency the possibility of clandestine bias could be prevented as well. Nevertheless, the exception only concerns the actual acts of text and data mining, while the development of new algorithms is outside of its scope. However, the potential to license or sell the enforcement algorithms that have been based on the results of TDM carried out under the exception could either compel larger tech companies to take the development of their own content recognition tools seriously, or could create an alternative market and an incentive to outsource the creation of such algorithms to other entities.

7. CONCLUSION

Copyright law has gone through a number of significant changes in the past years, as it continuously struggled to keep abreast of technological development and to maintain its original goal as well as the level of protection to right holders. As enforcement of copyright has become more difficult with the proliferation of new technologies in the production and dissemination of copyright-protected works, the need for solutions employing technology appeared as well. Although cutting edge, new technology manifested in artificial intelligence and machine learning provide new possibilities for algorithmic copyright enforcement, they also present and potentially aggravate issues such as the lack of transparency and accountability, bias and the limitation of basic rights such

as the freedom of expression and information. These problems require specific attention with the DSM Directive entering into force: as Article 17 regards online content sharing service providers to be carrying out the copyright relevant act of communication to the public, these service providers could be exempt from infringement for copyright liability only if they demonstrate that they have made their best efforts to ensure the unavailability of unauthorized works on their platforms. This situation could easily prompt service providers to use the best and most effective tools.

The issues that could potentially emanate from the employment of AI and machine learning-based algorithmic enforcement mechanisms could be attenuated by two other provisions of the DSM Directive: the mandatory exceptions on text and data mining. Even though the original legislative intent behind the TDM-exception was to secure the development of data science and to close the gap that has appeared between the scientific community of Europe and other jurisdictions with more lenient copyright regimes (such as the United States, where the fair use doctrine offers a more flexible approach towards text and data mining, or China, where enforcement of intellectual property rights is still not in par with the European system), it seems to have a secondary, unintentional positive impact on algorithmic enforcement. It also serves as an example of how the different rules and the different sides of the same issue could be balanced out within the same legal instrument. Similarly, it is a reminder, that regulation and legislation concerning technology or other fields highly influenced by technology merit thorough preliminary analysis. Reactive law-making where only the existing problems are addressed with little to no consideration to the future direction of technological development and its possible implications should be avoided as it has the potential to result in an already obsolete and defunct regulation from the time of its entering into effect. This way, the potential benefits of AI and machine learning to copyright law could prospectively be overshadowed by the disadvantages and various issues brought about by these new technological phenomena.

LIST OF REFERENCES

[1] Akester, P. (2009) *Technological Accommodation of Conflicts between Freedom of Expression and DRM: The First Empirical Assessment.* Rochester, New York: Social Science Research Network.

[2] Allgrove, B. (2004) *Legal Personality for Artificial Intellects: Pragmatic Solution or Science Fiction?* [online] Available from: https://ssrn.com/abstract=926015 [Accessed 15 January 2019].

[3] Bamberger, K. A. (2010) Technologies of Compliance: Risk and Regulation in a Digital Age. *Texas Law Review*, 88 (4).

[4] Banko, M. and Brill, E. (2001) Scaling to Very Very Large Corpora for Natural Language Disambiguation. In: Bonnie Lynn Webber (ed.). *Proceedings of the 39th Annual Meeting on Association for Computational Linguistics*, Toulouse, 6–11 July. USA: Association for Computational Linguistics.

[5] Bartholomew, T. B. (2015) The Death of Fair Use in Cyberspace: YouTube and the Problem with Content ID. *Duke Law & Technology Review*, 13 (1).

[6] Big Data Made Simple. (2014) *Top 14 useful applications of data mining.* [online] 20 August. Available from: https://bigdata-madesimple.com/14-useful-applications-of-data-mining/ [Accessed 4 February 2019].

[7] Calders, T. and Custers, B. (2013) What Is Data Mining and How Does It Work? In: Bart Custers et al (eds.) *Discrimination and Privacy in the Information Society.* 1st ed. Berlin: Springer.

[8] Čerka, P., Grigienė, J. and Sirbikytė, G. (2017) Is it possible to grant legal personality to artificial intelligence systems? *Computer Law & Security Review*, 33 (5).

[9] Channel Awesome. (2016) *Where's The Fair Use – Nostalgia Critic.* [online video] Available from: https://www.youtube.com/watch?v=zVqFAMOtwaI&t=53s [Accessed 10 January 2019].

[10] Citron, D. K. (2008) Technological Due Process. *Washington University Law Review*, 85 (6).

[11] Counter Extremism Project. (2018) *The eGlyph Web Crawler: ISIS Content on YouTube.* [online] Available from: https://www.counterextremism.com/sites/default/files/eGLYPH_web_crawler_white_paper_July_2018.pdf [Accessed 14 June 2019].

[12] Craig, C. J. (2017) Technological Neutrality: Recalibrating Copyright in the Information Age. *Theoretical Issues in Law*, 17 (2).

[13] Cummings, M. L. (2006) Automation and Accountability in Decision Support System Interface Design. *The Journal of Technology Studies*, 32.

[14] DeGroat, T. J. (2018) *19 Free Public Data Sets for Your Data Science Project.* [online] Available from: https://www.springboard.com/blog/free-public-data-sets-data-science-project/ [Accessed 15 June 2019].

[15] 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* (2001/L-167/10) 22 June. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001L0029&from=EN [Accessed 10 January 2019].

[16] 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* (2019/L-130/92) 17 May. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.130.01.0092.01.ENG&toc=OJ:L:2019:130:TOC [Accessed 19 May 2019]

[17] DMR. (2019) *160 YouTube Statistics and Facts.* [online] Available from: https://expandedramblings.com/index.php/youtube-statistics/ [Accessed 11 January 2019].

[18] Elkin-Koren, N. (2017) Fair Use by Design. *UCLA Law Review*, 64 (5).

[19] Facebook. (2019) *Rights Manager.* [online] Available from: https://rightsmanager.fb.com/ [Accessed 10 January 2019].

[20] Facebook. (2019) *Terms of Service, Section 3.3: The permissions you give us.* [online] Available from: https://www.facebook.com/terms.php [Accessed 7 February 2019].

[21] Fayyad, U., Piatetsky-Shapiro, G. and Smyth, P. (1996) The KDD Process for Extracting Useful Knowledge from Volumes of Data. *Communications of the ACM*, 39 (11).

[22] Filippov, S. (2014) Mapping Text and Data Mining in Academic and Research Communities in Europe. *The Lisbon Council Special Briefing Issue*, (16).

[23] Fisher, W. W. (1988) Reconstructing the Fair Use Doctrine. *Harvard Law Review*, 101 (8).

[24] Fisher, W. W. (2001) Theories of Intellectual Property. In: Stephen Munzer (ed.). *New Essays in the Legal and Political Theory of Property.* 1st ed. Cambridge: Cambridge University Press.

[25] Friedman, B. and Nissenbaum, H. (1996) Bias in Computer Systems. *ACM Transactions on Information Systems*, 14 (3).

[26] Geller, P. E. (2008) Beyond the Copyright Crisis: Principles for Change. *Journal of the Copyright Society of the USA*, 55.

[27] Google. (2019) *Featured policies.* [online] Available from: https://transparencyreport.google.com/youtube-policy/featured-policies/violent-extremism [Accessed 14 June 2019].

[28] Google. (2019) *Frequently asked questions about fair use.* [online] Available from: https://support.google.com/youtube/answer/6396261?hl=en [Accessed 15 June 2019].

[29] Greenberg, B. A. (2016) Rethinking Technology Neutrality. *Minnesota Law Review*, 100 (4).

[30] Halevy, A., Norvig, P. and Pereira, F. (2009) The Unreasonable Effectiveness of Data. *Intelligent Systems, IEEE*, 24 (2).

[31] I Hate Everything. (2015) *Cool Cat Saves The Kids – The Search For The Worst.* [online video] Available from: https://www.youtube.com/watch?v=HoTZZYm2HZI&t=42s [Accessed 10 January 2019].

[32] Joyce, C. (ed.). (2013) *Copyright Law.* 9th ed. New Providence: LexisNexis.

[33] Kerr, I. (2010) Digital Locks and the Automation Virtue. In Geist, Michael (ed.). *From „Radical Extremism" to „Balanced Copyright": Canadian Copyright and the Digital Agenda.* 1st ed. Toronto: Irwin Law.

[34] Knight, W. (2017) The Dark Secret at the Heart of AI. *MIT Technology Review*, 11 April. [online] Available from: https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/ [Accessed 13 January 2019].

[35] Latman, A. and Patry, W. F. (1986) *Latman's the Copyright Law.* 6th ed. Washington, D.C.: Bureau of National Affairs.

[36] Litman, J. (2002) Revising Copyright Law for the Information Age. In: Adam Thierer and Wayne Crews (eds.) *Copy Fights: The Future of Intellectual Property in the Information Age.* 1st ed. Washington, D.C: Cato Institute.

[37] Leval, P. N. (1990) Toward a Fair Use Standard. *Harvard Law Review*, 103.

[38] Lessig, L. (2006) *Code v. 2.0*, 2006, New York: Basic Books. Available from: http://codev2.cc/download+remix/Lessig-Codev2.pdf [Accessed 10 January 2019].

[39] Lester, T. and Pachamanova, D. (2017) The Dilemma of False Positives: Making Content ID Algorithms more Conducive to Fostering Innovative Fair Use in Music Creation. *UCLA Entertainment Law Review,* 24 (1).

[40] Ryszard S. Michalski, Jaime G. Carbonell and Tom M. Mitchell (eds.). (1983) *Machine Learning: An Artificial Intelligence Approach.* 1st ed. Berlin: Springer-Verlag.

[41] Mills, M. L. (1989) New Technology and the Limitations of Copyright Law: An Argument for Finding Alternatives to Copyright Legislation in an Era of Rapid Technological Change. *Chicago-Kent Law Review*, 65 (1).

