MASARYK UNIVERSITY JOURNAL OF LAW AND TECHNOLOGY

VOLUME **14** | NUMBER **2** | FALL **2020** | ISSN **1802-5943**

PEER REVIEWED

CONTENTS:

www.mujlt.law.muni.cz

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

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

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

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 **14** | NUMBER **2** | FALL **2020**

LIST OF ARTICLES

LIST OF COMMENTARIES

LIST OF BOOK REVIEWS

DOI 10.5817/MUJLT2020-2-1

PROCESSING OF GENETIC DATA UNDER GDPR: UNRESOLVED CONFLICT OF INTERESTS

by

PETRO SUKHOROLSKYI[*], VALERIIA HUTSALIUK[**]

Over the last decades, developments in the fields of genetics and bioinformatics caused a marked increase in the processing of human genetic data by various companies and institutions. This results in the adoption of several international documents and the emergence of legal norms on the protection of genetic data. The paper examines how and to what extent the interests and rights of the data subject with regard to the processing of genetic data are protected in the European Union. It is concluded that under the GDPR this task is implemented through classifying genetic data as sensitive, reliance on anonymisation and pseudonymisation, as well as introduction of the procedure of data protection impact assessment. Nevertheless, given the unique characteristics of genetic data distinguishing them from other categories of personal data, these measures cannot be regarded as sufficient and effective. The paper argues that current EU data protection legislation creates favourable conditions for genetic research, thereby ensuring particular public interests, but does not establish a special regime for genetic data processing appropriate to potential threats in this field and risks to the rights of data subjects.

KEY WORDS

Anonymisation, Balancing of Interests, Data Protection Impact Assessment, General Data Protection Regulation, Genetic Data, Pseudonymisation, Research Exemption, Sensitive Data, Special Categories of Personal Data

[*] petro.m.sukhorolskyi@lpnu.ua, Associate Professor at Lviv Polytechnic National University, Department of International Information, Ukraine.

[**] valeriiahutsaliuk@gmail.com, Lviv Polytechnic National University, Ukraine.

1. INTRODUCTION

The emergence at the national and international levels of legal rules protecting the rights of natural persons regarding the processing of their personal data is both a direct consequence of the rapid development of information technology in the second half of the twentieth century and an attempt to respond appropriately to the threats posed by it. However, science does not stand still and the information revolution we are witnessing is probably far from over. In this regard, the legislative and other public authorities are forced to constantly respond to the changing environment in which personal data protection rules adopted by them must be applied. This is not an easy task, as they have to act in the face of uncertainty of many factors and to balance between the various vital public and private interests, none of which can be ignored.[1]

The European Union is recognized as the world's leader in creating advanced standards of personal data protection. The new *General Data Protection Regulation 2016/679*[2] (hereinafter referred to as the "GDPR") adopted by it in 2016, which came into force in 2018, replacing the former *Directive 95/46/EC*[3], is precisely such an attempt to respond to the challenges of the time and to create a solid foundation for the protection of various private and public interests in this field. One of the innovations of the GDPR is the provisions concerning human genetic data the processing of which has radically increased in recent years.[4] This fact has not been overlooked by other international organizations concerned with issues such as development of science and personal data protection.

---

1 Borry, P. et al. (2018) The Challenges of the Expanded Availability of Genomic Information: An Agenda-Setting Paper. *The Journal of Community Genetics*, 9 (2), pp. 103–116.

2 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. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN [Accessed 7 March 2020].

3 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) 23 November. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en [Accessed 7 March 2020].

4 For instance, according to *Regalado*, by 2019 more than 26 million consumers had added their DNA to four leading commercial databases. If this trend continues, this figure is expected to rise to 100 million within 24 months. Regalado, A. (2019) More than 26 million people have taken an at-home ancestry test. *MIT Technology Review*. [online] Available from: https://www.technologyreview.com/s/612880/more-than-26-million-people-have-taken-an-at-home-ancestry-test/ [Accessed 7 March 2020].

In particular, in 2003, the *General Conference of UNESCO* adopted a landmark document entitled the *International Declaration on Human Genetic Data*. Even earlier, in 1997, the *Committee of Ministers of the Council of Europe* adopted the *Recommendation R (97) 5 on the Protection of Medical Data*, containing much reference to genetic data. In 2018, the provision on genetic data was added to the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS. No. 108)* through the adoption of the *Protocol (CETS No. 223)* amending the Convention.

Although the protection of genetic information derived from human tissue is not yet the subject of special interest of a wide range of legal scholars, it is still an important issue for detailed examination because it opens up entirely new problems and makes one think about the perspectives of the whole contemporary system of personal data protection. In such a case of conflict between two important interests, it is difficult to reconcile them in order to achieve a stable and harmonious balance. On the one hand, there are interests of individuals whose genetic data are processed, as well as significant public interests related to the control over extremely powerful technologies and the specific ways they are applied. On the other hand, there are equally important interests related to conducting research in the fields of genetics and bioinformatics that are crucial for overcoming certain urgent problems of humanity. Accordingly, there exist legitimate expectations of society for an increase of scientific knowledge, which are highlighted in the GDPR.[5]

Taking all these things into consideration, our main task is to investigate how and to what extent these interests are protected in the current EU legislation. In particular, we tried to find out whether the level of protection of natural persons with regard to the processing of their genetic data increases over time and whether it responds to the current realities and challenges posed by the rapid development of science and technology.

Over the last three decades, interrelated issues such as the legal protection of human genetic data, the maintenance of genetic privacy, and the prevention of genetic discrimination have repeatedly attracted attention of researchers from various scientific disciplines. Among the scholars who made a significant contribution to research in this field are *P. Billings*, *L. Bygrave*, *M. Gerstein*, *L. Gostin*, *Y. Erlich*, *B. Korf*, *T. Lemke*, *M. Taylor*. Since

[5] See Recital 113 of the GDPR.

the GDPR was adopted, a number of academic works (in particular, by *P. Borry*, *A. de Paor*, *K. Pormeister*, *M. Shabani*, *L. Quinn*, *P. Quinn*) directly related to the processing of personal genetic data under the current EU legislation have been presented.

2. GENETIC DATA AS A SPECIAL CATEGORY OF PERSONAL DATA

The GDPR contains several provisions concerning genetic data and the risks associated with their processing. Besides, the very definition of personal data is supplemented by a reference to genetic factors as one of the identifiers of a natural person.[6] In contrast, genetic data or characteristics are not mentioned in the Directive 95/46/EC at all. However, this does not mean that at the time when the Directive was in force, such data did not fall under the EU legislation or was not considered as personal data. In its documents the *Working Party on the protection of individuals with regard to the processing of personal data* – an advisory body established under Article 29 of the Directive (hereinafter referred to as the *Article 29 Working Party*) made repeated references to the issues related to genetic data and highlighted the need to ensure that they are properly handled. This matter is even addressed by a separate act of the *Working Party* entitled the *Working Document on Genetic Data*, which was adopted in 2004.[7] It is of special significance for us as it makes it possible to compare the EU's genetic data protection policy before and after the adoption of the GDPR.

The threats associated with the processing of genetic data are briefly mentioned in the GDPR. In particular, Recitals 71 and 75 outline the potential risks and possible discriminatory effects on natural persons on the basis of genetic or health status. However, it is doubtful whether these provisions provide a comprehensive and detailed picture of the threats in this field. For comparison, this issue is covered in greater detail in the Working Document of the *Article 29 Working Party*. It provides, *inter alia*, the following characteristics of genetic data distinguishing it from other categories of data and causing the necessity of greater protection:

---

[6] See Article 4 (1) of the GDPR.

[7] According to Article 30 of the Directive 95/46/EC, the *Working Party* is authorised to examine any question covering the application of the national measures adopted under the Directive and to advise on all matters relating to the protection of individuals with regard to the processing of personal data, as well as to perform other functions.

(1) genetic data reveal information not only about the data subject, but also about his or her blood relatives and certain groups of persons to which he or she belongs;
(2) as a rule, genetic information is unknown to the bearer him/herself and does not depend on the bearer's individual will since genetic data are non-modifiable;
(3) genetic data can be easily obtained from raw materials;
(4) genetic data may reveal more information in the future and be used by an increasing number of agencies for various purposes.[8]

The document also mentions the risks of genetic data re-use that might occur, *inter alia*, through additional analysis of stored biological materials and provides detailed information on threats of using such data for the purposes connected with employment,[9] insurance, identification, medical and scientific research. Besides, the *Article 29 Working Party* highlights

> *"the present absence of regulatory framework in the field of the on-line 'genetic testing direct to the public'"*.[10]

According to the GDPR, genetic data means

> *"personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question"*.[11]

---

[8] Article 29 Data Protection Working Party. (2004) *Working Document on Genetic Data*, 12178/03/EN WP 91, 17 March, pp. 4–5. Available from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp91_en.pdf [Accessed 9 March 2020].

[9] As for employment, the draft Regulation, adopted by *Parliament* at the first reading, stipulated that data collection for the purpose of genetic testing and analyses shall be prohibited in this field as a matter of principle. However, the relevant article was later removed. European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union* (2017/C- 378/399) 9 November, Article 82 (c). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014AP0212&from=EN [Accessed 7 March 2020].

[10] Article 29 Data Protection Working Party. (2004) *Working Document on Genetic Data*, 12178/03/EN WP 91, 17 March, pp. 13–14. Available from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp91_en.pdf [Accessed 9 March 2020].

[11] See Article 4 (13) of the GDPR.

It should be noted that in the draft Regulation, submitted by the European Commission in 2012, genetic data are defined in a different way as

> *"all data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development"*.[12]

The Working Document of the *Article 29 Working Party* sets out various definitions of genetic data which are taken from the Council of Europe Recommendation R (97) 5, Law of Luxembourg on the protection of persons with regard to the processing of personal data, and the *International Declaration on Human Genetic Data* adopted by *UNESCO*.[13] However, only in the last document as well as in the GDPR interpretation of genetic data is linked to the analysis of biological materials which should be carried out to obtain such data. This approach has been criticized by some researchers. In particular, *Shabani and Borry* consider this issue problematic because of the activities of DNA testing, medical, and other companies that use genealogical data gathered through both genetic investigation and various questionnaires filled out by their clients.[14] In addition, other factors like phenotypic characteristics may indicate some features of the personal genome. *Taylor* rightly points out that such information is far from being precise but this does not mean we can ignore its significance as well as potential harm caused by the improper use of such data.[15]

Such a narrow interpretation of genetic data is not fully justified, especially if taking primarily into account the interests of the data subject.[16] It is not excluded that in the future this definition can cause additional difficulties in the protection of individual's rights as he/she will have

---

[12] European Commission. (2012) *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM/2012/011 final – 2012/0011 (COD), 25 January, Article 4 (10). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN [Accessed 9 March 2020].

[13] Article 29 Data Protection Working Party. (2004) *Working Document on Genetic Data*, 12178/03/EN WP 91, 17 March, p. 4. Available from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp91_en.pdf [Accessed 9 March 2020].

[14] Shabani, M. and Borry, P. (2018) Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation. *European Journal of Human Genetics*, 26 (2), p. 152.

[15] Taylor, M. (2012) *Genetic Data and the Law: A Critical Perspective on Privacy Protection*. Cambridge: Cambridge University Press, p. 46.

[16] See also: De Paor, A. (2017) The European Union and Protection of Genetic Information. In: De Paor, A. (ed.). *Genetics, Disability and the Law: Towards an EU Legal Framework*. Cambridge: Cambridge University Press (Cambridge Disability Law and Policy Series), p. 230.

to prove that personal genetic data result from an analysis of a biological sample. Otherwise, provided that it is not medical data, he may be deprived of the rights guaranteed to the individual with regard to his personal data classified as sensitive. What is even more surprising is that the definition of genetic data under the GDPR refers to the

"analysis of a biological sample from the natural person in question",

that is, samples of a particular person who is the data subject. If a biological sample is taken from the blood relative of a particular individual (even in a case if the probability that they both have the same gene is extremely high), the result from the analysis of this sample will not be considered as this individual's genetic data. Consequently, he or she will have no rights related to this genetic information. In contrast, the definition of human genetic data from the aforementioned UNESCO Declaration, which can be considered as the most authoritative universal document in this field, only mentions that such information has to be *"obtained by analysis of nucleic acids or by other scientific analysis"* without making any reference to a biological material of a particular person.[17]

Thus, the GDPR does not take into account the considerations previously mentioned in the Working Document, namely the fact that genetic data reveal information about an individual's blood relatives, and does not ensure the protection of the rights of such persons.[18] The *Article 29 Working Party* was generally inclined to recognize some relatives' rights regarding the processing of genetic data (but without classifying them as data subjects) and noted the need for further study of this issue.[19] To address this problem, *Taylor* proposes to classify these persons as "secondary data subjects" and to clearly enshrine their rights.[20] It should also be recalled that the GDPR does not apply to deceased persons[21] and this creates additional risks for the aforementioned "secondary data subjects", since in such a case

[17] United Nations Educational, Scientific and Cultural Organization. (2003) *International Declaration on Human Genetic Data*, SHS/BIO/04/1, 16 October, Article 2 (i). Available from: http://portal.unesco.org/en/ev.php-URL_ID=17720&URL_DO=DO_TOPIC&URL_SECTION=201.html [Accessed 9 March 2020].

[18] Article 29 Data Protection Working Party. (2004) *Working Document on Genetic Data*, 12178/03/EN WP 91, 17 March, p. 4. Available from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp91_en.pdf [Accessed 9 March 2020].

[19] Op. cit., pp. 8–9.

[20] Taylor, M. (2012) *Genetic Data and the Law: A Critical Perspective on Privacy Protection*. Cambridge: Cambridge University Press, pp. 104, 117.

[21] See Recitals 27 and 158 of the GDPR.

the data is not protected by personal data protection law at all (unless the member states have adopted the relevant rules in accordance with the provisions of Recital 27).

Another important aspect is the protection of the rights of natural persons regarding their biological samples, which are the source of the bulk of genetic information the acquisition of which becomes more easily and cheaply available. That is, the threat to the person stemmed from unlawful handling of his or her biological samples could potentially be more serious than the one resulting from illegal processing of fragmented information about personal genome. Nevertheless, in accordance with the established principles governing personal data protection, the GDPR deals only with the data processing and the handling of biological samples falls outside of its scope. In this regard, *Taylor* proves the fallacy of the artificial distinction between the categories of interpreted genetic data (resulting from the analysis of a biological sample) and interpretable one (including biological samples), especially when the ultimate goal of regulation is to effectively protect the privacy of the individuals.[22] In any case, the justification of a separate regulation for the handling of genetic samples and the processing of data derived from these samples is questionable, given the fact that even companies collecting and using a large amount of genetic information often consider both as personal data.[23]

One of the key accomplishments of the GDPR is the clear and unambiguous assignment of genetic data to special categories of personal data. This imposes additional obligations on data controllers and is designed to guarantee the interests and rights of natural persons. Yet, in the past, the vast majority of genetic data was already classified as personal data belonging to special categories, namely to health data. In this regard, the *Working Document on Genetic Data* states that genetic data may reveal not only information on an individual's health status, but also his or her ethnic origin and, therefore, may also belong to the category of sensitive data. Besides, the *Working Party* drew the general conclusion that considering the

---

[22] Taylor, M. (2012) *Genetic Data and the Law: A Critical Perspective on Privacy Protection*. Cambridge: Cambridge University Press, pp. 158–165.

[23] For instance, *MyHeritage*, one of the world's largest genealogy research services companies, in its privacy policy statement, which contains the list of personal data that are collected and processed, places DNA samples, DNA Results, and DNA Reports in one group. MyHeritage. (2019) *MyHeritage Privacy Policy*. [online] Available from: https://www.myheritage.com/privacy-policy [Accessed 9 March 2020].

> *"extremely singular characteristics of genetic data and their link to information that may reveal the health condition or the ethnic origin, they should be treated as particularly sensitive data"*

within the meaning of the provisions of Directive 95/46/EC relating to special categories of personal data.[24] It is undeniable that classifying all personal genetic data as belonging to special categories and distinguishing them as a separate category is a step forward in ensuring adequate protection of the rights of individuals. On the other hand, unlike the Working Document, the GDPR does not recognize special characteristics and the exceptional sensitivity of genetic data, making it necessary to introduce special rules and measures. It only places genetic data in the extensive list of special categories of personal data, along with political opinions, religious or philosophical beliefs, trade union membership, etc. For comparison, in *Convention No. 108, as amended by the Additional Protocol of 2018*,[25] genetic data are classified as one out of the four groups of special categories of personal data. Moreover it is listed first and, at least, is clearly separated from all other categories.[26]

3. SAFEGUARDS FOR THE RIGHTS OF THE DATA SUBJECT

Taking into account the provisions of the GDPR and other relevant official documents,[27] it can be concluded that the task of guaranteeing the rights of individuals regarding the processing of their genetic data is implemented under the EU legislation through:

(a) classifying such data as sensitive;

---

[24] Article 29 Data Protection Working Party. (2004) *Working Document on Genetic Data*, 12178/03/EN WP 91, 17 March, p. 5. Available from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp91_en.pdf [Accessed 9 March 2020].

[25] Council of Europe. (2018) *Convention 108+ (Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data)*, 21 June, Article 6 (1). Available from: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf [Accessed 7 March 2020].

[26] It is worth noting that the lack of any other special provisions on genetic data in *Convention 108+* at a time when the urgency and significance of the matter is highlighted in many studies and genetic data processing has become widespread is, obviously, its serious drawback.

[27] For example, European Parliament. Committee on Petitions. (2019) *Petition No 0733/2018 by J.B. (Portuguese) on improving the protection of genetic data related to European Union citizens*, 15 March. Available from: https://www.europarl.europa.eu/doceo/document/PETI-CM-637225_EN.pdf [Accessed 7 March 2020].

(b) introduction of the procedure of data protection impact assessment;
(c) reliance on anonymisation and pseudonymisation of genetic data.

3.1. ADDITIONAL GUARANTEES REGARDING SENSITIVE DATA

Article 9 of the GDPR relating to the handling of special categories of personal data defines the legal grounds for their processing, in the absence of which such data cannot be processed. Although the list is extensive, given the specific nature of the use of genetic data, (1) the explicit consent of the data subject and

> (2) *"archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1)"*[28]

can be considered as two main grounds for their processing which cover the vast majority of cases. Comparing these provisions with the corresponding Article 8 of Directive 95/46/EC, it is noticeable that the list of legal grounds for the processing of special categories of data has been significantly broadened and supplemented, *inter alia*, by the aforementioned subparagraph on scientific research purposes relating directly to genetic data.

Another important difference is that the Directive specifying a short list of legal grounds enables member states to expand it for reasons of substantial public interest.[29] In contrast, the GDPR provides a broader range of grounds, but allows states to

> *"introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health"*.[30]

In assessing both options from the perspective of the data subject, it can be concluded that the new European standard established by the GDPR is less favourable to an individual, especially given the conventionality of borders when it comes to scientific research or the Internet service industry.[31] In realizing their right to introduce further conditions with regard to the processing of genetic data member states are limited by other

[28] See Article 9 (2) (a) and (j).
[29] See Article 8 (4) and Recital 34 of Directive 95/46/EC.
[30] See Article 9 (4) of the GDPR.
[31] Pormeister, K. (2017) Genetic data and the research exemption: is the GDPR going too far? *International Data Privacy Law*, 7 (2), p. 146.

provisions of the GDPR. In particular, Recital 9 refers to the negative effects of differences in national legislation on personal data protection, which prevent the free flow of data and constitute an obstacle to the pursuit of economic activities at the level of the Union. In addition, Recital 10 makes it clear that Article 9 (4) refers specifically to the possibility of introducing *"national provisions to further specify the application of the rules"* of the GDPR and not to a substantial deviation from its certain provisions (for instance, from those permitting the processing of genetic data for scientific research purposes without the consent of the data subject).

Other guarantees ensuring an adequate level of protection of the rights of individuals with regard to the processing of special categories of personal data, which are provided for in the GDPR, include the prohibition of automated individual decision-making based on such data (except in cases when the data subject has given his or her explicit consent or it is necessary for reasons of substantial public interest)[32] and the obligation of the controller and the processor to designate a data protection officer in the case where their core activities consist of processing on a large scale of special categories of data.[33] The draft Regulation submitted in 2012 comprised another important provision that empowered the *European Commission*

> *"to adopt delegated acts* [...] *for the purpose of further specifying the criteria, conditions and appropriate safeguards for the processing of the special categories of personal data"*.[34]

Obviously, such powers would make it possible to create uniform binding and detailed standards relating to the processing of genetic data within the EU, which would take into account the specific nature of this field. However, they, like most of the other powers of the *Commission* to adopt delegated acts pursuant to Article 92, were excluded in the later versions of the draft Regulation.

---

[32] See Article 22 (4) of the GDPR.

[33] See Article 37 (1) (c) of the GDPR.

[34] European Commission. (2012) *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM/2012/011 final – 2012/0011 (COD), 25 January, Article 9 (3). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN [Accessed 9 March 2020].

3.2. DATA PROTECTION IMPACT ASSESSMENT

The wording of Recital 89 leads to the conclusion that it is necessary to apply different approaches to the protection of individuals when it comes to the different types of personal data. In this regard, special emphasis should be placed on creating

> *"effective procedures and mechanisms which focus* [...] *on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons"*.[35]

One of such procedures provided for in Recitals 90 and 91 is a data protection impact assessment, the responsibility for which in accordance with Recital 84 remains with the data controller. Article 35 of the GDPR explicitly states that an impact assessment is required in the case of the *"processing on a large scale of special categories of data"*.[36] The grounds and procedures of such assessment are described in detail in the *Guidelines on Data Protection Impact Assessment* adopted in 2017 by the *Article 29 Working Party*.[37] This document explains, *inter alia*, what factors need to be taken into consideration when determining whether the processing is carried out on a large scale. The Guidelines also specifically state that the activities of

> *"a biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks"*

fall under the criteria of *"evaluation or scoring, including profiling and predicting"* [mentioned in Article 35 (3) of the GDPR] and, therefore, require an impact assessment.[38] Taking all this into account, it can be concluded that virtually all of the genetic data processing operations posing significant risks to society should be covered by the data protection impact assessment.

However, the feasibility and effectiveness of this assessment, as well as the objectivity of its results are quite another matter. In this regard, *Quinn and Quinn* point out that, in the case of the processing of a large

---

[35] See Recital 89 of the GDPR.

[36] See Article 35 (3) (b) of the GDPR.

[37] Article 29 Data Protection Working Party. (2017) *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, 17/EN WP 248, 4 April. Available from: http://ec.europa.eu/newsroom/document.cfm?doc_id=47711 [Accessed 9 March 2020].

[38] Op. cit., p. 9.

amount of genetic information, even a superficial assessment deals with a significant number of aspects. The consideration of all risks to the rights and freedoms of natural persons and the measures envisaged to address the risks, as provided for in Article 35 of the GDPR,

> *"would be a potentially enormous exercise demanding a truly multi--disciplinary perspective from disciplines such as ethics, law, genetics and sociology".*[39]

All of this raises doubts as to whether each data controller would be able to carry out such a procedure, whether the conclusions drawn up as a result of it would be objective and impartial, and as to whether, in general, such a mechanism is an effective way to safeguard the rights of natural persons with regard to the processing of their genetic data.

3.3. ANONYMISATION AND PSEUDONYMISATION

The third element of the protection of data subjects' rights according to the GDPR is the anonymisation and pseudonymisation of such data. Pursuant to Recital 26 information related to natural persons is classified into two groups: anonymous information and information concerning an identified or identifiable natural person (i.e. personal data). Furthermore, personal data which have undergone pseudonymisation should be considered as information on an identifiable natural person. This provision has been critically assessed by researchers who used pseudonymised genetic data in their studies and did not protect such data on an equal footing with personal data, as they believe it could have very negative consequences for genetic research.[40]

Article 4 of the GDPR defines pseudonymisation as

> *"the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures".*

[39] Quinn, P. and Quinn, L. (2018) Big genetic data and its big data protection challenges. *Computer Law & Security Review*, 34 (5), p. 1008.

[40] Shabani, M. and Borry, P. (2018) Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation. *European Journal of Human Genetics*, 26 (2), p. 151. See also: Mourby, M. et al. (2018) Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK. *Computer Law & Security Review*, 34 (2), pp. 222–233.

It places special emphasis on whether or not third parties are able to identify a person on the basis of such data. In this context, Recital 26 states that

> *"to determine whether the person is identifiable, account should be taken of all the means and factors reasonably likely to be used* [...] *to identify the natural person directly or indirectly"*,

inter alia, such factors as

> *"the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments"*.[41]

Although similar formulations are typical of international documents related to the processing of genetic data,[42] according to *Shabani and Borry*

> *"the existing heterogeneity in pseudonymisation methods* [...] *could be seen as a potential challenge in implementing the pertinent provisions"*.[43]

Regarding this issue it is doubtful whether one can correctly anticipate and take into account further technological advances in genetics and bioinformatics in order to draw the objective conclusion as to how much effort and resources would be necessary to identify the person by his or her pseudonymised data even in the near future. That is why the aforementioned provision can be treated as giving the data controller the possibility to rely on pseudonymisation as a guarantee for the protection of data subject rights, even when this procedure is not justified. Moreover, it is not clear what actions should be taken in a hypothetical future situation in which technological advances will make it possible to sharply reduce the time and effort required for identification of a person by his or her pseudonymised data, given the fact that such data will already be accessible to a wider range of persons.

---

41 See Recital 26 of the GDPR.

42 For example, the Recommendation of the Council of Europe, which contains a number of special provisions on genetic data, states the following: *"An individual shall not be regarded as 'identifiable' if identification requires an unreasonable amount of time and manpower"*. Council of Europe. Committee of Ministers. (1997) *Recommendation No. R (97) 5 on the Protection of Medical Data*, 30 October, paragraph 1. [online] Available from: https://rm.coe.int/1680505d5b [Accessed 7 March 2020].

43 Shabani, M. and Borry, P. (2018) Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation. *European Journal of Human Genetics*, 26 (2), p. 151.

Most of these points relate equally to another kind of depersonalisation of data, namely, anonymisation. Recital 156 and Article 89 of the GDPR relating to the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes emphasize the need to ensure the principle of data minimisation. In other words, personal data that are used for research purposes should be limited to what is necessary in relation to the purposes for which they are processed, given the obligation to respect the principle of proportionality and taking into consideration the need to use anonymous information wherever possible. The process of anonymising data that is conducted by the controller allows to exclude such data processing operations from the scope of the GDPR and removes the respective obligations of the controller to the data subject. It should be noted that Article 83 of the draft Regulation of 2012, which corresponds to Article 89 of the GDPR, in fact, provided for the explicit obligation to use anonymous information or pseudonyms for historical, statistical and scientific research purposes whenever possible.[44]

The main problem is that data anonymisation and pseudonymisation cannot be considered effective when it comes to the processing of genetic data. In particular, the *Opinion 05/2014 on anonymisation techniques* adopted by the *Article 29 Working Party* draws the attention of controllers to the fact that

> *"an anonymised dataset can still present residual risks to data subjects"*

and emphasizes that

> *"anonymisation should not be regarded as a one-off exercise and the attending risks should be reassessed regularly"*.[45]

Moreover, the Opinion refers to an example of genetic data, which, even without identifiers directly related to the data subject, can be further linked

---

[44] European Commission. (2012) *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM/2012/011 final – 2012/0011 (COD), 25 January, Article 83. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN [Accessed 9 March 2020].

[45] Article 29 Data Protection Working Party. (2014) *Opinion 05/2014 on Anonymisation Techniques*, 0829/14/EN WP216, 10 April, p. 4. Available from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf [Accessed 9 March 2020].

to him or her, especially in the light of current scientific advances.[46] In this regard, it is worth mentioning the study conducted by a team of scientists, led by *Erlich*, a computational geneticist at *MIT's Whitehead Institute for Biomedical Research*, in which they prove the ability to identify a person by his or her anonymised genetic data, as well as other data from publicly available sources.[47] Given current technological advances, *Quinn and Quinn* argue that

> *"anonymisation of big genetic research data may no longer be considered realistic"*.

They highlight three main factors making proper anonymisation elusive:

(1) the availability of big genetic data;
(2) the ability of researchers to access and share data around the world;
(3) the growth of computational power, as well as the development of ever more sophisticated identification algorithms.

In other words, the statement *"big human genetic data is always personal data"* is not far from the truth.[48]

The existing EU data protection legislation does not give sufficient attention to these facts and factors. This affects the corresponding privacy policy of global companies handling large amounts of genetic data, including those of EU citizens. For instance, *23andMe*, one of the world's largest genealogy research services companies, relies heavily on data anonymisation and pseudonymisation as safeguards for the protection of the rights and interests of data subjects when using genetic information for scientific research. But in doing so the company also recognizes that though it is difficult to identify the person by his or her de-identified genetic information, but not impossible, and warns about the likelihood of *"additional risks that are currently unforeseeable"*.[49] Thus, given the current

[46] Op. cit., p. 10.

[47] Gymrek, M. et al. (2013) Identifying personal genomes by surname inference. *Science*, 339, pp. 321–324. See also: Shabani, M. and Marelli, L. (2019) *Re-identifiability of genomic data and the GDPR: Assessing the re-identifiability of genomic data in light of the EU General Data Protection Regulation*. EMBO Rep, 20: e48316, 5 p. Available from: https://www.embopress.org/doi/10.15252/embr.201948316 [Accessed 7 March 2020].

[48] Quinn, P. and Quinn, L. (2018) Big genetic data and its big data protection challenges. *Computer Law & Security Review*, 34 (5), p. 1002.

[49] 23andMe. (2020) *Research Consent Document*, paragraph 5. [online] Available from: https://www.23andme.com/about/consent [Accessed 9 March 2020].

trends in genetic technology, it cannot be argued that the GDPR establishes the rules for the processing of genetic data which are advanced enough to provide an adequate response to the challenges ahead.

4. RESEARCH EXEMPTION

One of the most significant and controversial innovations of the GDPR is the introduction of the research exemption. This is about the relaxation of the rules on the handling of personal data, including derogations from the rights of the data subject when the processing of data is carried out

> *"for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes"*.

For comparison, Directive 95/46/EC did not provide for the general research exemption with respect to sensitive data, but member states had the right to lay down such exemptions for reasons of substantial public interest.[50]

Exemptions to the principles of the protection of personal data and restrictions of the rights of the data subject in the interest of science are found in several articles of the GDPR. In particular, Article 5 stipulates that the further data processing is allowed for scientific research purposes and shall not be considered as incompatible with the initial purposes (i.e. it allows exception to the purpose limitation principle)[51] and states that personal data may be stored for longer periods for such purposes (exception to the principle of storage limitation).[52] Article 9 (2) (j) establishes the research exemption to the general prohibition on the processing of special categories of personal data. Moreover, Article 14 (5) sets out an exception to the obligation of the data controller to provide the data subject with relevant information, where personal data have not been obtained from him or her, in cases where the provision of such information would involve a disproportionate effort for processing for archiving, scientific or historical research purposes. The same applies to the right of the data subject to have his or her personal data erased (*"right to be forgotten"*) specified in Article 17. Article 21 (6) allows for the derogation from the right to object in cases where data processing for scientific research

[50] See Article 8 (4) of the Directive 95/46/EC.

[51] For more on this issue, see Mészáros, J. and Ho, C. (2018) Big Data and Scientific Research: The Secondary Use of Personal Data under the Research Exemption in the GDPR. *Hungarian Journal of Legal Studies*, 59 (4), pp. 403–419.

[52] See Article 5 (1) (b) and (e) of the GDPR.

purposes is necessary for the performance of a task carried out for reasons of public interest. Finally, under Article 89 (2), Union or member state law may provide for derogations from a number of basic rights of the data subject (namely, the right of access, the right to rectification, the right to restriction of processing, and the right to object)

> *"in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes"*.

In addition, the research exemption is mentioned in several Recitals (50, 52, 53, 62, 65, and 113).[53]

As provided for in Article 89 and Recital 156, the legal safeguards protecting personal data from misuse for scientific research purposes amount to data minimisation, anonymisation, and pseudonymisation. Based on the above-mentioned considerations on the effectiveness of these tools when it comes to the processing of genetic data, it can be concluded that the GDPR provides favourable conditions for genetic research, while the rights of the data subjects with regard to the processing of their genetic data for scientific research purposes are threatened and are not clearly defined. In this respect, *Pormeister* asserts that even the title of Article 89 is somewhat misleading, because it refers to both safeguards and derogations relating to the processing of personal data under the research exemption, but

> *"a closer look will reveal that the referred article is more about derogations, and less about safeguards"*.[54]

It is worth noting that corresponding article of the draft Regulation of 2012 provided for more stringent conditions for research and relied on a rigorous rule – *"data subject's consent or anonymisation"*.[55]

Another important aspect refers to the definition of "scientific research" under the GDPR. In this respect, Recital 159 stipulates that

---

[53] In this regard, *Pormeister* claims that wide discretionary powers of member states to provide derogations from a number of data protection rights lead to significant differences between national laws concerning genetic research and, thus, threaten the interests of both data subjects and researchers. Pormeister, K. (2018) Genetic research and applicable law: the intra-EU conflict of laws as a regulatory challenge to cross-border genetic research. *Journal of Law and the Biosciences*, 5 (3), pp. 706–723.

[54] Pormeister, K. (2017) Genetic data and the research exemption: is the GDPR going too far? *International Data Privacy Law*, 7 (2), p. 140.

> *"the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research"*.

The references to the public interest are omitted in a number of provisions providing the research exemption. This makes it possible to apply it to nearly all research, including the one conducted solely for commercial purposes.

It should be noted that when drafting the GDPR, various stakeholders drew attention to this issue. In particular, Recital 126 of the Position of the European Parliament of 2014 with a view to the adoption of the GDPR (that corresponds to Recital 159 of the GDPR) contained the following wording:

> *"The processing of personal data for historical, statistical and scientific research purposes should not result in personal data being processed for other purposes, unless with the consent of the data subject or on the basis of Union or Member State law"*.[56]

The Position paper on the GDPR of the Biobanking and BioMolecular resources Research Infrastructure – European Research Infrastructure Consortium stresses the need for a clear distinction between research in the public interest and commercially oriented research and applying the exemption only to the first one.[57] With respect to this matter, *Pormeister* refers to the Estonian legislation on personal data protection, under which scientific research

---

[55] European Commission. (2012) *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM/2012/011 final – 2012/0011 (COD), 25 January, Article 83. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN [Accessed 9 March 2020].

[56] European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union* (2017/C-378/399) 9 November. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014AP0212&from=EN [Accessed 7 March 2020].

[57] BBMRI-ERIC (Biobanking and BioMolecular resources Research Infrastructure – European Research Infrastructure Consortium). (2015) *Position Paper on the General Data Protection* Regulation, p. 8. [online] Available from: https://www.bbmri-eric.eu/wp-content/uploads/BBMRI-ERIC-Position-Paper-General-Data-Protection-Regulation-October-2015_rev1_title.pdf [Accessed 9 March 2020]. See also: Shabani, M. and Borry, P. (2018) Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation. *European Journal of Human Genetics*, 26 (2), p. 153.

means only the one carried out by research and development institutions excluding privately founded companies.[58]

On the other hand, it cannot be argued that the research exemption established by the GDPR is completely unfounded. It is usually justified by the arguments arising from the peculiarities of scientific inquiry in the fields of genetics and bioinformatics. This refers, for example, to the requirement for the publication of genetic data together with genetic research findings in order to allow other scientists to verify the results and to download the data for their own further research, as well as to the impossibility of determining ahead of time the exact purpose of genetic data processing or the duration of the research. At the same time, the data minimisation principle is considered to be scarcely compatible with genetic studies, because, as pointed out by *Quinn and Quinn*, in order to achieve the required result scientists often need *"the entire haystack to find the needle"*.[59] In most cases, it is difficult to obtain the informed consent of all data subjects whose genetic data are used by research institutions, taking into account, *inter alia*, the unfeasibility of identifying all those who have undergone genetic testing and the fact that the direct identifiers associated with the persons involved have been removed.[60] In their privacy policy statements, companies that process large amounts of genetic data express doubts about the practical applicability of many of personal data processing rules. For instance, *23andMe* provides restrictions on such rights as the right to erasure and the right to withdraw consent. Namely, genetic data that a customer has previously provided and for which he or she has given consent to use in *23andMe's* research project cannot be removed from ongoing or completed studies that use such information.[61]

The GDPR states that the

"processing of personal data should be designed to serve mankind"

---

[58] Pormeister, K. (2017) Genetic data and the research exemption: is the GDPR going too far? *International Data Privacy Law*, 7 (2), p. 145.

[59] Quinn, P. and Quinn, L. (2018) Big genetic data and its big data protection challenges. *Computer Law & Security Review*, 34 (5), pp. 1006–1007.

[60] It is worth noting once again that this does not mean that it is impossible to identify each individual person. Thus, the existence of such "anonymised" data creates certain risks for data subjects.

[61] 23andMe. (2020) *Research Consent Document*. [online] Available from: https://www.23andme.com/about/consent [Accessed 9 March 2020]; 23andMe. (2018) *Exercising Rights Under the GDPR. Right to Erasure (Right to Be Forgotten)*. [online] Available from: https://permalinks.23andme.com/pdf/toolkit/erasure.pdf [Accessed 9 March 2020].

and that the right to the protection of personal data

> *"must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality"*.[62]

Thus, the primary aim of the GDPR is to ensure the necessary and appropriate preconditions for such balancing, taking into account, *inter alia*,

(1) the abstract weight of each principle,
(2) the intensity of interference with them, and
(3) the reliability of the empirical assumptions.[63]

Regarding the abstract weight, scientific genetic research is, of course, of special importance for society. It serves the substantial public interest and meets the legitimate expectations of society for an increase of knowledge.[64] However, the right to the protection of personal data and the right to privacy are important not only for a particular individual, but also for a society as a whole,[65] as the ensuring of these rights is an essential condition for the competitive economy, democratic governance and civic sector development. The extensive research exemption established by the GDPR and the existing safeguards for the right to the protection of personal data, which may prove to be not very strong and reliable,[66] make it look like the abstract weight of the public interest in scientific research is much greater, but it is not fully justified.

Referring to the intensity of interference, it is important to note that the implementation of an outdated principle "consent or anonymisation" would inevitably lead to a significant interference with genetic research and would greatly impede the fulfilment of the public interest. However, the current provisions of the GDPR also create the preconditions for significant interference with the right to the protection of personal data, and the situation is likely to deteriorate due to the further technological

---

[62] See Recital 4 of the GDPR.

[63] Alexy, R. (2003) On Balancing and Subsumption. A Structural Comparison. *Ratio Juris*, 16 (4), pp. 433–449.

[64] See Recital 113 of the GDPR.

[65] Taylor, M. (2012) *Genetic Data and the Law: A Critical Perspective on Privacy Protection*. Cambridge: Cambridge University Press, p. 13.

[66] Staunton, C., Slokenberga, S. and Mascalzoni, D. (2019) The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks. *European Journal of Human Genetics*, 27, pp. 1159–1167.

developments.[67] As for the reliability of the empirical assumptions, it is not uncommon, even nowadays, to find evidence of the uncontrolled accumulation of genetic data, including linking them with other categories of personal data. Given the rapid scientific and technological developments in this field[68] and the aforementioned characteristics of genetic data, the emergence of new evidence of the interference with the rights of the natural person concerning the processing of their genetic data should be expected in the near future.

5. CONCLUSIONS

The emergence of legal norms on the protection of genetic data in the EU legislation is both a natural consequence of the progress in biological and information technologies, which have caused a marked increase in the processing of such data by various companies and institutions, and an attempt to respond to human rights-related challenges. Most significant developments of the GDPR on genetic data include the clear and unambiguous assignment of such data to special categories of personal data, the introduction of a compulsory procedure of data protection impact assessment, and the settlement of the issue of pseudonymised data. Besides, it can be argued that current EU data protection legislation creates favourable conditions for genetic research and thus safeguards particular public interests.

However, the insufficient attention to the unique characteristics of genetic data distinguishing them from other categories of personal data, which are already mentioned in several authoritative international documents, can be considered as one of the main weaknesses of the GDPR. The consequence of this is the lack of specific regulation establishing a particular regime for genetic data processing appropriate to potential risks and threats in this field. A number of important aspects regarding the processing of genetic data, that over the last three decades have been repeatedly highlighted by various researchers, experts, and officials, fall outside the scope of the GDPR. This applies primarily to the comprehensive protection of genetic data and biological samples, the ensuring of rights

[67] For more on the far-reaching threats posed by big genetic data, see: Sorgner, S. L. (2017) Genetic Privacy, Big Genetic Data, and the Internet Panopticon. *Journal of Posthuman Studies*, 1 (1), pp. 87–103.