[42] Murphy, K. P. (2012) *Machine Learning: A Probabilistic Perspective.* 1st ed. Cambridge: Massachusetts Institute of Technology.

[43] Myška, M. (2009) The True Story of DRM. *Masaryk University Journal of Law and Technology*, 3 (2).

[44] Nordemann, J. B. (2017) Liability of Online Service Providers for Copyrighted Content – Regulatory Action Needed? In-Depth Analysis for the IMCO Committee. *Directorate--General for Internal Policies, Policy Department A (Economic and Scientific Policy), European Parliament.*

[45] *Newton v. Diamond* (2004) 388 F.3d 1189, 7 April.

[46] Omnicore. (2019) *Instagram by the Numbers: Stats, Demographics & Fun Facts.* [online] Available from: https://www.omnicoreagency.com/instagram-statistics/ [Accessed 11 January 2019].

[47] Perel, M. and Elkin-Koren, N. (2016) Accountability in Algorithmic Copyright Enforcement. *Stanford Technology Law Review*, 19 (3).

[48] Perel, M and Elkin-Koren, N. (2017) Black Box Tinkering: Beyond Disclosure in Algorihtmic Enforcement. *Florida Law Review*, 69 (1).

[49] PewDiePie. (2017) *Life is cringe – life is strange – S2E01.* [online video] Available from: https://www.youtube.com/watch?v=PX4zk0G4IjM [Accessed 10 January 2019].

[50] European Commission. (2016) *Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market.* (COM(2016) 593 final) 14 September. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0593 [Accessed 15 January 2019].

[51] European Parliament. (2018) *Report on the proposal for a directive of the European Parliament and of the Council on copyright in the Digital Single Market.* (COM(2016)0593 – C8-0383 (2016) – 2016/0280(COD)). Available from: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=%2F%2FEP%2F%2FTEXT%2BREPORT%2BA8-2018-0245%2B0%2BDO%2BXML%2BV0%2F%2FEN&language=EN [Accessed 7 February 2019].

[52] Richard, K. (2018) Fair Use in the Information Age. *Richmond Journal of Law & Technology*, 25 (1).

[53] *Ringgold v. Black Entertainment Television, Inc.* (1997) 126 F.3d 70, 16 September.

[54] *Sandoval v. New Line Cinema Corp.* (1998) 147 F.3d 215, 24 June.

[55] Sarikaya, R., Geoffrey E. and Deoras, A. (2014) Application of Deep Belief Networks for Natural Language Understanding. *IEEE Transactions on Audio, Speech and Language Processing*, 22 (4).

[56] Solum, L. B. (1991) Legal Personhood for Artificial Intelligences. *North Carolina Law Review*, 70 (4).

[57] Stamatoudi, I. and Torremans, P. (2014) *EU Copyright Law, a Commentary.* 1st ed. Cheltenham: Edward Elgar Publishing Limited.

[58] Stanford, S. (2018) *The Best Public Datasets for Machine Learning and Data Science.* [online] Available from: https://medium.com/towards-artificial-intelligence/the-50-best-public-datasets-for-machine-learning-d80e9f030279 [Accessed 15 June 2019].

[59] Thatcher, S. G. (2006) Fair Use in Theory and Practice: Reflections on its History and the Google Case. *Journal of Scholarly Publishing*, 37 (3).

[60] Triaille, J.P., de Meeus d'Argenteuil, J. and de Francquen, A. (2014) *Study on the legal framework of text and data mining (TDM).* 1st ed. Luxembourg: European Union. Available from: https://publications.europa.eu/en/publication-detail/-/publication/074ddf78-01e9-4a1d-9895-65290705e2a5/language-en [Accessed 4 February 2019].

[61] United States Copyright Office. (2019) *More information on fair use.* [online] Washington, D. C.: USCO. Available from: https://www.copyright.gov/fair-use/more-info.html [Accessed 23 May 2019].

[62] Vorhies, W. (2016) *CRISP-DM – a Standard Methodology to Ensure a Good Outcome.* [online] Data Science Central. Available from: https://www.datasciencecentral.com/profiles/blogs/crisp-dm-a-standard-methodology-to-ensure-a-good-outcome [Accessed 4 February 2019].

[63] Witten, I. H. and Frank, E. (2005) *Data Mining, Practical Machine Learning Tools and Techniques.* 2nd ed. San Francisco: Morgan Kaufmann Publishers.

[64] YouTube. (2017) *An update on our commitment to fight violent extremist content online.* [online] Available from: https://youtube.googleblog.com/2017/10/an-update-on-our-commitment-to-fight.html [Accessed 13 January 2019].

[65] YouTube. (2019) *Content Verification Program.* [online] Available from: https://support.google.com/youtube/answer/6005923 [Accessed 14 June 2019].

[66] YouTube. (2019) *Copyright Management Tools.* [online] Available from: https://support.google.com/youtube/answer/9245819?hl=en [Accessed 14 June 2019].

[67] YouTube. (2019) *Copyright Management Tools – Content ID.* [online] Available from: https://support.google.com/youtube/answer/9245819 [Accessed 10 January 2019].

[68] YouTube. (2019) *Copyright Match Tool.* [online] Available from: https://support.google.com/youtube/answer/7648743 [Accessed 14 June 2019].

[69] YouTube. (2019) *How Content ID works.* [online] Available from: https://support.google.com/youtube/answer/2797370?hl=en&ref_topic=2778544 [Accessed 10 January 2019].

[70] YouTube. (2019) *Terms of Service, Section 8: Rights you license.* [online] Available from: https://www.youtube.com/static?template=terms [Accessed 7 February 2019].

[71] YouTube. (2019) *YouTube in Numbers.* [online] Available from: https://www.youtube.com/yt/about/press/ [Accessed 14 June 2019].

[72] Zhang, M., Zhang, Y. and Fu, G. (2016) Tweet Sarcasm Detection Using Deep Neural Network. In: Eiichiro Sumita, Takenobu Tokunaga and Sadao Kurohashi (eds.). *Proceedings of COLING 2016, the 26th International Conference on Computational Linguistics: Technical Papers*, Osaka, Japan, 11–16 December. Japan: Japanese Association of Natural Language Processing.

<<< ARTICLES

COMMENTARIES >>>

DOI 10.5817/MUJLT2019-2-10

GRADING AG SZPUNAR'S OPINION IN CASE C-18/18 – A CAUTION AGAINST WORLDWIDE CONTENT BLOCKING AS DEFAULT[*]

by

DAN SVANTESSON[**]

On 4th of June 2019, Advocate General Szpunar delivered his Opinion in Case C-18/18 between Eva Glawischnig-Piesczek (an Austrian politician) and Facebook Ireland Limited. The politician had sought to have certain current and future content – argued to be defamatory – blocked by Facebook with worldwide effect. This is arguably the most important Internet speech-related case currently before the Court of Justice of the European Union (CJEU) and will doubtlessly influence court reasoning far beyond Europe.

This Comment analyses AG Szpunar's interesting, but problematic, Opinion with particular emphasis on his reasoning in relation to the question of scope of jurisdiction; that is, what is the appropriate geographical scope of orders in these circumstances, rendered by a court that has personal jurisdiction and subject matter jurisdiction.

KEY WORDS

Content Blocking, EU Law, Internet, Internet Intermediaries, Internet Jurisdiction, Scope of Jurisdiction

1. INTRODUCTION

The dispute in Case C-18/18 arose when *Eva Glawischnig-Piesczek* (an Austrian politician) sought to have certain content – argued to be defamatory – removed by *Facebook Ireland Limited* with worldwide effect.

[*] Professor *Svantesson* wrote an Expert Opinion on behalf of *Facebook Ireland Limited* in Case C-18/18. This contribution was supported by a grant from *Facebook Ireland Limited* but the views and opinions expressed are only those of the author.

[**] dasvante@bond.edu.au, Professor, Faculty of Law, Bond University, Australia.

In fact, she also sought to have possible future postings containing statements with identical wording, and/or having equivalent meaning, removed on *Facebook* with worldwide effect, regardless of whether such postings were made by the person responsible for the initial posting or any other current or future *Facebook* user.

Case C-18/18 is arguably the most important Internet speech-related case currently before the *Court of Justice of the European Union (CJEU)* and will doubtlessly influence court reasoning far beyond Europe. On 4th of June 2019, Advocate General *Szpunar* delivered his Opinion in the matter.

Scarred by my profession, I tend to approach documents such as AG *Szpunar's* Opinion from the perspective of what grade they deserve. Great papers are easy to mark. The same goes for particularly poor papers. The hardest are those that are partly good, or very good, and partly poor. In my view, AG *Szpunar's* Opinion in Case C-18/18 falls into this latter category. It is elegant in parts, and messy in others. Clear logical reasoning is bundled with what I see as inconsistencies, and sensible conclusions appear next to what, quite frankly, are surprisingly fanciful assertions.

Put in the simplest of terms, AG *Szpunar* addressed two themes of issues:

1. To what extent does Article 15(1) of the Directive on electronic commerce[1] limit blocking and monitoring imposed under the national law of a Member State; and
2. What limits apply as to the scope of jurisdiction of such orders? That is, what is the appropriate geographical scope of orders in these circumstances, rendered by a court that has personal jurisdiction and subject matter jurisdiction?[2]

In this brief note, I focus on the latter topic; that of scope of jurisdiction. However, I note in passing that, on the first matter, AG *Szpunar* took the view that the Directive on electronic commerce

[1] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. *Official Journal L 178, 17/07/2000 P. 0001–0016*. Available from: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32000L0031&from=EN [Accessed 2 September 2019].

[2] Svantesson, D. (2016) Jurisdiction in 3D – "scope of (remedial) jurisdiction" as a third dimension of jurisdiction. *Journal of Private International Law*, 12 (1), pp. 60–76.