[68] Korf, B. (2013) Genomic privacy in the Information age. *Clinical Chemistry*, 59 (8), pp. 1148–1150.

of the persons related to the data subject ("secondary data subjects"), the lack of efficiency of data anonymisation and pseudonymisation, etc. The extensive research exemption together with the broadest interpretation of scientific research may lead to significant derogations from the rights of the data subject. Under such conditions, much depends on member states which can introduce further limitations regarding the processing of genetic data and on data controllers that are to take into account existing risks to the rights of natural persons and to implement appropriate genetic data protection policies. Still, it cannot substitute for legislative guarantees of the rights of data subject at the EU level.

The root of the problem is that the commonly accepted standards of conducting genetic research are in many respects incompatible with the key principles of legislation ensuring privacy and personal data protection. By adopting the GDPR, the European Union made an attempt to reconcile these contradictory principles by moving beyond the previous approach relying exclusively on the data subject's consent and data anonymisation, that is scarcely compatible with contemporary genetic research. However, this could lead to the major imbalances between various private and public interests. Due to the above, the following trend can be discerned: the control over personal information is gradually slipping away from the data subject while the impact of genetic technology on society is becoming more and more apparent.

LIST OF REFERENCES

[1] 23andMe. (2018) *Exercising Rights Under the GDPR. Right to Erasure (Right to Be Forgotten)*. [online] Available from: https://permalinks.23andme.com/pdf/toolkit/erasure.pdf [Accessed 9 March 2020].

[2] 23andMe. (2020) *Privacy Highlights*. [online] Available from: https://www.23andme.com/about/privacy [Accessed 9 March 2020].

[3] 23andMe. (2020) *Research Consent Document*. [online] Available from: https://www.23andme.com/about/consent [Accessed 9 March 2020].

[4] Alexy, R. (2003) On Balancing and Subsumption. A Structural Comparison. *Ratio Juris*, 16 (4).

[5] Article 29 Data Protection Working Party. (2004) *Working Document on Genetic Data*, 12178/03/EN WP 91, 17 March. Available from: https://ec.europa.eu/justice/article-29/

documentation/opinion-recommendation/files/2004/wp91_en.pdf [Accessed 9 March 2020].

[6] Article 29 Data Protection Working Party. (2014) *Opinion 05/2014 on Anonymisation Techniques*, 0829/14/EN WP216, 10 April. Available from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf [Accessed 9 March 2020].

[7] Article 29 Data Protection Working Party. (2017) *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, 17/EN WP 248, 4 April. Available from: http://ec.europa.eu/newsroom/document.cfm?doc_id=47711 [Accessed 9 March 2020].

[8] BBMRI-ERIC (Biobanking and BioMolecular resources Research Infrastructure — European Research Infrastructure Consortium). (2015) *Position Paper on the General Data Protection Regulation*. [online] Available from: https://www.bbmri-eric.eu/wp-content/uploads/BBMRI-ERIC-Position-Paper-General-Data-Protection-Regulation-October-2015_rev1_title.pdf [Accessed 9 March 2020].

[9] Borry, P. et al. (2018) The Challenges of the Expanded Availability of Genomic Information: An Agenda-Setting Paper. *The Journal of Community Genetics*, 9 (2).

[10] Council of Europe. (2018) *Convention 108+ (Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data)*, 21 June. Available from: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf [Accessed 7 March 2020].

[11] Council of Europe. Committee of Ministers. (1997) *Recommendation No. R (97) 5 on the Protection of Medical Data*, 30 October. Available from: https://rm.coe.int/1680505d5b [Accessed 7 March 2020].

[12] De Paor, A. (2017) The European Union and Protection of Genetic Information. In: De Paor, A. (ed.). *Genetics, Disability and the Law: Towards an EU Legal Framework*. Cambridge: Cambridge University Press (Cambridge Disability Law and Policy Series).

[13] 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) 23 November. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en [Accessed 7 March 2020].

[14] European Commission. (2012) *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and*

on the free movement of such data (General Data Protection Regulation), COM/2012/011 final – 2012/0011 (COD), 25 January. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN [Accessed 9 March 2020].

[15] European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union* (2017/C-378/399) 9 November. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014AP0212&from=EN [Accessed 7 March 2020].

[16] European Parliament. Committee on Petitions. (2019) *Petition No 0733/2018 by J.B. (Portuguese) on improving the protection of genetic data related to European Union citizens*, 15 March. Available from: https://www.europarl.europa.eu/doceo/document/PETI-CM-637225_EN.pdf [Accessed 7 March 2020].

[17] Gymrek, M. et al. (2013) Identifying personal genomes by surname inference. *Science*, 339.

[18] Korf, B. (2013) Genomic privacy in the Information age. *Clinical Chemistry*, 59 (8).

[19] Mészáros, J. and Ho, C. (2018) Big Data and Scientific Research: The Secondary Use of Personal Data under the Research Exemption in the GDPR. *Hungarian Journal of Legal Studies*, 59 (4).

[20] Mourby, M. et al. (2018) Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK. *Computer Law & Security Review*, 34 (2).

[21] MyHeritage. (2019) *MyHeritage Privacy Policy*. [online] Available from: https://www.myheritage.com/privacy-policy [Accessed 9 March 2020].

[22] Pormeister, K. (2017) Genetic data and the research exemption: is the GDPR going too far? *International Data Privacy Law*, 7 (2).

[23] Pormeister, K. (2018) Genetic research and applicable law: the intra-EU conflict of laws as a regulatory challenge to cross-border genetic research. *Journal of Law and the Biosciences*, 5 (3).

[24] Quinn, P. and Quinn, L. (2018) Big genetic data and its big data protection challenges. *Computer Law & Security Review*, 34 (5).

[25] Regalado, A. (2019) More than 26 million people have taken an at-home ancestry test. *MIT Technology Review*. [online] Available from: https://www.technologyreview.com/s/

612880/more-than-26-million-people-have-taken-an-at-home-ancestry-test/ [Accessed 7 March 2020].

[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. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN [Accessed 7 March 2020].

[27] Shabani, M. and Borry, P. (2018) Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation. *European Journal of Human Genetics*, 26 (2).

[28] Shabani, M. and Marelli, L. (2019) *Re-identifiability of genomic data and the GDPR: Assessing the re-identifiability of genomic data in light of the EU General Data Protection Regulation*. EMBO Rep, 20: e48316, 5 p. [online] Available from: https://www.embopress.org/doi/10.15252/embr.201948316 [Accessed 7 March 2020].

[29] Sorgner, S. L. (2017) Genetic Privacy, Big Genetic Data, and the Internet Panopticon. *Journal of Posthuman Studies*, 1 (1).

[30] Staunton, C., Slokenberga, S. and Mascalzoni, D. (2019) The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks. *European Journal of Human Genetics*, 27.

[31] Taylor, M. (2012) *Genetic Data and the Law: A Critical Perspective on Privacy Protection*. Cambridge: Cambridge University Press.

[32] United Nations Educational, Scientific and Cultural Organization. (2003) *International Declaration on Human Genetic Data*, SHS/BIO/04/1, 16 October. Available from: http://portal.unesco.org/en/ev.php-URL_ID=17720&URL_DO=DO_TOPIC&URL_SECTION=201.html [Accessed 9 March 2020].

DOI 10.5817/MUJLT2020-2-2

LAW APPLICABLE TO LIABILITY FOR DAMAGES DUE TO TRAFFIC ACCIDENTS INVOLVING AUTONOMOUS VEHICLES

by

MAREK SWIERCZYNSKI[*], ŁUKASZ ŻARNOWIEC[**]

The authors examine the problem of the law applicable to liability for damages due to traffic accidents involving autonomous vehicles. Existing conflict-of-laws regulation adopted in the Rome II Regulation and both Hague Conventions of 1971 and 1973 is criticized. Upon examination of these legal instruments, it becomes clear that existing regulation is very complex and complicated. In effect authors recommend revisions to the legal framework. Proposed solutions are balanced and take into consideration both the interests of the injured persons, as well the persons claimed to be liable. New approach allows for more individual consideration of specific cases and direct to better outcome of the disputes. The findings may be useful in handling the cases related to use of algorithms of artificial intelligence in private international law.

KEY WORDS

Algorithms of Artificial Intelligence, Autonomous Vehicles, Conflict-of-laws Rules, Private International Law, Road Accidents, The Conflict of Laws

1. INTRODUCTION

Implementation of artificial intelligence algorithms into transport has a direct impact on the civil liability regime. High mobility of autonomous vehicles, different places of manufacturing, purchase and injury due

[*] m.swierczynski@uksw.edu.pl, Professor of Law at the Department of Civil Law and Private International Law of the Faculty of Law and Administration of the Cardinal Stefan Wyszyński University in Warsaw, Poland.

[**] l.zarnowiec@uksw.edu.pl, Professor of Law at the Department of Civil Law and Private International Law of the Faculty of Law and Administration of the Cardinal Stefan Wyszyński University in Warsaw, Poland.

to traffic accidents means that complex transnational torts scenarios are more probable. It is expected that autonomous vehicles will increase road safety.[1] Currently, approx. 90 % of traffic accidents are caused by human errors.[2] However, road accidents are unavoidable. Moreover, artificial intelligence algorithms controlling autonomous vehicles have to "make decisions" about the life and health of traffic participants in critical moments. The decision process can take place with or without the human intervention.[3] The degree of vehicles autonomy may vary. There are vehicles allowing the driver to take control of the car or equipped with artificial intelligence systems that only assist the driver.[4]

In order to determine who is liable for damages, it is necessary to take into account the technology used, including the degree of autonomy of the implemented algorithm and its impact on the occurrence of the traffic accident.[5] The allocation of liability depends on the circumstances of the individual case. It may involve the liability of the driver, the owner of the vehicle, but also of the manufacturer, parts manufacturer, importer, distributor, vehicle seller, software developer, transport provider or internet service provider.[6] Uncertainty exists as regards the allocation of responsibilities between different economic operators. Each case must be settled under applicable, national legal system (the applicable law). Depending on the person claimed to be liable the governing law is to be determined on the basis of different conflict-of-laws rules. Court may need

---

1 Michałowska, M. and Ogłoziński, M. (2017) *Smart Solutions in Today's Transport: 17th International Conference on Transport Systems Telematics*, TST 2017, Katowice – Ustroń, Poland, April 5–8, 2017, pp. 191–202.

2 Data based on the European Commission's report 'Saving lives: making cars safer in the EU' (COM(2016) 0787 final).

3 Cassart, A. (2017) Aéronefs sans pilote, voitures sans conducteur: la destination plus importante que le voyage. In: H. Jacquemin, A. De Streel (eds.). *L'intelligence artificielle et le droit.* Bruxelles, p. 319. As for the scope of decision autonomy of artificial intelligence, cf. Nevejans, N. (2017) *Traité de droit et d'éthique de la robotique civile.* Bordeaux, pp. 134–137.

4 Stone, P. et al. (2016) *Artificial Intelligence and Life in 2030. One Hundred Year Study on Artificial Intelligence: Report of the 2015–2016 Study Panel*, Stanford University, September 2016. [online] Available from: https://ai100.stanford.edu/sites/default/files/ai100report10032016fnl_singlep.pdf, p. 19 [Accessed 15 March 2020]. AI technologies may present new safety risks for users when they are embedded in products and services. For example, as result of a flaw in the object recognition technology, an autonomous car can wrongly identify an object on the road and cause an accident involving injuries and material damage [White paper on Artificial Intelligence – A European approach to excellence and trust, Brussels, 19.2.2020 COM(2020) 65 final (hereinafter referred to as „White Paper AI"), p. 12].

5 Gurney, J. (2013) Sue my car not me: Products liability and accidents involving autonomous vehicles. *University of Illinois Journal of Law, Technology and Policy*, 2, pp. 247–277; Marchand, G. and Lindor, R. (2012) The coming collision between autonomous vehicles and the liability system. *Santa Clara Law Review*, 52, pp. 1321–1340.

6 Gurney, J. (2013) Op. cit., pp. 258–266.

to apply not only the specific rules on traffic accidents but also conflict-of--laws rules on product liability or even general conflict-of-laws rules on torts/delicts.

There is an apparent connection between the general topic of this paper (conflict-of-laws) and the specific topic (autonomous vehicles). The connection is apparent in particular with regard to party autonomy, choice of law and how questions of liability can be solved in the context of autonomous vehicles. These issues are closely related to the different types of autonomous vehicles. As long as algorithms implemented in the vehicles act as simple executors of human will, one should establish a normative attribution to the human being in question. For the cases in which the autonomous vehicles exceed this dependency, no clear answer on the applicable law may be found in the existing conflict-of-laws regulation. The applicability of the current conflict-of-laws regulations needs therefore to be explained, taking into consideration the legislator's intention behind the respective rules.

Currently, determination of the law applicable to traffic accidents is highly problematic. In most European countries the governing law is to be determined on the basis of the *Convention on the law applicable to traffic accidents*, which dates back to the 1970s. The law of the place of accident is used as the basic connecting factor between the accident and the applicable law. However, there are exceptions to this main rule. An alternative is the applicability of the law of the country of registration of the vehicle. The question arises as to whether, with regard to the accidents involving autonomous vehicles, this solution is satisfactory. The current conflict-of--laws regulation seems to be excessively complex in case of traffic accidents.[7] That is why, clear and understandable conflict-of-laws rules protecting the injured persons are needed.[8]

In this paper we are going to answer the following research questions. Firstly, whether the existing conflict-of-laws regulation is adapted to the liability arising from the damages due to traffic accidents involving autonomous vehicle. Secondly, in case such rules are relevant, whether the result they produce is satisfactory and, in particular, does their application takes into account the protection of the injured party. Thirdly,

[7] Klyta, W. (2015) In: M. Pazdan (ed.). *System Prawa Prywatnego. Prawo prywatne międzynarodowe.* Warszawa, p. 883.

[8] Brożek, B. (2017) The Troublesome 'Person'. In: V. Kurki and T. Pietrzykowski (eds.). *Legal Personhood: Animals, Artificial Intelligence and the Unborn.* Cham, pp. 3–13.

what are the possible solutions and how the existing conflict-of-laws regulation could be changed.

2. LACK OF FULL HARMONISATION OF THE CONFLICT--OF-LAWS RULES ON TRAFFIC ACCIDENTS

The basic legal act in the EU on the applicable law to the non-contractual liability, which is the *Regulation (EC) No 864/2007 of the European Parliament and of the Council (Rome II)* does not provide complete set of conflict-of-laws rules. Among other exclusions and derogations, the Rome II Regulation provides in its Article 28 that international conventions may prevail and different set of conflict-of-laws rules can be applied by the court of the member state.[9] This is the case of both the *1971 Hague Convention on the Law Applicable to Traffic Accidents*[10] and the *1973 Hague Convention on Dangerous Product Liability*, which contain special conflict-of-laws rules applicable for damages due by traffic accidents involving autonomous vehicles. As we see, Article 28 of the Rome II Regulation allows for the coexistence of different sets of conflict-of-laws rules.

In result, different substantive laws may apply in cases relating to liability for damage caused by traffic accidents involving autonomous vehicles depending on the adjudicating court of a member state. That alone problem calls the need of unification and simplification of the system for determining the law applicable to traffic accidents. Such change would increase legal certainty and reduce the possibility of *forum shopping*,[11] which is a strategy of referring a case to a court of a particular country in order to apply a law more favourable to the claimant.[12] Under the current divergent and non-uniformed rules the proceedings can be costly and time-

[9] Nagy, C. (2010) The Rome II Regulation and Traffic Accidents: Uniform Conflict Rules with some Room for forum shopping – how so?. *Journal of Private International Law (Clunet)*, 6 (1), p. 93.

[10] Graziano, T. (2016) *Cross-border Traffic Accidents in the EU – the Potential Impact of Driverless Cars, European Parliament – Directorate-General for Internal Policies of the Union*. Brussels.

[11] On the risk of *forum shopping* under the Rome II Regulation due to the existence in some EU Member States of the 1971 and 1973 Hague Conventions, cf. Von Hein, J. (2009) Of Older Siblings and Distant Cousins: The Contribution of the Rome II Regulation to the Communitarisation of Private International Law. *Rabels Zeitschrift für ausländisches und internationales Privatrecht*, 73, p. 474; Unberath, H. and Cziupka, J. (2011) In: T. Rauscher (ed.). *Europäisches Zivilprozess- und Kollisionsrecht EuZPR/EuIPR Kommentar.* München, p. 749.

[12] On the definition of *forum shopping* see: point 96 of the Opinion of advocate general *Leger* delivered on 8 December 2005 in the case C-539/03 Roche Nederland BV, Roche Diagnostic Systems Inc., NV Roche SA, Hoffmann-La Roche AG, Produits Roche SA, Roche Products Ltd, F. Hoffmann-La Roche AG, Hoffmann-La Roche Wien GmbH, Roche AB v. Frederick Primus, Milton Goldenberg, ECLI:EU:C:2005:749.

-consuming for the injured party claiming damages. The mains questions involve the following issues:

1) how to identify the exact cause of the accident,
2) how to provide evidence of that cause and, consequently, and
3) how to decide against whom to pursue a claim for compensation? Is it the owner of the car or its insurer or the manufacturer of the car or its parts? Or, in case of the algorithms, the defendant should be an internet service provider?

The need for unification and simplification of the conflict-of-laws rules does not require that the injured party must be treated in favoured way. Legal framework of conflict-of-laws rules should be balanced and take into account also the legitimate interests of the person claimed to be liable. This argument is particularly relevant where the likelihood of liability is directly linked to the innovation. Making a producer solely liable for the damages would discourage innovation.

Where the law of another EU member state is designated, the network created by *Council Decision 2001/470/EC* of 28 May 2001 establishing a *European Judicial Network* in civil and commercial matters,[13] plays a part in assisting courts of the member states with regard to the content of foreign law.

3. THE CONFLICT-OF-LAWS REGULATION OF THE 1971 HAGUE CONVENTION

Number of European countries are members to the *Hague Convention of 4 May 1971 on the law applicable to traffic accidents*.[14] In accordance with the principle of universality, the Convention applies even where

[13] OJ L 174, 27.6.2001, p. 25. To guarantee access to appropriate, good-quality information, the Commission regularly updates it in the Internet-based public information system set up by Council Decision 2001/470/EC. See Report from the Commission to the Council, the European Parliament and the European Economic and Social Committee of 16 May 2006 on the application of Council Decision 2001/470/EC establishing a European Judicial Network in civil and commercial matters [COM(2006) 203 final – Not published in the Official Journal]. However, the available information is not always adequate and up to date and the website only contains information about EU legal systems while the Rome II Regulation may require judges to apply the law of a third State.

[14] As of 28 December 2018, the Convention is in force in 21 States, i.e. the United States of America and the United States of America: Austria, Belarus, Belgium, Bosnia and Herzegovina, Croatia, The Czech Republic, Macedonia, France, Latvia, Lithuania, Luxembourg, Montenegro, Morocco, The Netherlands, Poland, Serbia, Slovakia, Slovenia, Spain, Switzerland, Ukraine, data available at the website: https://www.hcch.net/en/instruments/conventions/status-table/?cid=81=81 [Accessed 15 March 2020].

the applicable law is not that of the State Party to the Convention, irrespective of whether the condition of conflict of laws reciprocity has been satisfied [Article 11(2)]. In the context of autonomous vehicles, it is important to underline that the Convention does not apply to the liability of manufacturers, dealers and repairers of vehicles [Article 2(1)]. These exclusion should be understood broadly and include manufacturers, sellers and repairers of components.[15] It is, however, difficult to justify why the Convention should not be applied to car manufacturers and at the same time be applicable to the manufacturers of their parts. Still, on the basis of such exclusion, we are of opinion that it includes components based on algorithms that had been used to control the autonomous functions of the vehicle or used in the cars software.

Traffic accident within the meaning of the Hague Convention means an accident involving one or more power-driven or non-powered vehicles involving traffic on a public road, in an area open to the public or in private property accessible to certain persons (Article 1, Sentence 2). The very concept of accident, although essential for determining the scope of the Convention and for determining the applicable law on the basis of the Convention, is not defined by the provisions of the Convention. It may be understood as a sudden external event involving one or more vehicles and leading to personal injury or damage to property.