> *"does not preclude a host provider which operates a social network platform from being ordered […] to seek and identify, among all the information disseminated by users of that platform, the information identical to the information that has been characterised as illegal by a court".*[3]

Furthermore,

> *"a host provider may [also] be ordered to seek and identify the information equivalent to that characterised as illegal only among the information disseminated by the user that disseminated that illegal information."*[4]

While he added that

> *"[a] court adjudicating on the removal of such equivalent information must ensure that the effects of its injunction are clear, precise and foreseeable",*[5]

and that such a court also

> *"must weigh up the fundamental rights involved and take account of the principle of proportionality",*[6]

if *Szpunar's* view is adopted by the CJEU, we have to expect far reaching consequences on free expression and access to information for both Internet users and for Internet intermediaries. This is especially so if such orders are worldwide in scope; after all, in that case we would have an Austrian court deciding what foreigners may post on a foreign social media platform even where the content is perfectly legal both where the platform user and platform are located. Such an intrusive approach may undoubtedly be justified in certain extreme situations, but not as a general default position; and as framed in this Opinion, it seems to be entirely at odds with AG *Spuznar's* concern regarding a "race to the bottom" approach on free expression he articulated just a few months earlier.[7]

---

[3] Opinion of Advocate General Szpunar in Glawischnig-Piesczek (C-18/18, EU:C:2019:458), para. 109.

[4] Ibid.

[5] Ibid.

[6] Ibid.

[7] Opinion of Advocate General Szpunar in Google (Territorial scope of de-referencing) (C-507/17, EU:C:2019:15).

2. THE TASK AS AG SZPUNAR SAW IT

On the topic in focus here, AG *Szpunar* saw his task as clearing up the question of

> *"whether a host provider may be ordered to remove content which has been characterised as illegal under the national law of a Member State not only in that Member State but also worldwide."*[8]

He concluded that:

> *"As regards the territorial scope of a removal obligation imposed on a host provider in the context of an injunction, it should be considered that that obligation is not regulated either by Article 15 (1) of Directive 2000/31 or by any other provision of that directive and that that provision therefore does not preclude that host provider from being ordered to remove worldwide information disseminated via a social network platform. Nor is that territorial scope regulated by EU law, since in the present case the applicant's action is not based on EU law."*[9]

In the first part of this paragraph, AG *Szpunar* is merely stating the obvious; the Directive on electronic commerce clearly does not regulate the scope of jurisdiction issue. In contrast, his claim that the territorial scope is not regulated by EU law since the applicant's action is not based on EU law is as surprising as it is concerning.

3. THE RELATIONSHIP WITH CASE C-507/17 (GOOGLE FRANCE)

In setting the scene for his task, AG *Szpunar* correctly observed that

1. *"the EU legislature has not harmonised the material rules on harm to private life and personality rights, including defamation."*[10]; and
2. *"the EU legislature [has not] harmonised the conflict-of-law rules in that field."*[11]

Appropriately, this led him to conclude that

---

[8] Opinion of Advocate General Szpunar in Glawischnig-Piesczek (C-18/18, EU:C:2019:458), para. 76.

[9] Op. cit., para. 109.

[10] Op. cit., para. 78.

[11] Ibid.

> *"when hearing actions in defamation, each court in the European Union applies the law designated as applicable under the national conflict rules."*[12]

As is well-known, however, it is not only customary, but logically necessary, to address the matter of jurisdiction before one enters the territory of identifying the applicable law. As also is well-known, the EU legislature has, indeed, harmonised the rules of jurisdiction when it comes to harm to private life and personality rights, including defamation.[13]

What then can have motivated this highly skilled private international law jurist to rush to the question of choice of law first? The answer is perhaps found in the paragraph that follows immediately after this oddity. There, AG *Szpunar* relies on the applicable law being national law to distinguish the case at hand from Case C-507/17 (*Google France*) in relation to which he reached a series of important conclusions[14] that potentially could have extended in a similar manner to this case:

> *"That case [Case C-507/17] concerns Directive 95/46/EC[15], […] which harmonises, at Union level, certain material rules on data protection. It was, notably, the fact that the applicable material rules are harmonised that led me to conclude that a service provider had to be required to delete the results displayed following a search carried out not only from a single Member State but from a place within the European Union."*[16]

In this context, AG *Szpunar* went on to stress that in his Opinion in Case C-507/17, he

> *"did not exclude the possibility that there might be situations in which the interest of the Union requires the application of the provisions of that directive beyond the territory of the European Union."*[17]

---

[12] Ibid.

[13] Regulation of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ 2012 L 351, p. 1).

[14] Opinion of Advocate General Szpunar in Google (Territorial scope of de-referencing) (C-507/17, EU:C:2019:15).

[15] Directive of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).

[16] Opinion of Advocate General Szpunar in Glawischnig-Piesczek (C-18/18, EU:C:2019:458), para. 79.

[17] Ibid.

Even in the light of this latter point – with which I am entirely comfortable[18] – it is remarkable that AG *Szpunar* here does not further engage with the implications of the distinction between Case C-507/17 and the case at hand.

As it was the fact the relevant substantive law *has been harmonised* that persuaded AG *Szpunar* to facilitate EU-wide de-indexing in Case C-507/17, and given that the relevant substantive law *has not been harmonised* in Case C-18/18, the logical conclusion must presumably be that in the case at hand, a blocking order may not apply EU-wide. It can hardly then be reasonable to allow it to be worldwide, not least as worldwide orders per definition also are EU-wide. In other words, under AG *Szpunar's* reasoning, where the relevant substantive law has been harmonised, a court has jurisdiction to issue orders that may apply EU-wide, and where no such harmonisation exists, the court has jurisdiction to issue orders that may still extend EU-wide, and indeed worldwide! Such a conclusion certainly puts us at risk of a "race to the bottom" and seems to undermine important safeguards provided for in EU law.

4. THE RELEVANCE OF THE BRUSSELS REGULATION

Pointing to the CJEU's decision in Case C-194/16 (*Bolagsupplysningen*), AG *Szpunar* correctly noted that

> *"the jurisdiction rules in Regulation No 1215/2012 [the Brussels Regulation] also apply to disputes concerning the removal of defamatory content placed online."*[19]

In this context, AG *Szpunar* added the dubious observation that

> *"only the interested parties entertain doubts as to the territorial extent of jurisdiction".*[20]

Making matters worse, AG *Szpunar* also stated that

---

[18] See e.g.: Svantesson, D. (2015) Limitless borderless forgetfulness? Limiting the geographical reach of the 'right to be forgotten'. *Oslo Law Review*, 2 (2), pp. 116–138.

[19] Opinion of Advocate General Szpunar in Glawischnig-Piesczek (C-18/18, EU:C:2019:458), para. 83.

[20] Ibid.

> *"according to the interpretations put on that judgment [eDate] in the literature, the forum of the centre of interests may adjudicate throughout the world on the damage caused".*[21]

The "literature" by which he supported this statement with extraordinarily far-reaching consequences is, however, limited to two works. While I hold the views of the relevant authors in the highest regard, marks must necessarily be detracted for such an oversimplification of what commentators have said on this matter.

AG *Szpunar's* statements seem to suggest that CJEU case law has already conclusively settled the matter of scope of jurisdiction in disputes concerning the removal of defamatory content placed online. Such a charitable conclusion is hardly justified.

Elsewhere, I have analysed in detail what Case C-194/16 (and the key cases that preceded it)[22] means for the question of scope of jurisdiction.[23] To focus on one single matter, the entire premise of the CJEU's conclusion in Case C-194/16 is based on the notion that

> *"in the light of the ubiquitous nature of the information and content placed online on a website and the fact that the scope of their distribution is, in principle, universal […], an application for the rectification of the former and the removal of the latter is a single and indivisible application".*[24]

AG *Szpunar* directly, and correctly, contradicts this, both in this Opinion, and in his Opinion in Case C-507/17, by pointing to the advantages of removing content with the help of geo-location technologies – recognising the relevance of geo-location technologies necessarily contradicts the notion that an application for the rectification or removal of content is a single and indivisible application. This issue ought to have been explored in detail, not sidestepped.

---

[21] Opinion of Advocate General Szpunar in Glawischnig-Piesczek (C-18/18, EU:C:2019:458), footnote 42.

[22] Judgment of 7 March 1995, Shevill, C-68/93, EU:C:1995:61 and Judgments of 25 October 2011, eDate Advertising GmbH, C-509/09 and Martinez C-161/10, EU:C:2011:685.

[23] Svantesson, D. (2018) European Union Claims of Jurisdiction over the Internet – an Analysis of Three Recent Key Developments. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 9, pp. 120–122.

[24] Judgment of 17 October 2017, Bolagsupplysningen OÜ, Case C-194/16, EU:C:2017:766, para. 48.

Despite the profoundly confusing state of the relevant law, AG *Szpunar* contented himself with a brief discussion of Cases C-509/09 and C-161/10 and concluded that

> *"the court of a Member State may, as a general rule, adjudicate on the removal of content outside the territory of that Member State, as the territorial extent of its jurisdiction is universal."*[25]

Elaborating on this in a footnote, he claims that

> *"[i]t is therefore a matter here of jurisdiction known as 'global' or 'general'".*[26]

The whole idea that, as a general rule, the courts of a Member State enjoy universal jurisdiction is simply incomprehensible and stands in stark contrast to public international law, and to traditional approaches to private international law. It is also a striking contrast to the sentiment expressed by the *European Commission* in its *amicus brief* filed in the controversial *Microsoft Warrant* case – heard in the *Supreme Court of the United States* on 27 February 2018:

> *"[a]ny domestic law that creates cross-border obligations – whether enacted by the United States, the European Union, or another state – should be applied and interpreted in a manner that is mindful of the restrictions of international law and considerations of international comity. The European Union's foundational treaties and case law enshrine the principles of "mutual regard to the spheres of jurisdiction" of sovereign states and of the need to interpret and apply EU legislation in a manner that is consistent with international law."*[27]

---

[25] Opinion of Advocate General Szpunar in Glawischnig-Piesczek (C-18/18, EU:C:2019:458), para. 86.