In principle, the law applicable to non-contractual civil liability in the event of a road traffic accident is, under the provisions of the Hague Convention, the law of the State in which the accident occurs (Article 3). However, Article 4 of the Convention provides many derogations from this general rule.

Although the Convention does not explicitly address the question of the choice of the law by the parties, such solution (based on the freedom of will of the parties) seems to be accepted by many authors,[16] and confirmed in the courts.[17] The law chosen by the parties has priority and

[15] Klyta, W. (2015) Op. cit., p. 891.

[16] Hoyer, H. (1991) Haager Straβenverkehrsübereinkommen und Rechtswahl der Parteien, *Zeitschrift für Rechtsvergleichung*, p. 341; Kegel, G. (2000) In: G. Kegel and K. Schurig (eds.). *Internationales Privatrecht.* München, p. 645; Halfmeier, A. and Sonder, N. (2011) In: G. Calliess (ed.). *Rome Regulations: Commentary on the European Rules of the Conflict of Laws.* Alphen aan den Rijn, p. 642; Ofner, H. (2011) Die Rom II – Verordnung – Neues Internationales Privatrecht für auβervertragliche Schuldverhältnisse in der Europäischen Union. *Zeitschrift für Rechtsvergleichung*, 1, p. 22.

exclude the application of the conflict-of-laws rules of the Conventions that are based on the objective connecting factors.[18]

4. COMPARISON OF 1973 HAGUE CONVENTION AND ROME II REGULATION

Due to the exclusion contained in the Article 2(1) of the *Hague Convention of 4 May 1971*, conflict-of-laws rules relevant to product liability are of particular importance when it comes to the liability of participants in the production and distribution chain of autonomous vehicles. Approaches for determination of the law applicable to product liability varies between EU Member States. Depending on the adjudicating court, different national law may be regarded as the governing law in the case under the same circumstances. Such negative effects of *forum shopping* are not fully eliminated by the ongoing unification of substantive law within the EU. The liability for damage caused by product, including autonomous vehicle, has been only partially harmonised under the *Directive 85/374/EEC*.[19] Moreover, the Directive does not regulate liability for damage caused by an intangible product (e.g. computer software).

In some member states,[20] the *Hague Convention of 2 October 1973 on the law applicable to product liability* is to be applied. The conflict-of-laws regulation adopted in this Convention is very complex. As a result, few States have signed the Convention and even fewer have ratified it.[21] The conflict-of-laws rules contained therein are not based on a single connecting factor, but on group of connecting factors jointly determining the applicable legal system.

---

[17] OGH, the ruling of 26 January 1995 2 Ob. 11/94. Available from: https://www.rip.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJT_19950126_OGH0002_0020OB00011_9400000_000 [Accessed 15 March 2020].

[18] The practical significance of this type of choice in relation to road accidents is explained by Graziano, T. (2016) Op. cit., p. 27 and Von Hein, J. (2009) Op. cit., p. 170.

[19] Under the *Product Liability Directive*, a manufacturer is liable for damage caused by a defective product. However, in the case of an AI based system such as autonomous cars, it may be difficult to prove that there is a defect in the product, the damage that has occurred and the causal link between the two. In addition, there is some uncertainty about how and to what extent the *Product Liability Directive* applies in the case of certain types of defects, for example if these result from weaknesses in the cybersecurity of the product (see White Paper AI, p. 13).

[20] These are Croatia, Finland, France, Luxembourg, The Netherlands, Slovenia, Spain – as of 27 December 2018, according to the data available on the website of the *Hague Conference on Private International Law* – http://www.hcch.net/index_en.php?act=conventionp.status&cid=84 [Accessed 15 March 2020].

[21] The status of the Convention is available from: https://www.hcch.net/en/instruments/conventions/status-table/?cid=84 [Accessed 15 March 2020].

The Convention does not explicitly address the question of the choice of the law made by the parties. Such solution is nevertheless accepted by some authors.[22]

In the member states that have not acceded to the 1973 Hague Convention, the determination of the law applicable to the assessment of product liability is made on the basis of the Rome II Regulation.

What is important in case of autonomous vehicles is that the conflict-of--law rules system set out in the Rome II Regulation covers not only non--contractual obligations based on principle of guilt but also such arising out of strict liability and that the law applicable also govern the question of the capacity to incur liability in tort (delict).

Primarily, the parties are allowed to choose the applicable law (Article 14).[23] Rome II Regulation introduced the principle of party autonomy and allows parties to choose applicable law, provided that certain conditions are met. The aim of this solution is to enhance legal certainty. So far courts of the member states' practice shows that the parties (even professional entrepreneurs) rarely apply this solution. Nevertheless, it has many benefits,[24] such as certainty of the parties that a given law will be the governing law for the dispute, which enables foreseeing the result of the dispute, and that the choice of *legi fori* (i.e. Czech law if the matter is seized by Czech courts) facilitates and accelerates judicial proceedings.

Article 14 para. 1 point (a) of the Rome II Regulation allows the parties to enter into agreement submitting the non-contractual obligations to the law of their choice, provided that such agreement is entered into after the event giving rise to the damage occurred (so called subsequent choice of law). This condition has its aim at protection of weaker parties (typically the injured ones).[25] Additionally, Article 14 para. 1 point (b) of the Regulation allows the parties pursuing a commercial activity, to enter

[22] Légier, G. (2007) *Le réglement Rome II sur la loi applicable aux obligations non contractuelles, JCP/La Semaine Juridique – Edition Générale*, 21 November 2007, I-207, pp. 54 and 56; Von Hein, J. (2009) Europäisches Internationales Deliktsrecht nach der Rom II – Verordnung. *Zeitschrift für Europäisches Privatrecht*, 1, p. 32.

[23] Żarnowiec, Ł. (2009) Prawo właściwe dla odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny w świetle przepisów rozporządzenia Rzym II. *Problemy Prawa Prywatnego Międzynarodowego*, 5, pp. 102–103.

[24] Pajor, T. (2002) *Comments on a preliminary draft proposal for a Council Regulation on the law applicable to non-contractual obligations*, pp. 4 and 12–13; Basedow, J. et al. (2003) Hamburg Group for Private International Law, Comments on the European Commission's Draft Proposal for a Council Regulation on the Law Applicable to Non–Contractual Obligations, *Rabels Zeitschrift für ausländisches und internationales Privatrecht*, 67, pp. 35–36.

[25] Czepelak, M. (2015) *Autonomia woli w prawie prywatnym międzynarodowym Unii Europejskiej*. Warszawa, p. 62.

into such agreement even before the event giving rise to the damage occurred, provided that an agreement is freely negotiated (so called prior choice of law). This second option may be useful for entrepreneurs remaining in sustainable economic relations, in particular those already bonded by mutual contractual obligations and further want to enhance their confidence and trust.[26] The choice may be explicit or implicit, provided that it is expressed or demonstrated with reasonable certainty by the circumstances of the case. Where establishing the existence of the agreement, the court has to respect the intentions of the parties. It may not prejudice the rights of third parties (Article 14 para. 1 sentence 2).

It is beyond doubt that this solution enhances legal certainty particularly in case of new technologies, such as autonomous cars as the entities pursuing commercial activity – by the reasonable choice of law – may exclude the applicability of an unknown foreign law. The above-mentioned rule enables, therefore, the introduction of a specific choice-of-law clause into a contract. Such a clause may cover not only contractual obligations, but also non-contractual obligations, in particular those arising from torts, which may occur between the parties in connection to the execution of the contract (i.e. on the rental of the autonomous vehicle). It enables the uniform application of the chosen law, both with regard to contractual and non-contractual obligations.

Similarly as in case of contractual obligations, where all the elements relevant to the situation at the time when the event giving rise to the damage occurs are located in a country other than the country whose law has been chosen, the choice of the parties shall not prejudice the application of provisions of the law of that other country which cannot be derogated from by agreement (Art. 14 para. 2 of the Rome II Regulation). An example would be national mandatory safety rules on the autonomous vehicles. This means that such "choice of law" is not full in a meaning that its effects in a material indication of a legal regulation of chosen law only and may not exclude applicability of mandatory rules of the law of such other country.

Secondly, Article 5 of the Rome II Regulation provides set of conflict-of--laws rules for the product liability.[27] Such solution is justified by two reasons. The first is the need to strike a balance between the need for

[26] Pazdan, M. (2017) *Prawo prywatne międzynarodowe*. Warszawa, p. 199.

adequate protection of victims and the legitimate interest of entities claimed to be liable.[28] The second reason is the elimination of accidental and surprising conflict-of-laws solutions.[29]

However, the scope of the conflict-of-laws rules contained in Article 5 is not fully clear. Most importantly, it is due to the lack of a definition of a "product". This has led to a discrepancy in the interpretations of these provisions. Some authors propose that the definition of the product from Article 2 of the *Product Liability Directive 85/374/EEC* should be used.[30] This means that the "product" is only a physical, movable item. This interpretation leads to the exclusion of non-material products, including any digital content, such as software based on algorithms. However, in view of the objectives of the Regulation as well as the recital 11 of its preamble, it seems more justifiable to give the concept of a "product" an autonomous meaning.[31] This approach make it possible to avoid unnecessary restriction and, consequently, allow to include all kinds of tangible and intangible, movable and immovable products capable of being traded,[32] including digital content and algorithms.

Nor does it seem appropriate to limit the scope of the conflict-of-laws rules of Article 5 of the Regulation to liability solely for damage caused by the *defective* product.[33] These rules specifically do not use the term of *"the defective"* product.[34] They refer to damage caused by a product which

---

[27] The creation of numerous exceptions to the general rule determining the law applicable to tort/delict obligations has been criticised in the literature – see Koziol, H. and Thiede, T. (2007) Kritische Bemerkungen zum derzeitigen Stand des Entwurfs einer Rom II – Verordnung. *Zeitschrift für vergleichende Rechtswissenschaft*, 106, pp. 235–247. Concerning the history of the work on this legal norm Heiderhoff, B. (2005) Eine europäische Kollisionsnorm für die Produkthaftung: Gedanken zur Rom II – Verordnung. *Zeitschrift für das Privatrecht der Europäischen Union*, 2, pp. 92–97.

[28] Basedow, J. et al. (2003) Op. cit., p. 15.

[29] Żarnowiec, Ł. (2009) Op. cit., p. 776.

[30] Stone, P. (2007) The Rome II Regulation On Choice Of Law In Tort. *Ankara Law Review*, 2, p. 118; Stone, P. (2009) Product Liability under the Rome II Regulation. In: J. Ahern, W. Binchy (eds.). *The Rome II*, p. 181; Huber, P. and Illmer, M. (2007) International Product Liability. A Commentary on Article 5 of The Rome II Regulation. *Yearbook of Private International Law*, 9, pp. 37–38; Von Hein, J. (2009) Op. cit., p. 26.

[31] Jagielska, M. (2005) Prawo właściwe dla odpowiedzialności za produkt – rozważania na tle projektu rozporządzenia WE o prawie właściwym dla zobowiązań pozaumownych. In: L. Ogiegło, W. Popiołek, M. Szpunar (eds.). *Rozprawy prawnicze*. Księga pamiątkowa Profesora Maksymiliana Pazdana, Kraków, p. 119.

[32] Plender, R. and Wilderspin, M. (2009) *The European Private International Law*. Oxford, p. 551.

[33] Illmer, M. (2009) The New European Private International Law of Product Liability – Steering Through Troubled Waters. *Rabels Zeitschrift für ausländisches und internationales Privatrecht*, 73, pp. 281–282.

[34] Dickinson, A. (2008) *The Rome II Regulation: The law applicable to non-contractual obligations*. Oxford, p. 370.

is not so much defective as dangerous, and that danger may be a natural characteristic of the category of product concerned, such as autonomous vehicle or its part, and not necessarily a result of its defect.

The conflict-of-laws rule expressed in Article 5 takes into account, on the one hand, the demand to protect the legitimate expectations of the injured party and, on the other hand, protects the interests of the liable entity (e.g. producer of autonomous vehicle).[35] The law that has priority is the law of habitual residence of the injured party at the time of the occurrence of the damage. This is the legal system of the country in which his personal interests are concentrated and with which the injured party is best acquainted. However, in the case of any of the solutions provided for in Article 5(1)(1)(a) to (c), the interests of the potentially liable party are also adequately protected.

In addition, an escape rule based on a much closer link provided by Article 5(2) may also apply. In practice, it is the case where special relationship between the party held liable and the first purchaser of the product exists. However, any automatism in application of such escape rule by the court should be avoided, and must be always based on an in-depth assessment of the circumstances of the individual accident.[36]

The Rome II Regulation is to applied by courts of the member states in universal way, which means that law determined as applicable under the Regulation must be applied whether or not it is the law of any EU member state. Also application of *renvoi* is excluded by Article 24 of Rome II Regulation. Such approach significantly decreases *forum shopping* risk.[37] Additionally, the Rome II Regulation, must be also applied irrespective of the nature of the court or tribunal seised. This means, among others, that criminal courts of the member states adjudicating non-contractual liability aspects related to crimes are obliged to determine applicable law on the basis of this Regulation.

5. RECOMMENDATIONS

As it follows from the above analysis existing conflict-of-laws regulation for the determination of the law applicable to the damages caused by traffic

[35] Comp. Hibbert, M. (2007) New EU choice of law rules for tort and product liability claims finalised. *European Product Liability Review*, 9, pp. 12–14.

[36] Żarnowiec, Ł. (2009) Op. cit., p. 784.

[37] Pazdan, M. (2017) Op. cit., p. 747.

accident involving an autonomous vehicle is complicated and complex. It creates a risk of *forum shopping* and, in addition, makes the legal situation of the injured party more difficult. We therefore recommend change of the conflict-of-laws regulation for accidents involving autonomous vehicles in order to harmonise and simplify the procedure for determination of the applicable law. Injured parties need to enjoy the same level of protection as persons having suffered harm caused by other technologies. At the same time technological innovation should be allowed to continue to develop.[38]

One of the possible solutions is to introduce additional conflict-of-laws rules on traffic accidents into the Rome II Regulation that will be based on the 1971 Hague Convention (this would mean assimilation of the Convention into a Regulation). In result the uniform method of determining the applicable law in all the member states participating in the Regulation could be applied by the courts of the member states, irrespective of whether or not the court state is party to the Hague Convention. Such solution partially eliminates the risk of *forum shopping*, leading to the application of the same law regardless of the location of the adjudicating court. At the same time, this means that practical problems encountered in the application of the Hague Convention would be mirrored in the Rome II Regulation. That is why this solution is not optimal and should not be recommended.[39]

The issue of road accidents involving autonomous vehicles does not, in our opinion, justify a fundamental change of the method of the applicable law determination, such as applying the new method based on favouring the injured party.[40] An example would be to split the tort statute (the applicable law) in such a way that the issues of the type of damage covered and the method of calculating compensation are governed by the law of the country of the injured party habitual residence.[41] This solution is not acceptable.[42] The person claimed to be liable should not be forced to take into account the potential application of different foreign

[38] White Paper AI, p. 15.

[39] Pazdan, M. et al. (2013) W odpowiedzi na ankietę skierowaną do państw członkowskich Unii, dotyczącą stosowania Rozporządzenia nr 864/2007 o prawie właściwym dla zobowiązań pozaumownych (Rzym II). *Problemy Prawa Prywatnego Międzynarodowego*, 12, p. 171.

[40] As in the case of the weaker party, e.g. consumers in private international law – cf. Jacquemin, H. and Hubin, J.-B. (2017) *Aspects contractuels et de responsabilité civile en matière d'intelligence artificielle*. Bruxelles, pp. 89–93.

laws.[43] In the case of autonomous vehicles, this argument becomes even more relevant as the person responsible for the damage does not necessarily have to be the vehicle driver.

It is therefore justified to preserve the general application of the law of the place where the direct damage occurred (the place of the accident). This constitutes a compromise for both the person to be liable and the injured party, who cannot count on application of the law of the country of his or her habitual residence.[44] In addition, it results in application of the same law to assess the liability of different entities potentially liable for the accident involving autonomous car, irrespective of their qualification as a driver, the owner of the vehicle, the transport provider or internet service provider. In the case of the multiple liability of several persons this would be a significant facilitation not only for the injured party, but also in the event of recourse claim between co-debtors.

The question is how to implement this legal framework to existing legislation. In our view, the general provisions of the Rome II Regulation and in particular its Article 4, should be used as the main legal basis. One should agree that the 1971 Hague Convention is an act of inferior quality to the Rome II Regulation.[45] It's outdated and complicated. It unjustifiably recognises the importance of the place of registration of a vehicle, which is a substitute for the habitual residence of the driver, owner or driver of the vehicle, thereby protecting only the interests of the driver, owner or driver of the vehicle and their insurer. There is no justification for subjecting the type of damage and its assessment to the law favourable to the person claimed to be liable. The priority in all the member states should be given to the provisions of the Rome II Regulation over those of the Convention, at least for those cases when both the injured party and

---

[41] Such a solution was proposed at the first reading of the draft Rome II regulation in the Parliament, but due to opposition from the Commission and the Council it was not included in the finally adopted text – Symonides. P. (2008) Rome II and Tort Conflicts: A Missed Opportunity. *American Journal of Comparative Law*, p. 205; Von Hein, J. (2009) Op. cit., pp. 155 and 160.

[42] Critical of such a solution: Unberath, H. and Cziupka, J. (2011) In: T. Rauscher (ed.). *Europäisches Zivilprozess- und Kollisionsrecht EuZPR/EuIPR Kommentar.* München, p. 741.

[43] Pazdan, M. et al. (2011) Op. cit., p. 171.

[44] Ibid.

[45] Staudinger, A. and Czaplinski, P. (2009) Verkehrsopferschutz im Lichte der Rom I-, Rom II- sowie Brüssel I-Verordnung. *Neue Juristische Wochenschrift*, 3, p. 2254.

the person held liable were, at the time of the accident, habitually resident in any of the member states.[46]

For both legal instruments, that is the Regulation and the Convention, the basic rule is practically the same, which means that the method for determining the applicable law would remain the same. Under the 1971 Hague Convention (Article 3) the law of the place of the accident is applicable. According to the Rome II Regulation, the governing law is the law of the place of direct damage [Article 4(1)].[47] For both these legal instruments, the *ex-post* choice of law is allowed (although such solution is not explicitly provided by the wording of the Convention).[48] It is worth recalling that the conflict-of-laws rules of the Rome II Regulation are also applicable in matters excluded from the scope of the 1971 Hague Convention.

The main difference would concern the situation when the injured party and the person claimed to be liable have their habitual residence in the same member state. In such case, the Rome II Regulation leads to the application of the law of the country of habitual residence of the parties to the dispute [Article 4(2)].[49] This is a significant advantage of the Rome II Regulation over the 1971 Hague Convention.[50] Furthermore, the Rome II Regulation allows the courts to use, where appropriate, the escape rule [Article 4(3)], without giving any significance to the connecting factor of the place of registration of the vehicle.[51]

Our recommended solution is therefore to give priority to the Rome II Regulation over the 1971 Hague Convention. This requires a corresponding revision to the wording of Article 28 of the Regulation.[52] One must state that it is disappointing that the opportunity offered by the review clause in Article 30 of the Regulation has not been used for this purpose so far.[53]

---

[46] Graziano, T. (2016) Op. cit., p. 31; Pazdan, M. et al. (2011) Op. cit., p. 171.

[47] As for the practical convergence resulting from the use of both connecting factors, cf. Nagy, C. (2010) Op. cit., pp. 98–99 and 102.

[48] On the benefits, cf. Mills, A. (2018) *Party Autonomy in Private International Law*. Oxford, pp. 390–454.

[49] As regards the practical relevance of this standard in relation to road traffic accidents, see Junker, A. (2008) Das internationale Privatrecht der Straβenverkehrsunfälle nach der Rom II – Verordnung, *JuristenZeitung*, 4, p. 174.

[50] Graziano, T. (2016) Op. cit., p. 27; Graziano, T. (2016) Op. cit., p. 55; Nagy, C. (2010) Op. cit., p. 107.

[51] Nagy, C. (2010) Op. cit., p. 107.

[52] Halfmeier, A. and Sonder, N. (2011) Op. cit., pp. 642–643; Nagy, C. (2010) Op. cit., p. 108.

[53] Dickinson, A. (2008) Op. cit., p. 362; Staudinger, A. and Czaplinski, P. (2009) Op. cit., p. 2254.

The following arguments can be used as the justification for such changes in correlation with the review clause in Article 30 of the Regulation. Firstly, a connection with the country where the direct damage occurred (*lex loci damni*) adopted under Article 4(1) the Rome II Regulation strikes a fair balance between the interests of the person claimed to be liable and the person sustaining the damage, and also reflects the modern approach to civil liability and the development of systems of strict liability.[54] The main argument is that, while the party claimed to be liable should be protected, the interests of the country where the damage occurred should also be taken into account. It is also justified by the expectations of the injured party. As for the perpetrator, it is argued that he should foresee the place of the result (damage) of his activities. It is also important that the place of damage can be determined with some ease. In recent *Florin Lazar* judgment rendered on 10 December 2015 (C-350/14), the ECJ observed that the uniform conflict-of-laws rules laid down in the Rome II Regulation purports to *"enhance the foreseeability of court decisions"* and to

> *"ensure a reasonable balance between the interests of the person claimed to be liable and the person who has sustained damage"*,

and that

> *"a connection with the country where the direct damage occurred* […] *strikes a fair balance between the interests of the person claimed to be liable and the person sustaining the damage"*.

In case of physical injuries caused to a person or the damage caused to goods, the country of the place where the direct damage occurs is the country of the place where the injuries were suffered or the goods were damaged. In the case of a road traffic accident, the damage is constituted by the injuries suffered by the direct victim, while the damage sustained by the close relatives of the latter must be regarded as indirect consequences of the accident. The ECJ clarified the interpretation of Article 4 para. 1 in *Florin Lazar* judgment with regard to difference between "direct damage" and an "indirect consequence" of the event, which has no bearing on the identification of the applicable law.

[54] Świerczyński, M. and Żarnowiec, Ł. (2015) In: Pazdan, M. (ed.). *System Prawa Prywatnego. Prawo prywatne międzynarodowe*. Warszawa, p. 766.

In some circumstances exclusive application of *lex loci damni* rule under Article 4 (1) would lead to excessive simplification of the process of determination of the applicable law, as it is possible that the "gravity" of a non-contractual obligation is located in a different country than the country in which the direct damage occurred. This is why Article 4 in next two paragraphs establishes two major exemptions from this the *lex loci* rule, making it less arbitrary, and the whole system more workable. Main exception to the principal rule is provided by Article 4 (2) of the Rome II Regulation. It states that where the person claimed to be liable and the person sustaining damage both have their habitual residence in the same country at the time when the damage occurs, the law of that country shall apply. This so called "common law of the parties" reflects the legitimate expectations of the two parties. Under Rome II Regulation courts of the member states should first enquiry whether the person claimed to be liable and the person sustaining damage both had their habitual residence in the same country at the time when the damage occurred, and only if the answer is negative apply law of country in which the direct damage occurred. In both cases the result of law determination can be still changed if the requirements of the "escape clause" are met.[55]

Additionally, an "escape clause" from both Article 4 (1) and (2) is provided by Article 4 para. 3 which allows a departure from both above rules. However, it must be clear from all the circumstances of the case that the tort/delict is manifestly more closely connected with a country other than that indicated in paragraphs 1 or 2, and only is such case, on the basis of this "escape clause" the law of that other country shall apply. There are several limitations preventing courts from excessive, abusive application of this "escape clause", such as requirements that tort/delict connection with such other country must be manifestly more closely connected and that this must be clear from all the circumstances of the case. A useful guideline is provided by the Regulation in the second sentence of Article 4 (3) where it is explained that a manifestly closer connection with another country might be based in particular on a pre-existing relationship between the parties, such as a contract, that is closely connected with the tort/delict in question. The escape clause, in the meaning of art. 4 para. 3, may play an essential role in practice. Courts of the member state are not allowed,

[55] Pazdan, M. (2017) Op. cit., p. 199.

however, to abuse this possibility, by, for example, refusing freedom of choice, or unjustified correction of the conflict-of-laws rules in order to obtain a particular, material aim (i.e. the realisation of the state interest related to the substantive regulation of autonomous vehicles and/or artificial intelligence). It would be incorrect to use Rome II Regulation by court of the member state just to justify application, depending on the case, of *legi fori* on different basis (e.g. *lex loci damni* rule or escape clause) whatever suits the judge better. There should be no preference of national law application and discrimination of foreign law.

In our opinion Rome II Regulation does not need to contain any conflict--of-laws rules which directly concern the obligations due to traffic accidents involving autonomous vehicles. The conflict-of-laws framework should be general, synthetic and neutral to face technological development. For this reason, courts of the member states may apply the law of a particular country with a substantial margin of appreciation. However, it does not mean that decision on the applicable law is to be left entirely to the discretion of court, which would be free to determine the national law most closely related to the relevant situation. No doubt, if accepted, such practice would raise the level of legal uncertainty, which might even endanger the safety of transport and use of autonomous vehicles.

The case is different with regard to the potential liability of the manufacturers (importers or sellers) of autonomous vehicles, their components or the digital content (software) on which they operate. In such case, the general public interest in supporting technological development and the call for fair risk-sharing should be taken into consideration. These objectives are fully met by conflict-of-laws rule on product liability laid down in Article 5 of the Rome II Regulation and general rules of its Article 4 does not need to be applied. Although it gives rise to some doubts on interpretation of Article 5, it seems that the adopted conflict-of-laws regulation is well balanced. It strikes a fair balance between the interests and risks of the innovative entrepreneur and users of such innovations, including persons potentially injured by the vehicle.

Another strong argument in favour of the application of Rome II Regulation over the Hague Conventions is that this Regulation also determines the scope of applicable law in some details. Applicable law under the Rome II Regulation covers both the source of an obligation, as well an obligation resulting from an obligation. It applies also to non-

-contractual obligations that are likely to arise [Article 2 (2)]. Pursuant to Article 15 of the Rome II Regulation the law applicable to non-contractual obligations under the Regulation governs in particular: the basis and extent of liability, including the determination of persons who may be held liable for acts performed by them; the grounds for exemption from liability, any limitation of liability and any division of liability; the existence, the nature and the assessment of damage or the remedy claimed; within the limits of powers conferred on the court by its procedural law, the measures which a court may take to prevent or terminate injury or damage or to ensure the provision of compensation; the question whether a right to claim damages or a remedy may be transferred, including by inheritance; persons entitled to compensation for damage sustained personally; liability for the acts of another person; the manner in which an obligation may be extinguished and rules of prescription and limitation, including rules relating to the commencement, interruption and suspension of a period of prescription or limitation.

The designated law also determines the persons entitled to compensation for damage they have sustained personally. It covers, among others, whether a person other than the "direct victim" may obtain compensation "by ricochet", following damage sustained by the victim. An example is psychological damage, which includes the suffering caused by the death of a close relative, or financial, sustained for example by the children or spouse of a deceased person.

In addition to the general guidelines of Article 15, the Rome II Regulation provides also several useful guidelines relating to the scope of the applicable law. The Regulation applies to non-contractual obligations in civil and commercial matters only, in situations involving a conflict of laws. It does not apply, in particular, to revenue, customs or administrative matters (Art. 1 para. 1). This exclusion needs to be absolutely reasonable as the public and civil law regulations on autonomous vehicles need to be clearly distinguished from one to another. Additionally, pursuant to Article 18 of the Rome II Regulation the person having suffered damage may bring his or her claim directly against the insurer of the person liable to provide compensation if the law applicable to the non-contractual obligation or the law applicable to the insurance contract so provides. This is so called direct action against the insurer of the person liable.

It is also worth to mention with regard to autonomous vehicles that Article 17 of the Regulation indicates that in assessing the conduct of the person claimed to be liable, account shall be taken, as a matter of fact and in so far as is appropriate, of the rules of safety and conduct which were in force at the place and time of the event giving rise to the liability (rules of safety and conduct). The term "rules of safety and conduct" should be interpreted as referring to all regulations having any relation to safety and conduct, including, for example, road safety rules in the case of an accident (see recital 34 of the Preamble of the Rome II Regulation).

The Rome II Regulation sets out also the framework for refusal of the application of a provision of the law of any country specified by the Regulation due to the public policy (*ordre public*) of the forum, provided that this exception is permitted only if application of such law is manifestly incompatible with the public policy of the *forum* (Article 26). For example, the application of a provision of the law designated by the Regulation which would have the effect of causing non--compensatory exemplary or punitive damages of an excessive nature to be awarded to the person injured by the accident involving autonomous vehicles should be treated as being contrary to the public policy (*ordre public*).

As we see there are many arguments in favour of the uniform application of the Rome II Regulation to all civil consequences resulting from the traffic accident involving autonomous vehicles. However, while endorsing the solution adopted in Article 5 of the Rome II Regulation, it is important to add that the basic objection raised against the EU conflict-of--laws regulation used for determination the law applicable to product liability is the dualism of the sources of law. Some EU member states are still bound by the 1973 Hague Convention.[56] The critical assessment of the Convention proves that a simple incorporation of its rules into the Rome II Regulation would be wrong. As in the case of the 1971 Hague Convention, a much better and simpler option seems to be to give full priority to the Rome II Regulation over the Convention. As stated above, this also requires revision to the wording of Article 28 of the Rome II Regulation.

[56] Pazdan, M. et al. (2013) Op. cit., pp. 177–178.

6. CONCLUSIONS

The following conclusions result from our analysis:

In order to determine who is liable for damages, it is necessary to take into account the technology used, including the degree of autonomy of the concerned vehicle and its impact on the occurrence of the traffic accident. The allocation of liability depends on the circumstances of the individual case.

Uncertainty exists as regards the allocation of responsibilities between different economic operators (e.g. driver, owner of the vehicle, manufacturer or service provider). Each case must be settled under applicable, national legal system (the applicable law). Depending on the person claimed to be liable the governing law is to be determined on the basis of different conflict-of-laws rules.

Court may need to apply not only the specific rules on traffic accidents but also conflict-of-laws rules on product liability (e.g. of the manufacturer of parts) or even general conflict-of-laws rules on torts/delicts.

Currently, determination of the law applicable to traffic accidents is highly problematic. The current conflict-of-laws regulation seems to be excessively complex in case of traffic accidents. This creates a risk of *forum shopping* and, in addition, makes the legal situation of the injured party more difficult.

The need for unification and simplification of the conflict-of-laws rules does not require that the injured party is to be treated in favoured way. Conflict-of-laws regulation should be balanced and take into account also the legitimate interests of the person claimed to be liable.

In this paper we recommend change of the conflict-of-laws regulation for accidents involving autonomous vehicles in order to harmonise and simplify the procedure for determination of the applicable law. Injured parties need to enjoy the same level of protection as persons having suffered harm caused by other technologies, whilst technological innovation should be allowed to continue to develop.

In this paper we also state that it is reasonable to use as a main basis the general provisions of the Rome II Regulation and in particular its Article 4. Rome II Regulation does not need to be supplemented by any special conflict-of-laws rules which would directly regulate the obligations arising from autonomous vehicles.

As to the potential liability of the manufacturers (importers or sellers) of autonomous vehicles, their components or the digital content (software) on which they operate, the conflict-of-laws rule on product liability laid down in Article 5 of the Rome II Regulation is satisfactory. It takes into account, on the one hand, the demand to protect the legitimate expectations of the injured party and, on the other hand, protects the interests of the liable entity (e.g. producer of autonomous vehicle).

LIST OF REFERENCES

[1] Basedow, J. et al. (2003) Hamburg Group for Private International Law, Comments on the European Commission's Draft Proposal for a Council Regulation on the Law Applicable to Non–Contractual Obligations. *Rabels Zeitschrift für ausländisches und internationales Privatrecht*, 67.

[2] Brożek, B. (2017) The Troublesome 'Person'. In: V. Kurki and T. Pietrzykowski (eds.). *Legal Personhood: Animals, Artificial Intelligence and the Unborn.* Cham.

[3] Cassart, A. (2017) Aéronefs sans pilote, voitures sans conducteur: la destination plus importante que le voyage. In: H. Jacquemin, A. De Streel (eds.). *L'intelligence artificielle et le droit.* Bruxelles.

[4] Czepelak, M. (2015) *Autonomia woli w prawie prywatnym międzynarodowym Unii Europejskiej*. Warszawa.

[5] Dickinson, A. (2008) *The Rome II Regulation: The law applicable to non-contractual obligations*. Oxford.

[6] European Commission's report 'Saving lives: making cars safer in the EU'. (COM(2016) 0787 final).

[7] Graziano, T. (2016) *Cross-border Traffic Accidents in the EU – the Potential Impact of Driverless Cars, European Parliament – Directorate-General for Internal Policies of the Union.* Brussels.

[8] Gurney, J. (2013) Sue my car not me: Products liability and accidents involving autonomous vehicles. *University of Illinois Journal of Law, Technology and Policy*, 2.

[9] Halfmeier, A. and Sonder, N. (2011) In: G. Calliess (ed.). *Rome Regulations: Commentary on the European Rules of the Conflict of Laws.* Alphen aan den Rijn.

[10] Heiderhoff, B. (2005) Eine europäische Kollisionsnorm für die Produkthaftung: Gedanken zur Rom II – Verordnung. *Zeitschrift für das Privatrecht der Europäischen Union*, 2.

[11] Hibbert, M. (2007) New EU choice of law rules for tort and product liability claims finalised. *European Product Liability Review*, 9.

[12] Hoyer, H. (1991) Haager Straβenverkehrsübereinkommen und Rechtswahl der Parteien. *Zeitschrift für Rechtsvergleichung.*

[13] Huber, P. and Illmer, M. (2007) International Product Liability. A Commentary on Article 5 of The Rome II Regulation. *Yearbook of Private International Law*, 9.

[14] Illmer, M. (2009) The New European Private International Law of Product Liability – Steering Through Troubled Waters. *Rabels Zeitschrift für ausländisches und internationales Privatrecht*, 73.

[15] Jacquemin, H. and Hubin, J.-B. (2017) *Aspects contractuels et de responsabilité civile en matière d'intelligence artificielle*. Bruxelles.

[16] Jagielska, M. (2005) Prawo właściwe dla odpowiedzialności za produkt – rozważania na tle projektu rozporządzenia WE o prawie właściwym dla zobowiązań pozaumownych. In: L. Ogiegło, W. Popiołek, M. Szpunar (eds.). *Rozprawy prawnicze.* Księga pamiątkowa Profesora Maksymiliana Pazdana, Kraków.

[17] Junker, A. (2008) Das internationale Privatrecht der Straβenverkehrsunfälle nach der Rom II – Verordnung. *JuristenZeitung*.

[18] Kegel, G. (2000) In: G. Kegel and K. Schurig (eds.). *Internationales Privatrecht.* München.

[19] Klyta, W. (2015) In: M. Pazdan (ed.). *System Prawa Prywatnego. Prawo prywatne międzynarodowe.* Warszawa.

[20] Koziol, H. and Thiede, T. (2007) Kritische Bemerkungen zum derzeitigen Stand des Entwurfs einer Rom II – Verordnung. *Zeitschrift für vergleichende Rechtswissenschaft*, 106.

[21] Légier, G. (2007) *Le réglement Rome II sur la loi applicable aux obligations non contractuelles, JCP/ La Semaine Juridique – Edition Générale*, 21 November 2007, I-207.

[22] Marchand, G. and Lindor, R. (2012) The coming collision between autonomous vehicles and the liability system. *Santa Clara Law Review*, 52.

[23] Michałowska, M. and Ogłoziński, M. (2017) *Smart Solutions in Today's Transport: 17th International Conference on Transport Systems Telematics*, TST 2017, Katowice – Ustroń, Poland, April 5–8, 2017.

[24] Mills, A. (2018) *Party Autonomy in Private International Law*. Oxford.

[25] Nagy, C. (2010) The Rome II Regulation and Traffic Accidents: Uniform Conflict Rules with some Room for forum shopping – how so?. *Journal of Private International Law (Clunet)*, 6 (1).

[26] Nevejans, N. (2017) *Traité de droit et d'éthique de la robotique civile.* Bordeaux.

[27] Ofner, H. (2011) Die Rom II – Verordnung – Neues Internationales Privatrecht für auβervertragliche Schuldverhältnisse in der Europäischen Union. *Zeitschrift für Europarecht, Internationales Privatrecht und Rechtsvergleichung*, 1.

[28] OGH, the ruling of 26 January 1995 2 Ob. 11/94. Available from: https://www.rip.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJT_19950126_OGH0002_0020OB00011_9400000_000 [Accessed 15 March 2020].

[29] Opinion of advocate general Leger delivered on 8 December 2005 in the case C-539/03 Roche Nederland BV, Roche Diagnostic Systems Inc., NV Roche SA, Hoffmann-La Roche AG, Produits Roche SA, Roche Products Ltd, F. Hoffmann-La Roche AG, Hoffmann-La Roche Wien GmbH, Roche AB v. Frederick Primus, Milton Goldenberg, ECLI:EU:C:2005:749.

[30] Pajor, T. (2002) Comments on a preliminary draft proposal for a Council Regulation on the law applicable to non-contractual obligations.

[31] Pazdan, M. (2017) *Prawo prywatne międzynarodowe*. Warszawa.

[32] Pazdan, M. et al. (2013) W odpowiedzi na ankietę skierowaną do państw członkowskich Unii, dotyczącą stosowania Rozporządzenia nr 864/2007 o prawie właściwym dla zobowiązań pozaumownych (Rzym II). *Problemy Prawa Prywatnego Międzynarodowego*, 12.

[33] Plender, R. and Wilderspin, M. (2009) *The European Private International Law*. Oxford.

[34] Staudinger, A. and Czaplinski, P. (2009) Verkehrsopferschutz im Lichte der Rom I-, Rom II- sowie Brüssel I-Verordnung. *Neue Juristische Wochenschrift*, 3.

[35] Stone, P. (2007) The Rome II Regulation On Choice Of Law In Tort. *Ankara Law Review*, 2.

[36] Stone, P. (2009) Product Liability under the Rome II Regulation. In: J. Ahern, W. Binchy (eds.). *The Rome II*.

[37] Stone, P. et al. (2016) *Artificial Intelligence and Life in 2030. One Hundred Year Study on Artificial Intelligence: Report of the 2015–2016 Study Panel*, Stanford University, September 2016. [online] Available from: https://ai100.stanford.edu/sites/default/files/ai100report10032016fnl_singlep.pdf [Accessed 15 March 2020].

[38] Świerczyński, M. and Żarnowiec, Ł. (2015) In: Pazdan, M. (ed.). *System Prawa Prywatnego. Prawo prywatne międzynarodowe*. Warszawa.

[39] Symonides, P. (2008) Rome II and Tort Conflicts: A Missed Opportunity. *American Journal of Comparative Law*.

[40] Unberath, H. and Cziupka, J. (2011) In: T. Rauscher (ed.). *Europäisches Zivilprozess- und Kollisionsrecht EuZPR/EuIPR Kommentar*. München.

[41] Von Hein, J. (2009) Europäisches Internationales Deliktsrecht nach der Rom II – Verordnung. *Zeitschrift für Europäisches Privatrecht*, 1.

[42] Von Hein, J. (2009) Of Older Siblings and Distant Cousins: The Contribution of the Rome II Regulation to the Communitarisation of Private International Law. *Rabels Zeitschrift für ausländisches und internationales Privatrecht*, 73.

[43] White paper on Artificial Intelligence – A European approach to excellence and trust, Brussels, 19. 2. 2020 COM(2020) 65 final.

[44] Żarnowiec, Ł. (2009) Prawo właściwe dla odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny w świetle przepisów rozporządzenia Rzym II. *Problemy Prawa Prywatnego Międzynarodowego*, 5.

DOI 10.5817/MUJLT2020-2-3

SOCIAL MEDIA ACCOUNT AS AN OBJECT OF VIRTUAL PROPERTY

by

KATERYNA NEKIT*

This article analyzes the concept of virtual property as well as the legal nature of social media accounts to explore whether these can be considered objects of property, in particular, of virtual property rights. It examines the essence of virtual property and reveals the specifics of owner's powers regarding to digital assets. It also specifies what kind of objects should be treated as digital assets. The technical and legal nature of a social media account are analyzed to reveal whether the latter can be considered as "possession" in terms of Protocol No. 1 to the Convention for the Protection of Human Rights and Fundamental Freedoms. Some legal issues regarding to the use of a social media account including the division of rights to business accounts and inheritance of social media accounts are investigated. The approaches in various countries to the problem of determination of the post-mortem fate of digital assets are analyzed, and a unified tendency to consider social media accounts as part of the estate transferred to the heir is revealed. The conclusion is drawn that the extension of the property regime to social media accounts could ensure an appropriate legal protection of users' rights.