[26] Opinion of Advocate General Szpunar in Glawischnig-Piesczek (C-18/18, EU:C:2019:458), footnote 43.

[27] European Union as Amicus Curiae in Support of Neither Party, p. 7. [online] Available from: https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf [Accessed 2 September 2019].

5. THE TERRITORIAL SCOPE OF A REMOVAL OBLIGATION

It is not entirely clear what AG *Szpunar* had in mind in his discussion (paras. 88–103) of what he described as the *"territorial scope of a removal obligation"*, as opposed to the preceding section (paras. 82–87) he described as addressing the *"territorial scope of the jurisdiction"*. Part of the discussion clearly relates to the question of scope of jurisdiction, or scope of remedial jurisdiction as *Justice Groberman* called it in a decision[28] of the *Court of Appeal for British Columbia*. That question is, however, unquestionably a part of the noted case law that has developed in relation to the Brussels Regulation.

Further, AG *Szpunar* suggested that

> *"both the question of the extraterritorial effects of an injunction imposing a removal obligation and the question of the territorial scope of such an obligation should be analysed not by reference to EU law but, in particular, by reference to public and private international law, which is not harmonised at EU level."*[29]

I fail to see the difference between *"the question of the extraterritorial effects of an injunction"*, and *"the question of the territorial scope of such an obligation"*. And at least for me, AG *Szpunar* added to the confusion when he proceeded to state that:

> *"In fact, there is nothing to indicate that the situation forming the subject matter of the main proceedings may come within the scope of EU law and therefore of the rules of international law that influence the interpretation of EU law."*[30]

Yet, as noted by AG *Szpunar* himself, the situation forming the subject matter of the main proceedings does, indeed, come within the scope of EU law in the form of the Brussels Regulation. Logically then, the rules of international law that influence the interpretation of EU law cannot be disregarded in that setting.

---

[28] Equustek Solutions Inc v Google Inc [2015] BCCA 265, para. 69.

[29] Opinion of Advocate General Szpunar in Glawischnig-Piesczek (C-18/18, EU:C:2019:458), para. 92.

[30] Ibid.

Whatever AG *Szpunar* meant with this section, it led him to conclude that:

1. the Directive on electronic commerce does not preclude a court from ordering a host provider to remove information disseminated via a social network platform worldwide; and
2. the territorial scope is not regulated by EU law since in the present case the applicant's action is not based on EU law.[31]

While the first of these conclusions may be uncontroversial, the latter certainly is not. AG *Szpunar* is here apparently conflating the question of applicable law with the question of jurisdiction. The territorial scope is clearly regulated by EU law in the form of the Brussels Regulation.[32]

After all this, AG *Szpunar* – in the end – reached a largely sensible conclusion:

> *"To conclude, it follows from the foregoing considerations that the court of a Member State may, in theory, adjudicate on the removal worldwide of information disseminated via the internet. However, owing to the differences between, on the one hand, national laws and, on the other, the protection of the private life and personality rights provided for in those laws, and in order to respect the widely recognised fundamental rights, such a court must, rather, adopt an approach of self-limitation. Therefore, in the interest of international comity, to which the Portuguese Government refers, that court should, as far as possible, limit the extraterritorial effects of its junctions concerning harm to private life and personality rights. The implementation of a removal obligation should not go beyond what is necessary to achieve the protection of the injured person. Thus, instead of removing the content, that court might, in an appropriate case, order that access to that information be disabled with the help of geo-blocking."*[33] (internal references excluded)

---

[31] Op. cit., para. 93.

[32] Perhaps AG *Szpunar* mean to, in this section, solely address the matter of applicable law in relation to decisions to remove content beyond Austria, but if so, it is surprising that he discusses which court would be better placed to rule on such removal [see Opinion of Advocate General Szpunar in Glawischnig-Piesczek (C-18/18, EU:C:2019:458) para. 97].

[33] Opinion of Advocate General Szpunar in Glawischnig-Piesczek (C-18/18, EU:C:2019:458), para. 100.

The warnings raised against worldwide orders in this paragraph, and indeed throughout the Opinion, are crucially important and AG *Szpunar* deserves full credit for bringing these concerns forward. Yet, a fundamental concern here is that AG *Szpunar* appears to define the scope of jurisdiction under the Brussels Regulation independently of international law considerations such as comity. He then introduces the comity consideration at a later stage. However, there is no doubt that EU law is bound by international law, and therefore, the Brussels Regulation cannot be read independent of public international law constraints such as the doctrine of comity. This holds true whether the applicable law is EU law, is harmonised by EU law, or is purely the national law of a Member State.

6. GEO-LOCATION TECHNOLOGIES

In relation to AG *Szpunar's* sensible suggestion that courts may order that access to content be disabled with the help of geo-location technologies in an appropriate cases, it is worth noting that, at the hearing the applicant argued that such measure would be ineffective due to the possibility of circumvention.

This is an argument that is made frequently. However, it is flawed,[34] and AG *Szpunar's* response that

> *"[t]hose considerations cannot be called into question by the applicant's argument that the geo-blocking of the illegal information could be easily circumvented by a proxy server or by other means"*[35]

is encouraging. It is also fully in line with his Opinion in Case C-507/17 that also endorsed the use of geo-location technologies.

7. CONCLUDING REMARKS

In the light of the above, if I had been assessing AG *Szpunar's* Opinion the way I assess student assignments, I would have hoped this was just a first draft that he would have the opportunity to rework and amend. The reality is of course quite different. This will forever stand as his Opinion in Case C-18/18. However, as the CJEU's judgment is still to come, the last word has not been uttered in relation to this case. A lot is at stake and I

[34] See further: Svantesson, D. (2017) *Solving the Internet Jurisdiction Puzzle*. Oxford: Oxford University Press, pp. 205–206.

[35] Opinion of Advocate General Szpunar in Glawischnig-Piesczek (C-18/18, EU:C:2019:458), para. 101.

hope the CJEU clarifies, once and for all, that a court with jurisdiction founded in EU law does not enjoy unfettered global jurisdiction just because it applies national law.

LIST OF REFERENCES

[1] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

[2] Directive of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281).

[3] Equustek Solutions Inc v Google Inc [2015] BCCA 265.

[4] European Union as Amicus Curiae in Support of Neither Party. [online] Available from: https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf [Accessed 2 September 2019].

[5] Judgment of 17 October 2017, Bolagsupplysningen OÜ, C-194/16, EU:C:2017:766.

[6] Judgment of 7 March 1995, Shevill, C-68/93, EU:C:1995:61.

[7] Judgments of 25 October 2011, eDate Advertising GmbH, C-509/09 and Martinez C-161/10, EU:C:2011:685.

[8] Opinion of Advocate General Szpunar in Glawischnig-Piesczek (C-18/18, EU:C:2019:458).

[9] Opinion of Advocate General Szpunar in Google (Territorial scope of de-referencing) (C-507/17, EU:C:2019:15).

[10] Regulation of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ 2012 L 351, p. 1).

[11] Svantesson, D. (2015) Limitless borderless forgetfulness? Limiting the geographical reach of the 'right to be forgotten'. *Oslo Law Review*, 2 (2).

[12] Svantesson, D. (2016) Jurisdiction in 3D – "scope of (remedial) jurisdiction" as a third dimension of jurisdiction. *Journal of Private International Law*, 12 (1).

[13] Svantesson, D. (2017) *Solving the Internet Jurisdiction Puzzle*. Oxford: Oxford University Press.

[14] Svantesson, D. (2018) European Union Claims of Jurisdiction over the Internet – an Analysis of Three Recent Key Developments. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 9.

DOI 10.5817/MUJLT2019-2-11

PROCEDURAL AND INSTITUTIONAL BACKING OF TRANSPARENCY IN ALGORITHMIC PROCESSING OF RIGHTS*

by

RADIM POLČÁK**

Efficient enforcement of legal substance requires proper procedures and capable institutions. In that respect, law is now being challenged by the emergence of automated systems that autonomously decide about matters concerning rights. The neuralgic point in enforcement of legal compliance of such systems, namely with regards to possible discrimination, is transparency. Currently, there exists, at least in the EU, particular individual right to know the logic of respective algorithms. The comment tries to narrow down the issue of actual enforceability of that right by investigating its basic procedural and institutional aspects.

KEY WORDS

Algorithmic State, Automated Decisions, Logic of Algorithms, Transparency of Algorithms

1. CONGRUENCE BETWEEN OFFICIAL ACTION AND DECLARED RULE

The last, and by far not the least important, of *Fuller's* principles of legality, is about congruence of substance and administration of rights, or of *"official action and declared rule"*[1]. All substantively grounded rights, however compliant with the earlier *Fuller's* principles, have no value if there are

* This comment is based on a research that was funded under the project C4E No. CZ.02.1.01/0.0/0.0/16_019/0000822. The author wishes to especially thank *Tomáš Sobek* who kindly provided inspiration for this comment thanks to his throughout knowledge of the work of late *Sir Terence Prachett*.

** radim.polcak@law.muni.cz, Head of the Institute of Law and Technology at the Faculty of Law, Masaryk University, The Czech Republic.

1 See Fuller, L. (1969) The Morality of Law. *Yale University Press*, p. 81.

no means available for their actual implementation. This principle of congruence of substance and procedure is being often materialised, amongst other places, at the *European Court of Human Rights* e.g. in cases when it takes too long for the courts in the member states to deliver justice.[2]

Besides cases of inability to deliver justice in reasonable time, there is a number of other possible cases of lack of congruence between substance and administration of rights. Despite these cases originate in hugely different domains, they all arise from disproportions between the law in books and the law in action which results in merely theoretical existence of respective rights. In all these cases, illegality (in *Fuller's* terms) arises from rights being just virtual but not actual.[3]

Following are two examples that illustrate the aforementioned virtuality of rights. These examples are in their natures very close to the below research questions, because they both relate to the role of state in getting complex information technologies under control.