KEY WORDS

Account, Digital Assets, Inheritance, Possession, Social Media, Users, Virtual Property

1. INTRODUCTION

The term "virtual property" has emerged in the context of attempts to identify approaches to the legal regulation of relationships associated

* katerinanekit@gmail.com, Associate Professor, Department of Civil Law, National University "Odessa Law Academy" Odessa, Ukraine.

with the so-called *Massively Multiplayer Online Games (MMOG)*, the rapid development of which no longer allowed to leave this issue aside. One of the first works to mention virtual property is a study by *E. Castronova*, who conducted a thorough economic analysis of MMOG *Norrath*. His analysis revealed striking statistics: 40,000 players were registered in the game, about 12,000 of them considered this place their permanent home; the average user of the game spent approximately 4 hours a day or more than 20 hours a week in the game; the gross domestic product of the game was estimated at USD 135 million; the value of the domestic currency in the exchange markets was approximately USD 0.0107, which exceeded the value of the yen and lira.[1]

The idea of virtual property that arose with respect to virtual items in online gaming has gradually gained a broader interpretation and extended to other types of virtual assets. Today, virtual property is considered to encompass not only in-game objects and avatars, but also domain names, URLs, eBooks, tickets, email accounts, social media accounts, websites, chats, bank accounts, cryptocurrencies and more.[2]

One of the most popular objects among listed is social media account. It is difficult to find a person who has no registration in at least one social network. The popularity of social media accounts alongside with gaps in legislative regulation of those create a huge amount of practical issues referred to the use of social media accounts. Considering not only moral, but also sometimes significant economic value of social media accounts, it is obviously necessary to provide an appropriate protection of the users' rights, preferably on the legislative level. A possible ground for such protection could be the recognition of social media accounts as a kind of virtual property, which in its turn should be qualified as a specific type of ownership.

2. THE CONCEPT AND ESSENCE OF VIRTUAL PROPERTY

According to *J. Fairfield*, virtual property is inherently a code that was designed to *"act more like land or mobility than ideas"*. Such code can be

[1] Castronova, E. (2001) Virtual worlds: a first-hand account of market and society on the Cyberian Frontier. *CESifo Working Paper Series*, 618, pp. 1–40.

[2] Fairfield, J. (2005) Virtual property. *Boston University Law Review*, 85, pp. 1047–1102. [online] Available from: https://ssrn.com/abstract=807966 [Accessed 26 April 2020]; Palka, P. (2017) *Virtual property: towards a general theory*. PhD. Florence: European University Institute, pp. 148–160.

considered virtual property if it meets three characteristics: rivalrousness, persistence, interconnectivity.[3] *Ch. Blazer* in his research proposes his own definition of virtual property. In his view, virtual property is a persistent computer code stored by a non-remote resource system, where one or more persons are empowered to control the computer code, including the removal of all other persons.[4] To the characteristics of the code that allows us to consider it as virtual property, proposed by *J. Fairfield*, *Ch. Blazer* suggests adding two more features: the presence of the secondary market and the value added by the user.[5] *Gr. Lastowka and D. Hunter*, describing virtual property in online games, view it as database records hosted on a server that allow a participant's computer monitor to display images already present within the software.[6] *DaKunha* proposes similar to *J. Fairfield's* definition of virtual property: virtual property is a software code designed to behave as if it had the qualities of the physical, belonging to the material world, movable things or parts of reality.[7]

These concepts focus on defining what should be considered as virtual property. In fact, we are talking about virtual property as an object of legal relations. However, obviously, there will be a right to this kind of property, which can be defined as a virtual property right. There is a need to study the nature and characteristics of virtual property as a special kind of right.

To determine the nature of virtual property, it is necessary to dwell on the starting points of the categories of "property" and "property right". The attention should be paid to the main point, while characterizing virtual property, that is the possibility of the existence of a right of ownership of incorporeal things.

Without claiming to be original, let us turn to Roman private law to study this issue. In the context of this study the division of things (*res*) into corporeal (*res corporales*) and incorporeal (*res incorporales*), proposed by the Romans, is of particular importance. According to *Gaius*, corporeal things are those that, by their nature, can be visible, such as earth, slave, clothing; incorporeal things are those that cannot be touched, but they exist

---

3 Op. cit., p. 1049.

4 Blazer, Ch. (2006) The five indicia of virtual property. *Pierce Law Review*, 5, p. 141.

5 Op. cit., p. 142.

6 Lastowka, G. and Hunter, D. (2004) The laws of the virtual worlds. *California Law Review*, 92 (1), p. 40.

7 DaCunha, N. (2010) Virtual property, real concerns. *Akron Intellectual Property Journal*, 4 (1), p. 42.

under the law, such as inheritance, usufruct or obligations.[8] Modern legal systems of the world to one degree or another follow this approach. Thus, in the Anglo-American legal tradition, ownership is usually interpreted quite widely. It is defined as a "bunch" or a set of rights or expectations in movable and immovable things that are protected from third parties, including the state.[9] Such rights include the right to use, own, remove third parties, and alienate things. "Things" are also interpreted quite broadly and include land rights, movable and incorporeal things.[10] An important difference of the Roman-Germanic legal tradition is the distinction between property as such and things. The concept of "thing" most often narrows and is limited only to bodily objects. For instance, the *German Civil Code (BGB)* restricts the objects of ownership only to bodily things. According to para. 90 of the Civil Code of Germany, things in terms of law are bodily objects.[11]

Despite the fact that Ukraine is a country of Roman-Germanic legal tradition, the approach enshrined in Ukrainian legislation on things is different. The Ukrainian law accepts that some incorporeal objects, such as electricity or gas, are equal to things because of their similarity to material things. The Ukrainian concept of property rights include the object of property rights that can be both corporeal and incorporeal. Thus, in accordance with Art. 316 of the Civil Code of Ukraine, the object of ownership is the thing (property). And according to Art. 190 of the Civil Code of Ukraine, property as a special object are considered a separate thing, a set of things, as well as property rights and obligations. Therefore, the concept of "thing" in Ukrainian law is widely interpreted, and includes not only objects of the material world, but also incorporeal things. Property rights and obligations are, in fact, incorporeal things, and therefore, the Ukrainian concept of ownership does not preclude the application of property rights provisions to virtual assets.

The next step in the analysis of the legal nature of virtual property is the distinction between virtual property and intellectual property, whose objects are actually property rights, that is, incorporeal things.

[8] Mousourakis, G. (2015) *Roman law and the origins of the civil law tradition*. Switzerland: Springer.

[9] Van der Walt, A. J. (2011) *Constitutional Property Law*. 3rd ed. Cape Town: Juta Law, pp. 114–115.

[10] Erlank, W. (2012) *Property in virtual worlds*. PhD. Stellenbosch: Stellenbosch University, p. 216.

[11] Op. cit., p. 222.

There is no common opinion on the correlation between virtual property rights and intellectual property rights. Since virtual property, as well as intellectual property, is intangible, it is often mixed with the latter.[12] In such case, the primary rights of the intellectual property owners and all related ones are governed by the *End User License Agreement (EULA)*. However, the result of this approach is the limitation of the virtual property owners' rights by the owners of intellectual property rights. This is why the concept of virtual property has appeared. Therefore, the idea is to make difference between intellectual and virtual property.

There are also some assumptions that intellectual property is a component of virtual property, that is, intellectual property is a separate category within virtual property. Consequently, *J. Gong* divide virtual property into four categories: avatars, domain names, virtual movables, and intellectual property.[13] However, it seems that the concept of intellectual and virtual property should not be confused, since the concept of virtual property was introduced precisely to refer to objects that do not exist in the material world but only in virtual reality.

According to *J. Fairfield*, online resources have nothing to do with intellectual property. On the contrary, these resources were designed to have the same characteristics as real movable things. This fact makes the ownership provisions an obvious source of regulation for such resources.[14] *J. Fairfield's* position has been supported in numerous follow-up studies. *Ch. Blazer* notes that the only similarity between virtual and intellectual property is that both of them relate to intangible interests, but their similarity ends there.[15]

Ch. Blazer analyzes features of virtual property in order to distinguish virtual property from intellectual property. According to *Ch. Blazer*, rivalrousness of virtual property objects make a fundamental difference between virtual and intellectual property (rivalrousness means the ability

---

[12] Hurter, E. (2009) The international domain name classification debate: are domain names "virtual property", intellectual property, property or no property at all? *The Comparative and International Law Journal of Southern Africa*, 42 (3), pp. 288–289; Nelmark, D. (2004) Virtual property: the challenges of regulating intangible, exclusionary property interests such as domain names. *Northwestern Journal of Technology and Intellectual Property*, 3, pp. 1–7; Stephens, M. (2002) Sales of in-game assets: an illustration of the continuing failure of intellectual property law to protect digital-content creators. *Texas Law Review*, 80, pp. 1513–1534.

[13] Gong, J. (2011) Defining and addressing virtual property to international treaties. *Boston University Journal of Science & Technology Law*, 17, pp. 101–107.

[14] Fairfield, J. (2005) Op. cit., p. 1046.

[15] Blazer, Ch. (2006) Op. cit., p. 140.

of an object to be controlled by only one person at a specific time – for example, by using an e-mail address, the user excludes all other persons from access to it).[16] Intellectual property is not only intangible but also uncompetitive. For example, listening to a song stored in MP3 format does not in any way limit the ability of others to listen to the same song. Restrictions on the use of intellectual property arise not from the rivalrousness of such property, but from the exclusive rights guaranteed by law. Thus, the simplest and most effective way to distinguish between virtual and intellectual property is to determine whether the property is competitive in nature or only protected by exclusive rights.[17]

Another feature of virtual property is also the distinction between virtual and intellectual property. Persistence is an attribute of traditional property that is often lacking in intangible objects. For example, a melody is persistent (stable) only as long as it sounds. A tune is protected by intellectual property rights only after it is fixed on a tangible medium, which at the same time is the subject of traditional (private) property rights. Therefore, intellectual property is characterized as intangible and unstable. On the contrary, virtual property, despite its intangibility, is persistent (permanent). For example, a user who uses the mail service may not without reasons expect that his / her e-mails will be kept for months, even if he / she only uses the account for a few minutes per day.[18]

Thus, the virtual property category was designed to protect users' rights to virtual objects. However, inevitably, there are some issues connected to the rights of providers / developers of virtual worlds, platforms and more. Therefore, an important issue is the balance of users' and providers' interests.

The positions of the researchers on this issue differ. For example, *J. Nelson* is in favour of defending virtual world developers and against granting the users virtual rights to in-game items. He points out that virtual worlds have been created by developers for years, and they put a lot of effort into their development. Granting virtual property rights to users will inevitably reduce the developer's authority over the objects they create, which is unfair.[19] In his turn, *J. Fairfield* notes that today it is no longer possible to dispense with the rights to virtual resources only for developers

[16] Fairfield, J. (2005) Op. cit., pp. 1047–1102.
[17] Blazer, Ch. (2006) Op. cit., p. 143.
[18] Op. cit., pp. 144–145.

of virtual worlds. Recently, the number of applications for theft of virtual items has increased. Thus, over 22,000 incidents of theft of virtual property were reported to South Korean police.[20] So the problem is that the developers of the virtual worlds do not have enough tools to influence the offenders. Even if the developer of the virtual world has reason to sue the offender, he or she has little incentive to file such a claim. Firstly, the operator of the virtual world does not lose anything, because there was only a transition of the virtual object from one user to another. Secondly, filing a lawsuit against a hacker can draw users' attention to the security flaws that could have their accounts compromised, and this will cause developer contractual liability. Therefore, if users do not acknowledge their virtual property rights to the items they own, they will be left without due compensation.[21]

One solution to the problem of securing the rights of both virtual world developers and users is to distinguish different levels of "ownership" within the virtual world. In this regard, *S. Abramovitch* proposes to distinguish three levels of "property" in virtual worlds. The first level is the virtual world itself, which is essentially a computer code protected by intellectual property rights. The second level are objects within the virtual world, such as avatars, swords, clothing, buildings, etc. that are analogous to real-world property objects. The third level are the in-game items, which are both intellectual property and virtual property objects. For example, a virtual book is both a physical object and its content is an intellectual property right; the designer line of clothing in the virtual world is both a physical object, but the design of these garments is protected by intellectual property right. This example can also be used to distinguish between intellectual property rights that a developer has to the object he created, content and software for the virtual world, and other rights that players may have to in-game objects embodying physical objects.[22]

---

[19] Nelson, J. W. (2010) The virtual property problem: what property rights in virtual resources might look like, how they might work, and why they are a bad idea. *McGeorge Law Review*, 41, p. 298.

[20] Ward, M. (2003) *Does Virtual Crime Need Real Justice?* BBC News.com. [online] Available from: http://news.bbc.co.uk/2/hi/technology/3138456.stm [Accessed 21 July 2020].

[21] Fairfield, J. (2005) Op. cit., p. 1081.

[22] Abramovitch, S. H. (2009) *Virtual property in virtual worlds*. Gowlings.com. [online] Available from: https://www.lexology.com/library/detail.aspx?g=5a3f3b03-a077-45d4-9981-36f713c92820 [Accessed 21 July 2020].

This approach is well suited to substantiate the possibility of coexistence of virtual property of users and rights of operators of virtual worlds or other web platforms. Virtual property rights to virtual objects will be related to intellectual property rights to virtual objects in the same mode as property rights in the physical world are related to intellectual property rights in the physical world. That is, the existence of virtual property rights will in no way affect the intellectual property rights embodied in virtual items. Just an alienation of a virtual property object will not mean the transfer of intellectual property rights to another person.

Virtual property right can be defined as a specific type of ownership, the object of which are digital assets. In addition to the specifics of the object (which will always be incorporeal things), this right will be characterized by the specifics of the grounds of origin, content, protection, etc.

The emergence of virtual property rights must be linked to the creation of a virtual object that has the properties of virtual property: rivalrousness, persistence, interconnectivity. These may be an user's account, avatar, and other multiplayer game items, a social media account, domain name, e-mail, and other digital assets that meet these attributes.

The specificity of virtual property rights is that the absolute nature of the owner's authority is manifested only in relations with third parties. That is, when establishing a virtual property right, there are two types of legal relationships. Firstly, there are legal relationships between the virtual property owner and third parties, in which the owner's powers are absolute. Secondly, there are legal relationships between the virtual property owner and the provider, in which the scope of the owner's powers may be limited by the interests of the developer / owner of the platform. For instance, if the game or social network operator decides that the game or social network should cease to exist, this will be the basis for terminating the virtual property rights without further compensation to the users. In addition, the capabilities of the virtual property owner will be determined by the features of a particular platform, since its specificity may prevent certain user actions. This approach as a whole will not contradict the concept of property rights, since, despite the absolute nature of traditional property rights, it may be restricted in certain cases.

The specificity of the content of the virtual property right is determined by its object. Some powers of the owner in case of virtual property will differ in comparison to material objects. For example, the right to possess,

which assumes the control over a thing, with respect to virtual property becomes different. As *P. Palka* points out, there are two options: simpler and more complex. In a simpler case, the virtual property is stored on the owner's device (computer or laptop, etc.). In this case, the owner independently controls the device, the information system, and has the actual ability to use, modify, delete the virtual object so on. In order for someone else to deprive the person of such digital possession, it is necessary to either physically select the device or enter the device through the Internet. In a more complex case, thanks to the information system architecture, more than one person has actual control over a digital object. For example, a file uploaded to the cloud is both controlled by the user and the provider. The user must have permission from the provider to control this feature. At the same time, the provider may also use, modify or delete the object. They do not do this because, first, they are committed to not touching these objects, and secondly, if they take some action on such objects, it will undermine the trust of other users, and the provider eventually may lose his customers who will switch to another provider. However, the hosts actually have these objects in possession. In this sense, digital ownership is not exclusive unlike the traditional ownership – several people can have in possession the same object at the same time. Thus, the only way to provide the protection of the users' rights to possess their digital property is to determine what providers are allowed and forbidden to do.[23]

From the above analysis, conducted by *P. Palka*, it becomes clear that the ability to use in the construction of virtual property also has its own specificity. *D. Sheldon* points out that the right to use virtual items provided to users by the license agreement is significantly restricted compared to the right to use the material thing. In addition to the restrictions in using of digital assets provided by the code, the license agreement restricts users to permissions only on certain behaviour.[24]

Thus, if in traditional property relations the owner satisfies his or her own interests by his or her own actions, the specificity of the virtual property relations is determined by the obligation between the provider and the user. As, on the one hand, the owner can independently use his

[23] Palka, P. (2017) Op. cit., pp. 160–161.

[24] Sheldon, D. (2007) Claiming ownership, but getting owned: contractual limitations on asserting property interests in virtual goods. *UCLA Law Review*, 54, p. 764.

or her virtual property and satisfy his or her interests without the assistance of others, but in order to exercise this power, it must first be provided by the operator, who must give the owner permanent access to the digital object.

The ability to dispose of the virtual assets will also have its own specifics, since the ability to dispose of virtual property will depend on the features of the platform and some other factors. Sometimes alienating a virtual property may not be technically possible. In other cases, the inability to alienate may be due to social reasons (*P. Palka* cites an example of an alienation of a *Twitter* account owned, for example, by *Donald Trump*, without notifying users)[25]. Obviously, such cases can have detrimental consequences for society. Nevertheless, the situation when the ability to dispose of virtual property is limited by the terms of a particular platform, is negatively assessed. For example, many multiplayer games provide for a kind of domestic market where players have the right to dispose of in-game or real-currency game items. However, the alienation or exchange of accounts or the alienation of game items outside the game is prohibited. In general, the restriction on the right to dispose comes down to three cases: providers do not allow the alienation of objects for real money; providers allow the sale of virtual items for real money, but only with the use of systems created and controlled by them; providers allow the sale of some assets but forbid the alienation of others.[26] This situation is estimated as a misuse of providers by their rights and should not be tolerated.

In addition, the ability to dispose of a virtual asset is specific because, unlike real-world objects, alienation of virtual objects requires the assistance of the provider or developer. That is, developers must ensure the possibility to transfer of virtual property from one person to another.

The same applies to the protection of virtual property rights: even if the court decides, for example, to require the thing from the wrongful owner and transfer it to the rightful owner, it is impossible to execute such decision without the assistance of the provider, since virtual property exists within a certain platform. In this case, either the obligation of providers to facilitate the enforcement of court decisions should be provided for, or the ability of enforcement agents to access the platform to enforce

[25] Palka, P. (2017) Op. cit., p. 219.
[26] Sheldon, D. (2007) Op. cit., p. 766.

the judgment, or to provide for the enforcement of court decisions using artificial intelligence built into the platform. In addition, in the case of providers being involved in the process of enforcement of virtual property judgments, it should be taken into account that modifying the database to transfer virtual property requires some cost. The question of whom these costs will be relied upon must be addressed. It seems fair to charge offenders the costs incurred by providers in enforcing court decisions.

3. THE CONCEPT AND LEGAL NATURE OF A SOCIAL MEDIA ACCOUNT

Most often, the definition of social media is given from the point of view of its relation to media and publishers. Thus, *T. Standage* says that social media are

> *"two-way, conversational environments in which information passes horizontally from one person to another along social networks, rather than being delivered vertically from an impersonal central source".*[27]

J.A. Obar and S. Wildman add that social media are interactive and

> *"can be characterized as a shift from user as consumer to user as participant".*[28]

J. Samples states that social media are platforms, not publishers; they provide the means for large numbers of people to produce and consume information.[29]

However, there are neither legal nor doctrinal definition of a social media account as an object of legal relationships. To understand the legal nature of such object first of all we need to analyse its technical essence.

The term "social media" encompasses any online platform that allows individuals to communicate, create content and interact socially.[30] Social media can include blogs, wikis, podcasts, photos and video sharing, virtual

---

[27] Standage, T. (2013) *Writing on the Wall: Social Media – The First 2,000 Years*. New York: Bloomsbury, p. 8.