The first example concerns data retention obligations that represent for more than a decade a mostly controversial issue across European jurisdictions.[4] Telecommunication operators have in some EU member states a duty to retain traffic data that are then available to law enforcement and security institutions. These obligations came under constitutional scrutiny across the EU and elsewhere namely because of concerns over privacy and personal data protection.

Regardless of whether traffic data are acquired by law enforcement upon data retention obligations or other procedural means, their availability represents a *conditio sine qua non* for prosecution of certain types of crimes.[5] Typically cyberstalking is quite impossible to prove without relevant traffic data that show statistics and technical details of actions of the perpetrator. If some jurisdiction would not allow access to traffic data,[6] cyberstalking would become a virtual crime in the sense that this crime would be only

---

[2] See for example Edel, F. (2007) *The length of civil and criminal proceedings in the case-law of the European Court of Human Rights.* Strasbourg: Council of Europe Publishing.

[3] For the meaning of "virtuality" and "actuality", see Lévy, P. (2002) *Becoming Virtual – Reality in the Digital Age.* Plenum Trade.

[4] See for example Boehm, F. and Cole, M. D. (2014) *Data Retention after the Judgement of the Court of Justice of the European Union.* EP Greens/EFA Group. Available online from: http://orbilu.uni.lu

[5] See for example a U.S. Congress. (2011) *Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes: Hearing Before the Subcommittee on Crime, Terrorism, and Homeland Security of the Committee on the Judiciary, House of Representatives.* U.S. Government Printing Office.

theoretically present in criminal statutes but would never actually appear in front of a court.

The second example is a case that involved *Google StreetView*. The *FCC* investigated an allegation that *Google* used an algorithm that was skimming the content, including highly sensitive personal data, from wireless networks in areas through which the *StreetView* cars were roaming.[7] *FCC* was only able to prove that *Google* cars were sniffing unsecured Wi-Fi networks, while there was lack of evidence that the same was done also to secured networks.[8] *Google* was at the end fined USD25,000 for what *David Kravets* named in *Wired* as *"stonewalling the investigation"*.[9]

The obstacles for which *Google* was fined were quite far from morally despicable. They can be simply explained as not enough willingness of *Google* to incriminate itself.

Google was asked to provide a copy of the actual data that it collected by sniffing wireless networks. In response, *Google* stated that

> *"it is not prudent or necessary for any governmental authority to examine the communications and personal information of U.S. citizens in order to resolve this matter"*.[10]

Put aside the question as to what extent it was "prudent and necessary" for *Google* to originally gather and process that data in the first place, what matters more is rather that the *FCC* was not given that data at all.

If, hypothetically, more pressure was put on *Google* by the *FCC*, *Google* could have e.g. given the *FCC* all the data collected by *StreetView* cars in raw format and asserted it possessed no means or motivation to interpret them. In that case, the *FCC* would have been left with an endless amount of binary data and a need to find someone to interpret them. A second option for

---

[6] It is to be noted here that some EU jurisdictions derogated the data retention duties, but traffic data are still available there through other procedural means (typically through general provisions related to stored communications). While there are some EU jurisdictions that do not provide for a duty to retain traffic data, there are no EU jurisdictions where traffic data would not be used by law enforcement.

[7] For analysis of this case, see Polcak, R. and Svantesson, D. (2017) *Information Sovereignty*. Edward Elgar Publishing, p. 170.

[8] See the FCC Notice of Apparent Liability for Forfeiture of 13 April 2012, File No EB-10-EH-4055. It is available in an unredacted version from: http://www.wired.com/images_blogs/threatlevel/2012/05/unredactedfccgoog.pdf

[9] See Kravets, D. (2012) An Intentional Mistake: The Anatomy of Google's Wi-Fi Sniffing Debacle. *Wired*, 2 May. [online] Available from: https://www.wired.com/2012/05/google-wifi-fcc-investigation/ [Accessed 5 September 2019].

[10] See supra *FCC Notice*, fn. 89 (this footnote was for some reason blacked out in a redacted version that was later officially published by the *FCC*).

Google would be to assert that "the communications and personal information of U.S. citizens" had been deleted. The *FCC* would then either have to believe it or to prove that such a statement was not truthful which would require digging the respective data from somewhere. The second alternative is for obvious reasons rather unrealistic.[11]

Both above examples demonstrate clear disproportion between legislated and administered rights. First case shows a possible normative deficit when substantive provisions are not seconded with procedural rules needed for enforcement of respective substance. Second case shows actual practical (or institutional) deficit when procedural provisions do exist, but technical complexity of respective matter makes it impossible to efficiently use them and there is no way of normatively fixing it.

Lack of congruence between substance and administration of rights is hugely present also in algorithmic administration of rights.[12] The problem is relatively simple here – the lack of normative grounds, the amount and relevance of technical obstacles,[13] high costs, or all these factors at the same time,[14] prevent individuals as well as law enforcement from efficient review of legal compliance of respective algorithms.[15]

The growing importance of this issue even provoked the establishment of a research group within the *International Academy of Constitutional Law* titled *Algorithmic State, Society and Market – Constitutional Dimensions*. Its mission statement notes that

> *"[s]ince information and data are the new sources of power in the algorithmic society, patterns of market consolidation risk generating technological asymmetry which gravitates to a handful of multinational private players. The state then finds itself in a peculiar position, as it becomes partly dependent on the technologies of these players while vying*

[11] Lack of ability for a sovereign to exercise its powers is referred to in these regards by *Healey* as "cyber-Somalia". See Healey, J. (2011) The spectrum of National Responsibility for Cyberattacks. *The Brown Journal of World Affaires*, 18 (1), p. 63.

[12] The same issue is tackled from a different perspective in Pasquale, F. (2017) Toward a Fourth Law of Robotics: Preserving Attribution, Responsibility, and Explainability in an Algorithmic Society. *Ohio State Law Journal*, 78, p. 1243.

[13] For other issues in legitimacy (or legality) of algorithmic administration of rights, see for example Gurumurthy, A. and Bharthur, D. (2018) Democracy and the Algorithmic Turn. *Sur – International Journal on Human Rights*, 27, p. 39.

[14] For a detailed analysis of problematic factors, see Bodo, B. et al. (2017) Tackling the Algorithmic Control Crisis – The Technical, Legal, and Ethical Challenges of Research into Algorithmic Agents. *Yale Journal of Law & Technology*, 19, p. 133.

[15] See Wolfe, A. (1990) Algorithmic Justice. *Cardozo Law Review*, 11, p. 1409.

for a similar position with respect to the data it collects and analyses, all at the same time as it retains the power (and legal responsibility) to regulate the industry and guarantee the protection of constitutional rights."

Currently, there are two ways in which the law tries to normatively deal with this issue – either through transparency of algorithms or through compulsory human review of individual algorithmic decisions. Transparency aims at making algorithm as such reviewable in order to find our whether its code is in line with corresponding legal rules.[16] The right for a human review aims at individual confrontation of a resulting decision rendered by an algorithm with a human assessment. The difference between both these legal tools is that transparency covers congruence *in abstracto* while the right for human review lays down a congruence review *in concreto*.

This comment, that is also to accompany a research proposal to the aforementioned research group, primarily focuses on the congruence *in abstracto*, i.e. transparency of algorithms. In order to break this complex problem down, we further look at two of its mostly relevant elements: procedure and institutions. Our aim in this comment is not to resolve any of these two issues, but rather to identify their scope and name their neuralgic points. At first, we will briefly look at the right to know the logic of rights-administering algorithms and try to define the question as to *what* should that right mean in particular from procedural perspective. Secondly, we will formulate subsequent research question as to *who* should implement and enforce such procedure.

2. PROCEDURAL ISSUES IN COMPLIANCE REVIEW

The right to know the logic of algorithmic processing of rights is already laid down in some countries – e.g. in the EU it is legislated in Art. 12 in connection with Recital 63 of the GDPR. At first sight, this right seems to serve as a procedural norm that deals with the issue of transparency of algorithms and consequently with congruence between substance and administration of algorithmically processed rights.

However, the right to know the logic of algorithmic decisions does not actually represent a norm (or truly a "right") but rather only a general

[16] See Perel, M. and Elkin-Koren, N. (2017) Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement. *Florida Law Review*, 69, p. 181.

principle. The scope of this right is so general that it is utterly impossible to directly (i.e. through syllogistic application upon particular facts) transform it into particular rights claimable by individuals who were affected by algorithmic decisions. In other words, if someone's loan application gets algorithmically rejected and the rejected applicant claims the right to know the logic of respective algorithm, there is no way to imply what exactly she is entitled to get.[17] If a court ruling would state e.g. that the plaintiff is "entitled to receive information on the logic of processing of her loan application", nobody (including the defendant) would be able to determine what should be done in order to comply.

One might understand the transparency right in the way that the applicant is entitled to receive just general information about factors that are taken into account by the algorithm. In that case, there is no way for the applicant or an independent reviewer to prove or even guess whether the algorithm works in line with substantive laws (e.g. with laws that ban discrimination).

Another possible interpretation is that the applicant is entitled to receive the actual code of the algorithm. In that case, which is not even overly probable due to legal constraints such as protection of copyrights or trade secrets, the applicant would be provided with an actual computer code and left to her own regarding its meanings – or provided with an explanation of the code that she will be never able to verify against the actual code.