[28] Obar, J. A. and Wildman, S. (2015) Social Media Definition and the Governance Challenge: An Introduction to the Special Issue. *Telecommunications Policy*, 39 (9), p. 746.

[29] Samples, J. (2020) Why the Government Should Not Regulate Content Moderation of Social Media. *Cato Institute Policy Analysis*, 865, pp. 1–31.

worlds and social networking sites, such as *Facebook*, *Instagram*, *LinkedIn* and *Twitter*.[31]

Technically, a user account is a relationship established between a user and a computer, network or information service. In this relationship, a user is identified by a username and password, which are optional for computers and networks, but mandatory for registrations and subscriptions to online services.[32] An account can also be defined as a collection of data associated with a particular user of a multiuser computer system. Each account comprises a username and a password, and is the subject of security access levels, disk storage space, etc.[33]

Therefore, the conclusion can be made that a social media account (profile) is a personal page, where a user posts his or her personal information, uploads video, audio and other content, and by means of which he or she interacts with other people. The use of this page is only possible after a special procedure of authorization by creation of a username (login) and password. Thus, an account includes several elements: firstly, authentication information (which is necessary for authentication of the user by a provider and includes a username and a password); secondly, an account is linked to a database on the server provider, where information from this account is stored. This database connects a user with information available from social media.

Social media accounts have a complex structure and differ from one another depending on the opportunities given by a particular platform. Nevertheless, there are always certain elements in the structure of social media account. These are: a username and a password as a way of authorization of the user; information posted by a user on his or her personal page (content); the user's correspondence and personal data.

---

[30] Edosomwan, S., Prakasa, S., Kouame, D., Watson, J. and Seymour, T. (2011) The History of Social Media and its Impact on Business. *The Journal of Applied Management and Entrepreneurship*, 16 (3), pp. 79–91; Fuchs, C. (2014) *Social Media: A Critical Introduction*. London: Sage.

[31] Naito, A. (2012) A Fourth Amendment Status Update: Applying Constitutional Privacy Protection to Employees' Social Media Use. *Journal of Constitutional Law*, 14 (3), pp. 849–883; Park, S. and Abril, P. (2016) Digital Self-Ownership: A Publicity-Rights Framework for Determining Employee Social Media Rights. *American Business Law Journal*, 53 (3), pp. 537–598.

[32] Pcmag.com. (2019) *User account Definition from PC Magazine Encyclopedia*. [online] Available from: https://www.pcmag.com/encyclopedia/term/53549/user-account [Accessed 26 April 2020].

[33] Encyclopedia.com. (2019) *User account | Encyclopedia.com*. [online] Available from: https://www.encyclopedia.com/computing/dictionaries-thesauruses-pictures-and-press-releases/user-account [Accessed 26 April 2020].

Therefore, the legal regulation of social media accounts involves contract law provisions (*Terms of Service* developed by social media owners), intellectual property rights, data protection and privacy regulation, and property rights. Considering the above-mentioned, we can suggest the distinguishing of a legal regime of separate elements of the account and a legal regime of the account in general. To determine the legal nature of a social media account, we need to answer the question of whether it can be considered as an object of property or virtual property right.

As it was stated before, an object can be considered a kind of virtual property if it meets three characteristics: rivalrousness, persistence, interconnectivity. All of these could be applied to social media account. Social media account is rivalrous since it can be controlled by only one person at a specific time – the user excludes all other persons from access to it. An account is persistent as it will be kept for months, even if one only uses it for a few minutes per day and in case he or she does not use it for a long period of time. An account can also be characterized as interconnected since there is a possibility to use it together with other users who get such permission from the owner.

The grounds to consider an account to be an object of property rights could be found in the practice of the *European Court of Human Rights* (hereinafter referred to as *ECtHR*).

As it is known, the ECtHR has adopted a broad concept of property in its case law. The court stressed in its judgement in *Gasus v. Netherlands*[34] that the notion of "possession" is not limited to physical goods. The notion "possessions" in Art. 1 of *Protocol No. 1 to the Convention for the Protection of Human Rights and Fundamental Freedoms* (hereinafter referred to as *Convention*)

> *"has an autonomous meaning which is certainly not limited to ownership of physical goods: certain other rights and interests constituting assets can also be regarded as "property rights" and thus as "possessions" for the purposes of this provision"*.[35]

[34] See *Gasus Dosier- und Fördertechnik GmbH v Netherlands, Merits*. (1995) Application No 15375/89, A/306-B, [1995] ECHR 7. (1995). 20 EHRR 403, IHRL 3433 (ECHR 1995), 23rd February 1995, European Court of Human Rights [ECHR].

Later it was adopted an autonomous interpretation of the term "possessions", according to which it has an autonomous meaning which is independent from the formal classifications in national law.[36]

In addition to movable and immovable things, "possession" in the ECtHR's practice encompasses property and non-property interests, such as claims and debt, court actions, company shares and other financial instruments, licenses for business, future income, intellectual property, rental and real estate rights, social benefits and pensions, professional clients and more. In general, the rights fall within the scope of Art. 1 of the Convention, if they meet three terms: significant economic value, possibility of identification in a tangible or intangible object, unconditional legal affiliation with the person concerned.

Currently, business shifts online, consequently, more and more personal webpages, blogs, and online accounts hold monetary value. According to *Forbes*, around 13.2 million women bloggers receive some sort of profit from their blogs, ranging from free products to a trip to Hawaii or a monthly stipend.[37] Social networking sites can also generate income for an account holder. A so-called "Twitter party", where a host invites followers to tweet about a product for one hour, can bring to the host from USD 750 to USD 5000, depending on the number of participants.[38] Profit generated from these sites is dependent on the number of people who click on advertisements.[39]

The resent case law indicates that the economic value of social media account is determined by the account's list of followers. Recently, courts have come to the conclusion that social media connections may amount

---

[35] Douglas, Z., Pauwelyn, J., Vinuales, J. E. (2014) *The foundations of international investments law: bringing theory into practice*. Oxford: Oxford University Press, p. 65. [online] Available from: https://books.google.com.ua/books?id=cl9iAwAAQBAJ&pg=PA65&lpg=PA65&dq=autonomous+meaning+which+is+independent+from+the+formal+classification&source=bl&ots=y3Gm06EEaO&sig=ACfU3U2KOQKwU-Z3h_8dHgycL3ATrmwqyg&hl=ru&sa=X&ved=2ahUKEwjeqJCg8pnpAhVWr4sKHY9RCKQQ6AEwAHoECAQQAQ#v=onepage&q=autonomous%20meaning%20which%20is%20independent%20from%20the%20formal%20classification&f=false [Accessed 20 April 2020].

[36] See *Saghinadze and Others v. Georgia*. (2010) Application no. 18768/05, Council of Europe: European Court of Human Rights, 27 May 2010. [online] Available from: https://www.refworld.org/cases,ECHR,4c04c1f22.html [Accessed 8 May 2020].

[37] Larissa, F. (2012). *Is Blogging Really a Way for Women to Earn a Living?* Forbes.com. [online] Available from: http://www.forbes.com/sites/larissafaw/2012/04/25/is-blogging-really-a-way-for-women-to-earn-a-living-2/ [Accessed 8 May 2020].

[38] Ibid.

[39] LaMotta, L. (2007) *How to Make Money Online*. Forbes.com. [online] Available from: http://www.forbes.com/2007/11/09/microsoft-yahoo-coke-ent-tech-cx_ll_1108makemoneyonline.html [Accessed 8 May 2020].

to a customer list and, consequently, be protected as trade secrets. Relevant factors that are used to evaluate the independent economic value in a trade secret case include: the time and resources spent on generating a customer list, whether access to the information was strictly limited, and whether it would be difficult to replicate the information included in the customer list.[40]

For instance, in *PhoneDog v. Kravitz*[41] the court found that the economic value of a social media account with 17,000 followers lies in the account's list of followers and the traffic that those followers generated to the *PhoneDog* website because the *Twitter* account produces revenue from advertisers.[42] In *Eagle v. Morgan*[43] the court concluded that the employer had made a *"substantial investment of time, effort and money"* into creating the *LinkedIn* account.[44] In *CDM Media USA, Inc. v. Simms*[45], a technology marketing and media company asserted that a *LinkedIn* group that included 679 names of current or potential customers was a trade secret. The court denied the former employee's motion to dismiss the case because the plaintiff proved that *"the membership list was a valuable secret commodity"* due to the limited access and amount of time, effort, and cost the marketing and media company expended to develop the *LinkedIn* membership list.[46]

Another argument in favor of recognizing accounts as a type of property can be found in the practice of the US bankruptcy courts. As in some respects business social media accounts provide value to the business with access to customers and potential customers, bankruptcy courts have found that business accounts on social media, including pages for business run by individual employees, are property interests which are recognised as intangible assets under the *Bankruptcy Code*.[47] Recent bankruptcy cases conclude that the administrative privileges and associated digital rights are

---

[40] Leeson, P. A. (2016) How many #followers do you have?: evaluating the rise of social media and issues concerning in re CTLI's determination that social media accounts are property of the estate. *Catholic University Law Review*, 66 (2), p. 510.

[41] See *PhoneDog v. Kravitz*. (2011) No. C 11-03474 MEJ. 2011 WL 5415612 (N.D. Cal. Nov. 8, 2011)

[42] Op. cit., p. 511.

[43] See *Eagle v. Morgan.* (2013) No. 11-4303, 2013 WL 943350, at *9 (E.D. Pa. Mar. 12, 2013).

[44] Leeson, P. A. (2016) Op. cit., p. 511.

[45] See *CDM Media USA, Inc. v. Simms*. (2015) No. 14 CV 9111. 2015 WL 1399050 (N.D. III. Mar. 25, 2015).

[46] Leeson, P. A. (2016) Op. cit., p. 512.

[47] See *In re CTLI, LLC* (2015), 528 B.R. 359, 359 (Bankr. S.D. Tex. Apr. 3, 2015); *In re Borders Grp.* (2011), No. 11-10614 (MG), 2011 WL 5520261, at *13 (Bankr. S.D.N.Y. Dec. 7, 2011).

bona fide assets and business goodwill.[48] Moreover, there are discussed modes of followers' estimation. Thus, *Tristan Louis* has suggested estimating the value of an individual user by taking the market cap and dividing it by the number of users.[49] *PhoneDog* in his case claimed that industry standards valued each *Twitter* follower at USD 2.50 per month.[50]

Thus, an account (especially the one with many followers) does have economic value. This value could be determined by the value of followers or considering the maximum amount a consumer is willing to pay for an item in a free market economy.[51] Accounts with many followers have higher demand because they are more attractive for advertising and give more opportunities to influence people. The fact that there are individuals interested in obtaining someone's account means that accounts do have value.

If we recognize that an account has economic value and, respectively, can be covered by the right to possessions in terms of the Convention, it can be qualified as a kind of property and an object of virtual property right.

4. LEGAL ISSUES OF THE USE OF SOCIAL MEDIA ACCOUNT

Most common issues that occur when using social media accounts are connected to business accounts and post-mortem fate of accounts.

Business social media accounts are companies' profiles created and managed by their employees. The problem could arise in case an employee, who managed such company's page, dismisses. In such case, the issue of who gets the rights to the account must be resolved. For instance, in *PhoneDog v. Kravitz*[52], the employee, who provided social media marketing for a company was dismissed. However, he continued to use the company's *Twitter* account, which had 17,000 subscribers. He just changed the handle of the account from *@PhoneDog_Noah* to *@noahkravitz*. The plaintiff claimed that the *Twitter* password was a trade secret and its

[48] Park, S. and Abril, P. (2016) Op. cit., p. 30.

[49] Louis, T. (2013) *How Much Is A User Worth?* Forbes.com. [online] Available from: https://www.forbes.com/sites/tristanlouis/2013/08/31/how-much-is-a-user-worth/#31bdc8b41c51 [Accessed 26 April 2020].

[50] See *PhoneDog v. Kravitz*. (2011) No. C 11-03474 MEJ, 2011 WL 5415612, at *3 (N.D. Cal. Nov. 8, 2011).

[51] Investopedia. (2019) *Economic Value*. [online] Available from: https://www.investopedia.com/terms/e/economic-value.asp [Accessed 13 April 2020].

[52] See *PhoneDog v. Kravitz.* (2011) No. C 11-03474 MEJ. 2011 WL 5415612 (N.D. Cal. Nov. 8, 2011).

continued unauthorized use was misappropriation. The court accepted that under certain circumstances a *Twitter* password could be a trade secret.[53]

In *Eagle v. Morgan*[54], the use of the *LinkedIn* profile became the subject of judicial proceedings. The plaintiff, being the owner of the company, created an account on *LinkedIn* for professional and personal purposes. After the company was taken over by another one, the plaintiff was replaced by another manager. At the same time, the new owners of the company obtained access to the plaintiff's profile, changed the password and the photo and replaced plaintiff's name with that of the new manager. At the same time, some professional information in relation to the claimant was left in the profile, including list of contacts. On this basis, the plaintiff filed the lawsuit on several grounds, including identity theft. The court concluded that the plaintiff had proved tortious interference by her employer but failed to award any damages.[55]

In *Ardis Health, LLC v. Nankivell*[56], the defendant, who provided social media marketing in the company, refused to provide access to the company's accounts after his dismissal. The court ordered him to do it as the defendant signed the agreement that information from accounts belonged to the claimant.

Thus, in situations where a dispute between the company and workers concerning business accounts might appear, it is sensible to specify in a special contract who has the rights in respect of the separate elements of the social media account – profile, access, content, followers.[57] Companies should develop their own policy concerning social networks where all possible consequences regarding to the rights in relation to social media accounts of the company should be covered.

One more issue connected with social media accounts is the determination of their destiny after the user's death.

Currently possible actions with accounts in case of their owners' death are defined by internal instructions for use in search engines or social networking sites. In such internal rules consequences are defined by users

---

[53] Park, S. and Abril, P. (2016) Op. cit., p. 5.

[54] See *Eagle v. Morgan.* (2013) No. 11-4303, 2013 WL 943350, at *9 (E.D. Pa. Mar. 12, 2013).

[55] Park, S. and Abril, P. (2016) Op. cit., p. 6.

[56] See *Ardis Health, LLC v. Nankivell.* (2011) No. 11 Civ. 5013 (NRB). 2011 WL 4965172 (S.D.N.Y. Oct. 19, 2011).

[57] Lizerbram, D. (2013) *A Legal Perspective: Who Owns Social Media Profiles?*. [blog] Marketo. Available from: https://blog.marketo.com/2012/08/a-legal-perspective-who-owns-social-media-profiles.html [Accessed 26 April 2020].

or by a system (for example, *Yahoo!* provides for removal of the account on the user's death whereas *Facebook* gives to users an opportunity to dispose of the account on death). At the same time, there is no legal regulation of such actions in most countries, nor there any legal provisions on the possibility to officially bequeath social media account.

However, in the USA there are already some cases of state intervention in legal regulation of inheritance of accounts. The first step in this direction was taken in 2014, when an *Act to Amend Title 12 of the Delaware Code Relating to Fiduciary Access to Digital Assets and Digital Accounts* was accepted. This Act determines the notion of "digital account" and "digital asset", and gives the possibility to appoint a fiduciary over a digital account or a digital asset, who may exercise all rights in digital assets and digital accounts of an account holder, to the extent permitted by law or any *End User License Agreement*.[58] Later, in 2015, in the majority of states of the USA the *Uniform Fiduciary Access to Digital Assets Act* was enacted. It allows individuals to specify in their will that the executor of their estate can have access to their e-mail and social media profiles.[59] The law, in fact, uses the construction of a fiduciary or trust for disposal of digital assets of a deceased person.[60]

In those states where the *Uniform Fiduciary Access to Digital Assets Act* was not enacted, companies decide themselves, whether to provide access to digital accounts of the deceased family member to his/her relatives. For example, in *Yahoo's Terms of Service* agreement the provisions on closure of accounts in case of the user's death are enshrined. Based on this provisions *Yahoo!* bans the access to the user's account in case of his or her death. Such an approach caused a lawsuit in the State of Massachusetts (in this State the *Uniform Fiduciary Access to Digital Assets Act* was not enacted). In *Ajemian v. Yahoo!, Inc.*[61], the *Supreme Court of the State*

---

[58] House of Representatives 147th General Assembly. (2014) *An Act to Amend Title 12 of the Delaware Code Relating to Fiduciary Access to Digital Assets and Digital Accounts*. House Bill no. 345. Available from: http://legis.delaware.gov/BillDetail/23219 [Accessed 26 April 2020].

[59] The Conversation. (2018) *Estate planning for your digital assets*. [online] Available from: https://theconversation.com/estate-planning-for-your-digital-assets-90613 [Accessed 26 April 2020].

[60] National Conference of Commissioners on Uniform State Laws. (2015) *Revised Uniform Fiduciary Access to Digital Assets Act (2015)*. [online] Available from: https://my.uniformlaws.org/viewdocument/final-act-no-comments-33?CommunityKey=f7237fc4-74c2-4728-81c6-b39a91ecdf22&tab=librarydocuments [Accessed 26 April 2020].

[61] See *Ajemian v. Yahoo!, Inc. 84 N.E.3d 766*. (2017) No. 17-1005, 2018 WL 489291 (U.S. Mar. 26, 2018).

of Massachusetts concluded that the personal representatives may provide lawful consent on the deceased's behalf to the release of the contents of the *Yahoo!* e-mail account. Thus, there is ambiguous situation in practice. On the one hand, *Terms of Service* agreements are in their essence a contract and, consequently, create binding obligations on the parties. On the other hand, the possibility of the platform to delete e-mails or profiles which are in its possession, but in fact belong to the user, established by the *Terms of Service*, is unfair. As mentioned in *Ajemian v. Yahoo!, Inc.*, even if the *Terms of Service* agreement were fully enforceable, which would have given the *Yahoo!* the possibility to delete a user's account, it nonetheless could not justify the destruction of e-mail messages after a court orders that they be provided to the user or his or her personal representatives as such destruction would constitute contempt of a court order.[62]

The possibility of inheriting social media accounts is recognized also in European case law. Thus, the *Federal Court of Justice in Karlsruhe* has recently allowed inheritance of accounts in *Facebook*. According to the judgment, online data should be treated in the same way as private diaries or letters, and pass to heirs. The case involved the parents of a 15--year-old girl killed by a train in 2012. The deceased girl's parents wanted access to her account to try to find out whether her death had been by suicide or accident. *Facebook* had refused access to the account after their daughter's death, citing privacy concerns about the girl's contacts. Under its current policy, the company only allows relatives of the deceased person partial access to the account, allowing them to change the page into an online memorial or to delete it entirely. The lower German court found for the parents in 2015, supporting the claim that *Facebook* data was covered by inheritance law as the equivalent of private correspondence. But in 2017, an appeals court overturned the ruling, on the grounds that any contract between the girl and the company ended with her death and could not pass to the parents. The case went to the *Federal Court of Justice*, and her parents have now reportedly taken over the account. According to what the judge said, it was common to hand over private diaries and correspondence to legal heirs after death, and there was no reason to treat digital data any

[62] Ibid.

differently. Moreover, the court added that the parents had a right to know to whom their child, a minor, had spoken online.[63]

Therefore, the situation is similar to that in the USA: relatives can require online service providers to give access to the account of the deceased family member, and providers have to give such an access.

Thus, currently the fate of social media accounts directly depends on the *Terms of Service*, which can grant to the social media provider the right to dispose of this property. Most of them are written to allow a service provider wide opportunities in determining if digital assets are descendible and how they are to be distributed. The provisions drafted by a service provider, not an account holder, determine how digital assets are treated after an account holder's death. Thus, account holders must exclusively rely on service providers' good will in allowing any transfer of their assets at death.[64] That is not contrary to the basic principles of contract law as users accept these terms by signing up to the agreement. However, recent cases in the US and Germany courts show that courts tend to protect users' (or their relatives') interests. Therefore, we can assume that in the near future some provisions of *Terms of Service*, which forbid authorising access to accounts or provide an opportunity to online service providers to dispose of users' accounts, will be considered as discriminatory and illegal. As *Banta N.M.* rightly points out,

> *"any contractual provision that prohibits transfer, even if procedurally valid, should be void as against public policy. Prohibiting contracts from transferring assets fundamentally alters the character of succession law, which promotes transfer guided by the testamentary intent of a decedent, and is contrary to the reason contracts were originally accepted as a means of transfer".*[65]

She adds, that

> *"service providers are not focused on protecting an individual's control over assets he or she created, earned, or uploaded. Protecting an individual's control over assets or property interests is a concern of courts and*

[63] BBC News. (2018) *Parents win rights to dead child's Facebook*. [online] Available from: https://www.bbc.com/news/world-europe-44804599 [Accessed 26 April 2020].