Third option is that the applicant gets an opportunity to reversely engineer the algorithm in the way that the algorithm would be made available for testing of inputs and outputs. Such testing might then lead to a sort of recreation of the way in which the algorithm works. Similar to the previous case, finding out anything useful about the actual "logic of processing" is quite impossible here if the applicant is a common person and does not have behind her an army of boffins with a supercomputer technology.[18]

If we assume that the algorithm in question really lacks congruence with substantive rights, e.g. by being unreasonably discriminatory, a question remains as to how it is actually possible to reach particular legally relevant

[17] An attempt regarding clarification of this right is made in part dedicated to Art. 12 of the GDPR in Kuner, C. Bygrave, L. and Docksey, C. (2019) *The EU General Data Protection Regulation – A Commentary.* Oxford University Press, forthcoming.

[18] In addition, the availability of the algorithm for a reverse engineering would not give the investigator a proper picture in case of autonomous systems – see infra.

conclusion about such lack of congruence. The problem simply is that the transparency requirement is so general that it has no practical meaning in regular cases of complex or even autonomous algorithms.

3. INSTITUTIONAL ISSUES IN COMPLIANCE REVIEW

The issue of transparency seems a bit easier with man-made algorithms, because there possibly exists some "man" who ordered coding or even directly coded respective lack of congruence into the algorithm. Such person should then be able under existing legal procedures to state such lack of congruence in a legally relevant way (e.g. as a witness at court). However, the probability of that happening in real life is quite the same as it was with *Google* incriminating itself in the above Wi-Fi sniffing example.

Even worse from transparency perspective are cases when algorithms are made autonomously with no direct human involvement, i.e. in the case of neural networks or other AI-based systems that are only coded by humans to learn.[19] The resulting autonomously generated algorithm is in these cases unreadable even for an army of boffins. If such algorithm unreasonably discriminates or does anything similarly unlawful, it might be quite impossible even for its creator to find the core of the problem, not even speaking about repairing it.[20]

Both above reasons are good enough for assuming that any other than utterly simple algorithms need to be legally tackled either as black or nearly-black boxes.[21] While it is certainly possible to provide for normative requirements for turning black in this case into some shade of grey (such as those transparency requirements mentioned above), there still remains a question as to institutional backing of such arrangements.[22]

---

[19] See for example Lehr, D. and Ohm, P. (2017) Playing with the Data: What Legal Scholars Should Learn about Machine Learning. *University of California, Davis, Law Review*, 51, p. 653.

[20] A good example is the recent row over the *Tay* chatbot. Despite being developed by one of most advanced hi-tech corporations, *Microsoft*, *Tay* was constantly tweeting hate speech and nobody was able to fix that (so the only way for *Microsoft* to deal with all the shame was to simply switch *Tay* off). See Neff, G. and Nagz, P. (2016) Talking to Bots: Symbiotic Agency and the Case of Tay. *International Journal of Communication*, 10, p. 4915. The selection of most hateful autonomous tweets was published in Kleeman, S. (2016) Here Are the Microsoft Twitter Bot's Craziest Racist Rants. *gizmodo.com*, 24 March. [online] Available from: https://gizmodo.com/here-are-the-microsoft-twitter-bot-s-craziest-racist-ra-1766820160 [Accessed 5 September 2019].

[21] See for example Bose, U. (2015) The Black Box Solution of Autonomous Liability. *Washington University Law Review*, 92, p. 1325.

[22] The core role of institutional component of the rule of law represents a defining feature of institutional normativism. For a compendium of this methodological approach, see McCormick, N. and Weinberger, O. (1986) *An Institutional Theory of Law – New Approaches to Legal Positivism.* D Riedel Publishing.

In other words, one question is to provide for normative (or procedural) possibility of compliance review of algorithms, while the other issue is to have institutions pragmatically capable of doing so.[23]

One possible approach to the latter, institutional, issue is offered in the work of late *Sir Terence David John Pratchett*. His ant-powered computer[24] later named *Hex* also looks, even to its creator, *Ponder Stibbons*, as a black box, because calculations do not only depend here on man-made algorithms but mostly on behaviour of ants and, perhaps, also on complex informational effects of an anthill.[25] *Pratchett* paints here an institutional model where *Stibbons* is given the authority to declare that the *Hex* is faulty or broken and also the authority to adjust or repair it. That authority, however, is not based on the assumption that *Stibbons* precisely knows what is happening in the *Hex*, but because he is, thanks to his intelligence, experience, wisdom, moral profile and other personal properties, believed being capable of properly sensing that the results rendered by *Hex* are somewhat faulty.

The tricky element of this institutional arrangement is the required level of explicit reasoning for *Stibbons* to demonstrate a defect of the *Hex* as well as the required level of explanation of what and why *Stibbons* does in order to fix it. *Terry Prachett* puts it straight – *Stibbons'* thinking is so complex that it would not make sense for him to reason anything to anybody, because nobody would be able to understand him anyway.

It is obviously not possible to implement in full *Sir Terence's* model for identifying and fixing malfunctions in algorithmic processing of rights. One reason is that creators of respective systems do not always have to be as available and as capable as *Ponder Stibbons*. In addition, it is not entirely in line with rule of law principles to establish control or adjudicative competence only upon personal properties without at least a minimum requirement for knowing why, how and what is being done with the (allegedly) faulty machine.

At the same time, we already learned that relying purely on state--administered law enforcement is neither economically efficient nor

[23] See Baker, J. J. (2018) Beyond the Information Age: The Duty of Technology Competence in the Algorithmic Society. *South Carolina Law Review*, 69, p. 557.

[24] The first appearance of the *Hex* computer was in *Pratchett's* novel *Soul Music* from 1994.

[25] *Pratchett* does not mention that explicitly, but there is a good reason to believe that the *Hex* in fact uses fascinating complexity effects described by *Peter Coveney* and *Roger Highfield* in Coveney, P. and Highfield, R. (1996) *Frontiers of Complexity.* Penguin Random House, pp. 190–236.

technically possible in regulatory areas with strong technological aspect.[26] Consequently, we now witness a massive shift in technologically determined areas of law from state-administered behavioural rules to performance-based rules that are autonomously developed by those who are technically in charge (typically by service providers).[27] This move from state-ordered behaviour to state-ordered autonomous rulemaking has been already successfully applied in cybersecurity or personal data protection.[28]

In that sense, it is inevitable to allow the *Stibbons* regulatory model into areas such as algorithmic processing of rights not necessarily in its entirety, but at least in part. It means at first allowing and motivating an inclusion into the control and adjustment process also of those, who might not be officially legitimised, but whose technical competences and experience provide for reasonable and complex understanding of respective technology.

Also, it seems quite appropriate to admit that decisions about lack of legal compliance of algorithms will not always have to be based on perfect logical analysis and accordingly reasoned. That admittance is especially problematic, because one might say that code is a code and it ultimately breaks down to simple logical instructions as to turning I into O and *vice versa*. There is then no logical reason why a court or a similar body should be unable to come with exhausting logical argumentation as to what is wrong and how it should be fixed. The issue of *ipso facto* limited reviewability of decisions about lack of congruence of algorithms and laws is therefore highly problematic.[29]

---

[26] See Polcak, R. and Svantesson, D. (2017) *Information Sovereignty.* Edward Elgar Publishing, p. 6.

[27] For an explanation of nature and functioning of performance-based rules, see for example Coglianese, C. (2017) The Limits of Performance-Based Regulation. *University of Michigan Journal of Law Reform*, 50 (3), p. 525.

[28] Statutory examples include the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) or Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.

[29] Similar in nature are recent cases of security concerns over certain telecommunication technologies – these concerns are often well grounded, but it is impossible for security authorities to directly point to a particular threatening line of code or to a particular chip. Media then tend to interpret these situations as allegations with no particular evidence.

4. CONCLUSIONS

This comment looked at congruence between substance and administration of algorithmically processed rights. It particularly focused on procedural and institutional backing of assessment of compliance of algorithms with applicable laws. The purpose of this comment was to identify particular assignments for comparative constitutional research in this field.

The first identified research assignment is based on the assumption that transparency requirement regarding algorithms is so broad that it covers everything and nothing at the same time, so there is a need to formulate at least a bit more particular procedural right (or rights). If such right or rights are found and formulated, they may be used either directly by being implemented into the black-letter law, codes of conduct etc. or indirectly through interpretation of the existing vastly general transparency requirements (such as those laid down currently in the GDPR) by courts or other public authorities.

Second particular research task that was identified in this comment relates to the extent to which particular legal systems are able to swallow a possible shift from recent standards of input and output legitimacy[30] of authoritative decisions[31] in order to provide for efficiency of abstract review of algorithms that administer rights. This task assumes that courts and other legitimised authorities are incapable of properly reviewing complex algorithms.

Even if a technically capable body is found or established, it might not be possible in regular cases to logically reason why some complex (or even autonomous) algorithm is not in line with rules that it is to administer. Consequently, there is a need to tackle the challenge of a required level of reasoning of legally relevant statements (mostly judgments, administrative decisions, official statements etc.) that declare lack of congruence between an algorithm and applicable law.

---

[30] For the meaning of the terms "input-" and "output legitimacy", see for example Loth, M. A. (2007) Courts in Search of Legitimacy: The Case of Wrongful Life. In: Sellers, M. (ed.). *Autonomy in the Law.* Springer Netherlands, pp. 73–96.

[31] For a comprehensive comparative study of such standards in the US and Europe, see De Lasser, M. (2009) *Judicial deliberations: a comparative analysis of transparency and legitimacy*. Oxford University Press.

LIST OF REFERENCES

[1] Baker, J. J. (2018) Beyond the Information Age: The Duty of Technology Competence in the Algorithmic Society. *South Carolina Law Review*, 69.

[2] Bodo, B. et al. (2017) Tackling the Algorithmic Control Crisis – The Technical, Legal, and Ethical Challenges of Research into Algorithmic Agents. *Yale Journal of Law & Technology*, 19.

[3] Boehm, F. and Cole, M. D. (2014) *Data Retention after the Judgement of the Court of Justice of the European Union.* EP Greens/EFA Group. Available online from: http://orbilu.uni.lu

[4] Bose, U. (2015) The Black Box Solution of Autonomous Liability. *Washington University Law Review*, 92.

[5] Coglianese, C. (2017) The Limits of Performance-Based Regulation. *University of Michigan Journal of Law Reform*, 50 (3).

[6] Coveney, P. and Highfield, R. (1996) *Frontiers of Complexity.* Penguin Random House.

[7] De Lasser, M. (2009) *Judicial deliberations: a comparative analysis of transparency and legitimacy*. Oxford University Press.

[8] Edel, F. (2007) *The length of civil and criminal proceedings in the case-law of the European Court of Human Rights.* Strasbourg: Council of Europe Publishing.

[9] Fuller, L. (1969) The Morality of Law. *Yale University Press*.

[10] Gurumurthy, A. and Bharthur, D. (2018) Democracy and the Algorithmic Turn. *Sur – International Journal on Human Rights*, 27.

[11] Healey, J. (2011) The spectrum of National Responsibility for Cyberattacks. *The Brown Journal of World Affairs*, 18 (1).

[12] Kleeman, S. (2016) Here Are the Microsoft Twitter Bot's Craziest Racist Rants. *gizmodo.com*, 24 March. [online] Available from: https://gizmodo.com/here-are-the-microsoft-twitter-bot-s-craziest-racist-ra-1766820160 [Accessed 5 September 2019].

[13] Kravets, D. (2012) An Intentional Mistake: The Anatomy of Google's Wi-Fi Sniffing Debacle. *Wired*, 2 May. [online] Available from: https://www.wired.com/2012/05/google-wifi-fcc-investigation/ [Accessed 5 September 2019].

[14] Kuner, C. Bygrave, L. and Docksey, C. (2019) *The EU General Data Protection Regulation – A Commentary.* Oxford University Press, forthcoming.

[15] Lehr, D. and Ohm, P. (2017) Playing with the Data: What Legal Scholars Should Learn about Machine Learning. *University of California, Davis, Law Review*, 51.

[16] Lévy, P. (2002) *Becoming Virtual – Reality in the Digital Age.* Plenum Trade.

[17] Loth, M. A. (2007) Courts in Search of Legitimacy: The Case of Wrongful Life. In: Sellers, M. (ed.). *Autonomy in the Law.* Amsterdam: Springer Netherlands.

[18] McCormick, N. and Weinberger, O. (1986) *An Institutional Theory of Law – New Approaches to Legal Positivism.* D Riedel Publishing.

[19] Neff, G. and Nagz, P. (2016) Talking to Bots: Symbiotic Agency and the Case of Tay. *International Journal of Communication*, 10.

[20] Pasquale, F. (2017) Toward a Fourth Law of Robotics: Preserving Attribution, Responsibility, and Explainability in an Algorithmic Society. *Ohio State Law Journal*, 78.

[21] Perel, M. and Elkin-Koren, N. (2017) Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement. *Florida Law Review*, 69.

[22] Polcak, R. and Svantesson, D. (2017) *Information Sovereignty.* Edward Elgar Publishing.

[23] U.S. Congress. (2011) *Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes: Hearing Before the Subcommittee on Crime, Terrorism, and Homeland Security of the Committee on the Judiciary, House of Representatives.* U.S. Government Printing Office.

[24] Wolfe, A. (1990) Algorithmic Justice. *Cardozo Law Review*, 11.

<<< COMMENTARIES

BOOK REVIEWS >>>

DOI 10.5817/MUJLT2019-2-12

AUTONOMOUS VEHICLES AND THE LAW: TECHNOLOGY, ALGORITHMS AND ETHICS. LIM, Y. H.

by

VERONIKA ŽOLNERČÍKOVÁ*

Lim, Y. H. (2018) Autonomous Vehicles and the Law: Technology, Algorithms and Ethics. Cheltenham: Edward Elgar Publishing, 147 p.

The ninth instalment of Elgar law, technology and society series, *Autonomous Vehicles and the Law: Technology, Algorithms and Ethics*, is focused on autonomous vehicles, new technology on the rise that stirs discussions in various fields of law, such as data protection, tort liability, traffic laws, cybersecurity and ethics.

Elgar law, technology and society series aims to provide an interdisciplinary forum for debate concerning legal and social implications of digital technology.[1] The interdisciplinary approach of the reviewed book is allowed by the author's double degrees in Computer Science and in Law.[2]

Autonomous Vehicles and the Law: Technology, Algorithms and Ethics represents a concise contribution to the debate on artificial intelligence and law, explaining the underlining technology on an example of self-driving vehicles. The book provides a profound background on the self-driving technology with the purpose to explain it in an understandable manner to lawyers.

* zolnercv@law.muni.cz, Ph.D. candidate at the Institute of Law and Technology at Masaryk University, Brno, The Czech Republic.

1 *Elgar law, technology and society series*. [online] Available from: https://www.e-elgar.com/shop/books?book_series=Elgar%20Law,%20Technology%20and%20Society%20series [Accessed 20 August 2019].

2 See p. viii of the book.

As stated in the book's *Preface*, the author's intent was to clarify exaggerations and misconceptions about autonomous vehicles.[3] According to her, those first appeared in the popular press but spread to the academic literature as well. As a remedy she proposes firstly to bring about the general understanding of the issue and subsequently to formulate new ideas on the regulation concerning autonomous vehicles in the publication.[4]

The main hypothesis of this book, as stated in the *Introduction*, is that autonomous vehicles are not as safe as manufacturers tend to claim and that much of the legal literature is based on misconceptions[5]. The most important of which is that autonomous vehicles are based on a brand-new technology, when in reality functions of self-driving vehicles are set within the well-known framework of computer programs.[6] Therefore, they might be not the solution we are looking for, since some of these features are already present in conventional vehicles and their functions are limited.[7]

After the assessment of the state of the art of the technology, the author confirms her hypothesis that the technology is not yet ready for full operation and neither statistics nor science proves it would be safer than current road traffic system.[8]

Furthermore, the author considers the public focus on autonomous mobility to be a hype.[9] Therefore, her goal is to clarify the inherent limitations of the technology putting to use her knowledge on the subject.[10] Subsequently, current legal standards are assessed, and new regulations and ethical considerations are discussed.[11] The first goal is achieved by a thorough theoretical explanation of the technology. The second goal, the assessment from the legal standpoint, is more of a collection of the author's own ideas on the matter.

The book can be, in the reviewer's opinion, divided into two parts based on the prevalent content of its chapters and the method used. *Chapters 2 to 4* and *chapter 7* focus solely on the technical aspects of autonomous vehicles,

---

[3] See p. ix of the book.
[4] Ibid.
[5] See pp. 1–3 and pp. 136–137 of the book.
[6] See p. 2 of the book.
[7] Ibid.
[8] See p. 133 of the book.
[9] See p. ix of the book.
[10] See pp. 1–3 of the book.
[11] See p. 3 of the book.

mainly on available data concerning accidents of autonomous vehicles.[12] These are more of a descriptive nature. On the contrary, *chapter 5 and 6* cover legal and ethical issues and reflect author's own thoughts on the matter.

Concerning the legal and ethical part, the book provides a good summary of current regulatory approaches in the chapter *The road less travelled for regulators*[13] and a detailed analysis of ethical guidelines presented by an *Ethics Committee* set by the German *Ministry of Transport and Digital Infrastructure* in chapter *Ethical responsibilities and autonomous vehicles*[14]. What do these chapters bring to legal academic literature on the matter?

The road less travelled tackles the problem of verifiable standards of care. It focuses mostly on the software of the vehicle, allowing us to explore this specific issue in detail. Additionally, the chapter *Ethical responsibilities and autonomous vehicles* offers an in-depth analysis of the German ethical guidelines, aiming to go beyond the trolley problem.[15] The enforceability of proposed ethics guidelines is measured against the real amount of control the programmer can have over different types of programming of autonomous vehicles. Both chapters are welcomed additions to academic literature on the subject offering a specialized view on the matter.

That said, the framing of the legal and ethical part is very confusing. Whereas during the technical chapters of the book the focus lies on the United Kingdom, the United States of America and Australia, their regulations and case law, chapter 5, *The road less travelled for regulators*, suddenly includes only US laws and then EU Product Defect Directive and Road Traffic Act in Germany. The next chapter focuses only on Ethical guidelines in Germany. The reason behind focusing on these specific documents is not explained in the book. Nor is mentioned the existence of other relevant regulations, such as the regulation in Netherlands, which is on top of the *Autonomous Vehicles Readiness Index*[16] and surely worth mentioning. As a result, a non-informed reader might get the idea that such

[12] Worldwide accidents of *Tesla Model S*, *Tesla Model X* and *Uber* taking place from 2016 to 2018 are included.

[13] See pp. 99–116 of the book.

[14] See pp. 117–132 of the book.

[15] See pp. 117–118 of the book.

[16] KPMG. (2019) *2019 Autonomous Vehicles Readiness Index*. [online] Available from: https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/02/2019-autonomous-vehicles-readiness-index.pdf [Accessed 20 August 2019].

regulation is unavailable. However, a regulation is effective or is in the approval proceedings also in Canada, China, Japan, Norway, United Arab Emirates, Singapore and others.[17]

Furthermore, the manuscript is based on literature published before 26 May 2018.[18] It also reflects accidents occurring during the year 2018.[19] But when talking about the EU Product Defect laws, only *Guidelines on Regulating Robotics*[20] from 2014 are mentioned. On the other hand, the *Report with Recommendations to the Commission on Civil Law Rules on Robotics*[21] from July 2017 is omitted as well as the document *Liability for Emerging Digital Technologies*[22] from April 2018. Both are relevant for autonomous mobility and the debate around liability for product defects.

The choices of the author to include some documents and not others for the assessment in chapter 5 might be intentional. However, a clear methodology regarding the selection of mentioned documents is missing. That disables the researchers who would like to be able to follow author's train of thoughts from doing so.

Chapter 3 called *Verifiable standards of care* is the most crucial chapter of the book. It is beneficial to everyone who is interested in the topic, whether a legal professional or a member of the general public. It is very well written, and it provides an up-to-date summary of road traffic accidents involving autonomous vehicles in an understandable manner, yet with more expertise than we are used to from newspaper articles.

Even though this chapter does not primarily address the issue of allocation of liability, it serves as a foundation for further debate about the matter. It differentiates among the malfunctions of sensors, the car as a whole and the driving software. The author states in every case who is (in her opinion) the one in breach with standard of care. The standard of care, she is using, is based on the legislation in the UK, US and Australia.

---

[17] Ibid.

[18] See p. ix of the book.

[19] See pp. 99–116 of the book.

[20] Palmerini, M. (2014) *Guidelines on Regulating Robotics*. [online] Available from: http://www.robolaw.eu/index.htm [Accessed 20 August 2019].

[21] European Parliament. (2017) *Report with Recommendations to the Commission on Civil Law Rules on Robotics*. [online] Available from: http://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html [Accessed 20 August 2019].

[22] European Commission. (2018) *Liability for Emerging Digital Technologies*. [online] Available from: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137 [Accessed 20 August 2019].

The next chapter, *Software: difficult to verify standards of care*, specifically addresses the issue software in autonomous vehicles from the technical perspective. The author differentiates between so-called verifiable standards of care, which are applied to the physical components and the non-existent standards for software. These revolve around the technology that should be used for the development of autonomous software[23] as well as datasets[24], from which it shall learn. This chapter is also a must-read to anyone who wants to further their knowledge of autonomous vehicles. It offers easily understandable explanations on different programming choices, differences between automatic and autonomous functions of software and issues with the burden of proof when it comes to software.

The overall problem of software regulation is well summarised at the beginning of the next chapter[25] called *The road less travelled for regulators*. The knowledge gained on possible programming choices is useful in the chapter on ethics. Both chapters were discussed earlier in the review.

Overall, the book is beneficial to everyone interested in autonomous mobility and easily understandable for people with legal background. Benefits of the book lie especially in this thorough analysis of series of accidents of autonomous vehicles from 2016 to 2018, their causes and how they influenced the development of the field. All presented cases are followed with a summary on how this affects or should affect relevant regulation in the field. The author's unique perspective, as a lawyer and a computer scientist, allows her to stress the issues that are most challenging from a legal perspective.

The book aimed high – it attempted to clarify some common misconceptions both from a technical and legal standpoint. The reviewer is of the opinion that it did a great job doing so especially from the technical point of view. The shortcomings of the publication are mentioned above and affected only the parts on regulation and ethics. The only regrettable thing is that the concise format might have prevented the author to explain more about her choices or to argue more about certain issues.

[23] See pp. 82–94 of the book.
[24] See pp. 94–99 of the book.
[25] See pp. 99–110 of the book.

For those looking for complex information on autonomous vehicles, this book does not cover all. For example, it does not tackle some issues related to standards of care and product defect liability, such as interconnected road traffic systems or possible choices on how to mitigate damages with other legal tools than just liability. However, this is covered thoroughly in other literature, which can greatly complement the book by *Lim*.[26] For a broader view on the topic of autonomous mobility, the book *Autonomous driving* by *Maurer et al.*[27] can be also recommended by the reviewer.

What the book *Autonomous Vehicles and the Law: Technology, Algorithms and Ethics* does offers compared to other literature is a unique interdisciplinary perspective that will be invaluable to those who crave more information on the operation of autonomous technology, such as scholars or policy makers, and a pleasant read to others.

LIST OF REFERENCES

[1] Collingwood, L. (2017) Privacy Implications and Liability Issues of Autonomous Vehicles. *Information & Communications Technology Law*, 26 (1).

[2] De Bruyne, J. and Tanghe, J. (2018) Liability for Damage Caused by Autonomous Vehicles: A Belgian Perspective. *Journal of European Tort Law*, 8 (3).

[3] *Elgar law, technology and society series*. [online] Available from: https://www.e-elgar.com/shop/books?book_series=Elgar%20Law,%20Technology%20and%20Society%20series [Accessed 20 August 2019].

[4] European Commission. (2018) *Liability for Emerging Digital Technologies*. [online] Available from: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137 [Accessed 20 August 2019].

[5] European Parliament. (2017) *Report with Recommendations to the Commission on Civil Law Rules on Robotics*. [online] Available from: http://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html [Accessed 20 August 2019].

[26] See Schellekens, M. (2015) Self-driving Cars and the Chilling Effect of Liability law. *Computer Law & Security Review*, 31 (4), pp. 506–517; Schellekens, M. (2018) No-fault Compensation Schemes for Self-driving Vehicles. *Law, Innovation and Technology*, 10 (2), pp. 314–333; Prakken, H. (2017) On the Problem of Making Autonomous Vehicles Conform to Traffic Law. *Artificial Intelligence and Law*, 25 (3), pp. 341–363; Prakken, H. (2017) On Making Autonomous Vehicles Respect Traffic Law: A Case Study for Dutch Law. *Proceedings of the 16th edition of the International Conference on Artificial Intelligence and Law*, pp. 241–244; De Bruyne, J. and Tanghe, J. (2018) Liability for Damage Caused by Autonomous Vehicles: A Belgian Perspective. *Journal of European Tort Law*, 8 (3), pp. 324–371; Collingwood, L. (2017) Privacy Implications and Liability Issues of Autonomous Vehicles. *Information & Communications Technology Law*, 26 (1), pp. 32–45.

[27] Maurer, M. et al. (2016) *Autonomous Driving: Technical, Legal and Social Aspects*. Berlin: Springer Berlin Heidelberg.

[6] KPMG. (2019) *2019 Autonomous Vehicles Readiness Index*. [online] Available from: https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/02/2019-autonomous-vehicles-readiness-index.pdf [Accessed 20 August 2019].

[7] Maurer, M. et al. (2016) *Autonomous Driving: Technical, Legal and Social Aspects.* Berlin: Springer Berlin Heidelberg.

[8] Palmerini, M. (2014) *Guidelines on Regulating Robotics*. [online] Available from: http://www.robolaw.eu/index.htm [Accessed 20 August 2019].

[9] Prakken, H. (2017) On Making Autonomous Vehicles Respect Traffic Law: A Case Study for Dutch Law. *Proceedings of the 16th edition of the International Conference on Artificial Intelligence and Law*.

[10] Prakken, H. (2017) On the Problem of Making Autonomous Vehicles Conform to Traffic Law. *Artificial Intelligence and Law*, 25 (3).

[11] Schellekens, M. (2015) Self-driving Cars and the Chilling Effect of Liability law. *Computer Law & Security Review*, 31 (4).

[12] Schellekens, M. (2018) No-fault Compensation Schemes for Self-driving Vehicles. *Law, Innovation and Technology*, 10 (2).

MUJLT Official Partner (Czech Republic)

ROWAN LEGAL, advokátní kancelář s.r.o.
www.rowanlegal.com/cz/

Cyberspace 2018 Partners

Vodafone Czech Republic
www.vodafone.cz

Wolters Kluwer ČR
www.wkcr.cz

Zákony pro lidi - AION CS
www.zakonyprolidi.cz

CODEXIS - ATLAS consulting
www.codexis.cz

Notes for Contributors

Focus and Scope

Masaryk University Journal of Law and Technology (ISSN on-line 1802-5951, ISSN printed 1802-5943) is a peer-reviewed academic journal which publishes original articles in the field of information and communication technology law. All submissions should deal with phenomena related to law in modern technologies (e.g. privacy and data protection, intellectual property, biotechnologies, cyber security and cyber warfare, energy law). We prefer submissions dealing with contemporary issues.

Structure of research articles

Each research article should contain a title, a name of the author, an e-mail, keywords, an abstract (max. 1 500 characters including spaces), a text (max. 45 000 characters including spaces and footnotes) and list of references.

Structure of comments

All comments should contain a title, a name of the author, an e-mail, keywords, a text (max. 18 000 characters) and a list of references.

Structure of book reviews

Each book review should contain a title of the book, a name of the author, an e-mail, a full citation, a text (max. 18 000 characters) and a list of references.

Structure of citations

Citations in accordance with AGPS Style Guide 5th ed. (Harvard standard), examples:

Book, one author: Dahl, R. (2004) *Charlie and the Chocolate Factory*. 6th ed. New York: Knopf.
Book, multiple authors: Daniels, K., Patterson, G. and Dunston, Y. (2014) *The Ultimate Student Teaching Guide.* 2nd ed. Los Angeles: SAGE Publications, pp.145-151.
Article: Battilana, J. and Casciaro, T. (2013) The Network Secrets of Great Change Agents. *Harvard Business Review*, 91(7) pp. 62-68.
Case: *Evans v. Governor of H. M. Prison Brockhill* (1985) [unreported] Court of Appeal (Civil Division), 19 June.
Citation Guide is available from: https://journals.muni.cz/public/journals/36/download/Citationguide.pdf

Formatting recommendations

Use of automatic styles, automatic text and bold characters should be omitted.
Use of any special forms of formatting, pictures, graphs, etc. should be consulted.
Only automatic footnotes should be used for notes, citations, etc.
Blank lines should be used only to divide chapters (not paragraphs).
First words of paragraphs should not be indented.
Chapters should be numbered in ordinary way – example: "5.2 Partial Conclusions".

Submissions

Further information available at
https://journals.muni.cz/mujlt/about

LIST OF ARTICLES

LIST OF COMMENTARIES

LIST OF BOOK REVIEWS