[64] Banta, N. M. (2014) Inherit the Cloud: The Role of Private Contracts in Distributing or Deleting Digital Assets at Death. *Fordham Law Review*, 83 (2), p. 821.

[65] Op. cit., p. 803.

legislatures. Courts and legislatures should continue to determine whether public policy favors digital asset inheritance".[66]

Despite a large number of questions in the sphere of inheritance of digital assets, it is suggested to take care of digital property's, in particular, social media accounts, fate by inscription of some specific provisions in the will, having in mind, however, provisions of *Terms of Service* and in its limits.[67]

We should mention also that the *European Law Institute* is currently establishing a joint study group with the *Uniform Law Commission* in the USA to see if the *Uniform Fiduciary Access to Digital Assets Act* could be used as a model for European legislation.[68] It means that there is likely to be a unified approach to determination of the post-mortem fate of digital assets in the world. To ensure protection and digital assets management it would be worthwhile to appoint a digital executor. Management of digital assets, including social media accounts, is possible within the framework of a trust or fiduciary, which are known, respectively, in the common law and civil law systems.

5. CONCLUSIONS

Despite the huge number of relations arising regarding social media accounts, no country in the world has a clear legal regulation of such relations. In order to ensure their proper regulation, it is necessary first of all to determine the legal nature of social media accounts. The analysis of the recent judicial practice and modern legal literature reveals a tendency for an account to be considered as a digital asset. Digital assets are more and more often treated as property, they are considered to be objects of property right and the theory on virtual property rights in this context becomes more and more discussable today.

Social media accounts meet all characteristics of virtual property as they are rivalrous, persistent, interconnected. They also meet all characteristics of "possession" in terms of *Protocol No. 1 to the Convention for the Protection of Human Rights and Fundamental Freedoms*, as they can have significant

---

[66] Op. cit., p. 829.

[67] Conway, H. and Grattan S. (2017) The "New" New Property: Dealing with Digital Assets on Death. In: *Modern Studies in Property Law*. Oxford and Portland, Oregon: Hart Publishing, p. 111.

[68] Op. cit., p. 113

economic value, possibility of identification in tangible or intangible object, unconditional legal affiliation with the person concerned. Notwithstanding that digital assets may not have an objective monetary value, they still could have a great deal of emotional value. From this point of view, social media accounts could be divided into business and private accounts. While the former will have primarily economic value, the latter will be characterized by greater moral value. However, that does not prevent the possibility to treat them as property, since emotional or sentimental interests in property are also taken into account in many cases. Thus, in *Ark Land Co. v. Harper*[69], it was mentioned, that

> *"the economic value of the property is not the exclusive test for deciding whether to partition in kind or by sale. Evidence of longstanding ownership, coupled with sentimental or emotional interests in the property, may also be considered in deciding whether the interests of the party opposing the sale will be prejudiced by the property's sale".*[70]

Besides, emotional harm can be compensated under tort law. Thus, preserving digital correspondence, pictures, videos, and posts for their emotional value is as important as preserving assets with monetary value.[71]

In case we recognise social media accounts as a type of property and objects of virtual property rights, they could get appropriate legal protection. All issues, related to the division of rights on business social media accounts, the inheritance of social media accounts, thefts of accounts could be covered by provisions on property protection. However, it would be necessary to take into account the specifics of the virtual property right while dealing with social media accounts. Thus, the usual powers of the owner would differ regarding digital assets. Such powers should be in balance with the interests of the developer / owner of the platform. This approach as a whole will not contradict the concept of property right, since, despite the absolute nature of traditional property right, it may be restricted in certain cases. Nevertheless, the provisions of the *Terms of Services*, which establish general rules on the use of social media account, should be balanced from the point of view of users' protection. Since owners of digital platforms are in most cases monopolists, there is a room for state

[69] See *Ark Land Co. v. Harper*. (2004) No. 599 S.E.2d 754, 761 (W. Va. 2004).
[70] Ibid.
[71] Banta, N. M. (2014) Op. cit., p. 851.

intervention with the aim to protect consumers. Notwithstanding that *Terms of Services* are a private contract in their essence, they still could establish the ownership to digital assets, in particular, social media accounts. In order to ensure the possibility to exercise users' rights regarding digital assets, *Terms of Service* should stipulate the obligation of online service providers to assist users in the exercising of their rights. The misuse of providers by their rights should be prohibited.

LIST OF REFERENCES

[1] Abramovitch, S. H. (2009). *Virtual property in virtual worlds*. Gowlings.com. [online] Available from: https://www.lexology.com/library/detail.aspx?g=5a3f3b03-a077-45d4-9981-36f713c92820 [Accessed 21 July 2020].

[2] *Ajemian v. Yahoo!, Inc. 84 N.E.3d 766*. (2017) No. 17-1005, 2018 WL 489291 (U.S. Mar. 26, 2018).

[3] *Ardis Health, LLC v. Nankivell*. (2011) No. 11 Civ. 5013 (NRB). 2011 WL 4965172 (S.D.N.Y. Oct. 19, 2011).

[4] *Ark Land Co. v. Harper*. (2004) No. 599 S.E.2d 754, 761 (W. Va. 2004).

[5] Banta, N. M. (2014). Inherit the Cloud: The Role of Private Contracts in Distributing or Deleting Digital Assets at Death. *Fordham Law Review*, 83 (2).

[6] BBC News. (2018) *Parents win rights to dead child's Facebook*. [online] Available from: https://www.bbc.com/news/world-europe-44804599 [Accessed 26 April 2020].

[7] Blazer, Ch. (2006) The five indicia of virtual property. *Pierce Law Review*, 5.

[8] Castronova, E. (2001) Virtual worlds: a first-hand account of market and society on the Cyberian Frontier. *CESifo Working Paper Series*, 618.

[9] *CDM Media USA, Inc. v. Simms*. (2015) No. 14 CV 9111. 2015 WL 1399050 (N.D. III. Mar. 25, 2015).

[10] Conway, H. and Grattan S. (2017) The "New" New Property: Dealing with Digital Assets on Death. In: *Modern Studies in Property Law*. Oxford and Portland, Oregon: Hart Publishing.

[11] DaCunha, N. (2010) Virtual property, real concerns. *Akron Intellectual Property Journal*, 4 (1).

[12] Douglas, Z., Pauwelyn, J., Vinuales, J. E. (2014) *The foundations of international investments law: bringing theory into practice*. Oxford: Oxford University Press. [online] Available from: https://books.google.com.ua/books?id=cl9iAwAAQBAJ&pg=PA65&lpg=PA65&dq=autonomous+meaning+which+is+independent+from+the+formal+classification&source=

bl&ots=y3Gm06EEaO&sig=ACfU3U2KOQKwU-Z3h_8dHgycL3ATrmwqyg&hl=ru&sa=X&ved=2ahUKEwjeqJCg8pnpAhVWr4sKHY9RCKQQ6AEwAHoECAQQAQ#v=onepage&q=autonomous%20meaning%20which%20is%20independent%20from%20the%20formal%20classification&f=false [Accessed 20 April 2020].

[13] *Eagle v. Morgan*. (2013) No. 11-4303, 2013 WL 943350, at *9 (E.D. Pa. Mar. 12, 2013).

[14] Edosomwan, S., Prakasa, S., Kouame, D., Watson, J. and Seymour, T. (2011) The History of Social Media and its Impact on Business. *The Journal of Applied Management and Entrepreneurship*, 16 (3).

[15] Encyclopedia.com. (2019) *User account | Encyclopedia.com*. [online] Available from: https://www.encyclopedia.com/computing/dictionaries-thesauruses-pictures-and-press-releases/user-account [Accessed 26 April 2020].

[16] Erlank, W. (2012) *Property in virtual worlds*. PhD. Stellenbosch: Stellenbosch University.

[17] Fairfield, J. (2005) Virtual property. *Boston University Law Review*, 85. [online] Available from: https://ssrn.com/abstract=807966 [Accessed 26 April 2020].

[18] Fuchs, C. (2014) *Social Media: A Critical Introduction*. London: Sage.

[19] *Gasus Dosier- und Fördertechnik GmbH v Netherlands, Merits*. (1995) Application No. 15375/89, A/306-B, [1995] ECHR 7. (1995). 20 EHRR 403, IHRL 3433 (ECHR 1995), 23rd February 1995, European Court of Human Rights [ECHR].

[20] Gong, J. (2011) Defining and addressing virtual property to international treaties. *Boston University Journal of Science & Technology Law*, 17.

[21] House of Representatives 147th General Assembly. (2014) *An Act to Amend Title 12 of the Delaware Code Relating to Fiduciary Access to Digital Assets and Digital Accounts*. House Bill no. 345. Available from: http://legis.delaware.gov/BillDetail/23219 [Accessed 26 April 2020].

[22] Hurter, E. (2009) The international domain name classification debate: are domain names "virtual property", intellectual property, property or no property at all? *The Comparative and International Law Journal of Southern Africa*, 42 (3).

[23] *In re Borders Grp*. (2011) No. 11-10614 (MG), 2011 WL 5520261, at *13 (Bankr. S.D.N.Y. Dec. 7, 2011).

[24] *In re CTLI, LLC*. (2015) 528 B.R. 359, 359 (Bankr. S.D. Tex. Apr. 3, 2015).

[25] Investopedia. (2019) *Economic Value*. [online] Available from: https://www.investopedia.com/terms/e/economic-value.asp [Accessed 13 April 2020].

[26] LaMotta, L. (2007) *How to Make Money Online*. Forbes.com. [online] Available from: http://www.forbes.com/2007/11/09/microsoft-yahoo-coke-ent-tech-cx_ll_1108makemoney online.html [Accessed 8 May 2020].

[27] Larissa, F. (2012). *Is Blogging Really a Way for Women to Earn a Living?* Forbes.com. [online] Available from: http://www.forbes.com/sites/larissafaw/2012/04/25/is-blogging-really-a-way-for-women-to-earn-a-living-2/ [Accessed 8 May 2020].

[28] Lastowka, G. and Hunter, D. (2004) The laws of the virtual worlds. *California Law Review*, 92 (1).

[29] Leeson, P. A. (2016) How many #followers do you have?: evaluating the rise of social media and issues concerning in re CTLI's determination that social media accounts are property of the estate. *Catholic University Law Review*, 66 (2).

[30] Lizerbram, D. (2013) *A Legal Perspective: Who Owns Social Media Profiles?* [blog] Marketo. Available from: https://blog.marketo.com/2012/08/a-legal-perspective-who-owns-social-media-profiles.html [Accessed 26 April 2020].

[31] Louis, T. (2013) *How Much Is A User Worth?* Forbes.com. [online] Available from: https://www.forbes.com/sites/tristanlouis/2013/08/31/how-much-is-a-user-worth/#31bdc 8b41c51 [Accessed 26 April 2020].

[32] Mousourakis, G. (2015) *Roman law and the origins of the civil law tradition*. Switzerland: Springer.

[33] Naito, A. (2012) A Fourth Amendment Status Update: Applying Constitutional Privacy Protection to Employees' Social Media Use. *Journal of Constitutional Law*, 14 (3).

[34] National Conference of Commissioners on Uniform State Laws. (2015) *Revised Uniform Fiduciary Access to Digital Assets Act (2015)*. [online] Available from: https://my.uniform laws.org/viewdocument/final-act-no-comments-33?CommunityKey=f7237fc4-74c2-4728-81c6-b39a91ecdf22&tab=librarydocuments [Accessed 26 April 2020].

[35] Nelmark, D. (2004) Virtual property: the challenges of regulating intangible, exclusionary property interests such as domain names. *Northwestern Journal of Technology and Intellectual Property*, 3.

[36] Nelson, J. W. (2010). The virtual property problem: what property rights in virtual resources might look like, how they might work, and why they are a bad idea. *McGeorge Law Review*, 41.

[37] Obar, J. A. and Wildman, S. (2015) Social Media Definition and the Governance Challenge: An Introduction to the Special Issue. *Telecommunications Policy*, 39 (9).

[38] Palka, P. (2017) *Virtual property: towards a general theory*. PhD. Florence: European University Institute.

[39] Park, S. and Abril, P. (2016) Digital Self-Ownership: A Publicity-Rights Framework for Determining Employee Social Media Rights. *American Business Law Journal*, 53 (3).

[40] Pcmag.com. (2019) *User account Definition from PC Magazine Encyclopedia*. [online] Available from: https://www.pcmag.com/encyclopedia/term/53549/user-account [Accessed 26 April 2020].

[41] *PhoneDog v. Kravitz*. (2011) No. C 11-03474 MEJ. 2011 WL 5415612 (N.D. Cal. Nov. 8, 2011).

[42] *Saghinadze and Others v. Georgia.* (2010) Application no. 18768/05, Council of Europe: European Court of Human Rights, 27 May 2010. [online] Available from: https://www.refworld.org/cases,ECHR,4c04c1f22.html [Accessed 8 May 2020].

[43] Samples, J. (2020) Why the Government Should Not Regulate Content Moderation of Social Media. *Cato Institute Policy Analysis*, 865.

[44] Sheldon, D. (2007) Claiming ownership, but getting owned: contractual limitations on asserting property interests in virtual goods. *UCLA Law Review*, 54.

[45] Standage, T. (2013) *Writing on the Wall: Social Media – The First 2,000 Years*. New York: Bloomsbury.

[46] Stephens, M. (2002) Sales of in-game assets: an illustration of the continuing failure of intellectual property law to protect digital-content creators. *Texas Law Review*, 80.

[47] The Conversation. (2018) *Estate planning for your digital assets*. [online] Available from: https://theconversation.com/estate-planning-for-your-digital-assets-90613 [Accessed 26 April 2020].

[48] Van der Walt, A. J. (2011) *Constitutional Property Law*. 3rd ed. Cape Town: Juta Law.

DOI 10.5817/MUJLT2020-2-4

MALICIOUS CYBER OPERATIONS, "HACKBACKS" AND INTERNATIONAL LAW: AN AUSTRIAN EXAMPLE AS A BASIS FOR DISCUSSION ON PERMISSIBLE RESPONSES[*]

by

ERICH SCHWEIGHOFER[**], ISABELLA BRUNNER[***], JAKOB ZANOL[****]

In January 2020, Austria publicly announced that some of its governmental institutions have been hit by a significant malicious cyber operation and that it cannot be denied – at least for the moment – that a state was behind this operation. One month later, the Austrian Foreign Ministry declared the cyber operation to be officially over. While Austria noted that it took "countermeasures" against the operation, it is not entirely clear what it meant by that. This article elaborates the question what response options a state like Austria would have against a malicious cyber operation under the current framework of international law. It, hence, tries to answer when a "hackback" is lawful under international law and when it is not.

KEY WORDS

Countermeasures, Cyber Defense, Cyberspace, Hackback, International Law, Law of State Responsibility, Malicious Cyber Operation

[*] This contribution is inspired from and supported by both the Austrian *KIRAS-Project ACCSA* (https://www.kiras.at/gefoerderte-projekte/detail/d/accsa-austrian-cyber-crises-support-activities-1/) and the *Center for Intelligence and Security Studies* (*CISS* – https://www.unibw.de/ciss). The project *ACCSA* is financed by the *Austrian Federal Ministry for Transport, Innovation and Technology* and the *Austrian Research Promotion Agency* (*FFG* – https://www.ffg.at/en).

[**] erich.schweighofer@univie.ac.at, University of Vienna, Department of International Law; Centre for Computers and Law, Austria.

[***] isabella.brunner@univie.ac.at, University of Vienna, Department of International Law, Austria.

[****] jakob.zanol@univie.ac.at, University of Vienna, Department of International Law; Centre for Computers and Law, Austria.

1. INTRODUCTION

In January 2020, Austria publicly announced that the *Austrian Foreign Ministry* has been hit by a significant malicious cyber operation and that it cannot be denied – at least for the moment[1] – that a state was behind this operation.[2] In February 2020, the *Foreign Ministry* declared the malicious operation to be officially over.[3] While Austria noted that it took "countermeasures" ("*Gegenmaßnahmen*")[4] it is not entirely clear what it meant by that. According to an Austrian blog, technicians managed to get rid of the malware, putting the hacking group "in the defensive".[5] There is no further information available whether Austria considered response options under international law. This leads us to the question what a state – in this case Austria – *could* do (or could have done) in such a case, i.e. what measures would be allowed under the current framework of international law. This contribution, therefore, seeks to shine light on the specific reactions international law allows a state in case it was injured by a wrongful conduct, specifically with respect to wrongful cyber operations. It will, hence, try to answer when a "hackback" is lawful under international law and when it is not.

This contribution defines "hackback" as a measure taken through "cyber means" by a state against the territory of another state to cease a wrongful conduct (in the form of a cyber operation) the former state has been the target of. At the outset, this means that this contribution does not cover questions regarding possible measures of redress of non-state actors that have been the target of malicious cyber operations.

---

1 In a press release, the *Austrian Foreign Ministry* noted that *"the investigation is still ongoing"* about who is behind the "attack", see Austrian Federal Ministry for European and International Affairs. (2020) *Cyber Attack on the Foreign Ministry is Over*. [press release] 13 February. Available from: www.bmeia.gv.at/en/the-ministry/press/announcements/2020/02/cyber-attack-on-the-foreign-ministry-is-over/ [Accessed 19 August 2020].

2 Austrian Press Agency. (2020) *Schwerwiegender Angriff auf IT-Systeme des Außenministeriums*. [press release] 4 January. Available from: https://www.ots.at/presseaussendung/OTS_20200104_OTS0020/schwerwiegender-angriff-auf-it-systeme-des-aussenministeriums [Accessed 19 August 2020].

3 Austrian Federal Ministry for European and International Affairs. (2020) *Cyber Attack on the Foreign Ministry is Over*. [press release] 13 February. Available from: www.bmeia.gv.at/en/the-ministry/press/announcements/2020/02/cyber-attack-on-the-foreign-ministry-is-over/ [Accessed 19 August 2020].

4 Ibid.

5 Moechel, E. (2020) *Vorläufige Bilanz des Cyberangriffs auf das Außenministerium*. [blog entry] 16 February. Radio FM4. Available from: https://fm4.orf.at/stories/2998771/ [Accessed 20 August 2020].

This paper will first address the concept of attribution of a wrongful conduct to a state and briefly introduce the reader to the so-called "due diligence principle". In a second step, it will analyse three ways international law allows a reaction (hackback) to a malicious cyber operation endangering a state's territorial integrity: 1) as a lawful countermeasure, 2) as an exercise of the right of self-defence, or 3) as a reaction out of necessity. Given that most cyber operations happen below the threshold of an armed attack[6] (only in case of the latter would a state be able to respond in self-defence[7]), it makes sense to take a look at countermeasures first before addressing self-defensive measures. "Necessity" as a response option should be seen as a last resort, given the high threshold and non-reliance on attribution (on these criteria, see in detail below). Hence it will be dealt with last.

There are many open questions related to these three measures that we cannot all cover in this paper. One, for example, would relate to the extensive debate about the application of international law to cyber operations, and whether some provisions apply or do not apply in the cyber context. For the purpose of this contribution, we align with the larger international community and scholarly opinion that the conventional rules of international law (be it treaty obligations, general principles or custom) apply to cyber operations.[8] We also assume that measures taken in self--defence as well as countermeasures can only be taken against a state and that the initial malicious cyber operation would have to be attributed to that state.[9] Since that latter aspect of attribution is a *conditio sine qua non* of two

---

[6] Guitton, C. (2017) *Inside the Enemy's Computer: Identifying Cyber-Attackers*. London: Hurst & Company, p. 107.

[7] Charter of the United Nations and Statute of the International Court of Justice, 26 June 1945 (1 UNTS XVI). Article 51.

[8] With UNGA Resolution 68/243, the international community endorsed the 2013 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE), which acknowledges that *"international law, and in particular the Charter of the United Nations, is applicable"*; see United Nations General Assembly. (2014) *Developments in the Field of Information and Telecommunications in the Context of International Security*. UN Doc A/RES/68/243. New York: United Nations. [online] Available from: https://undocs.org/A/RES/68/243 [Accessed 20 August 2020]; United Nations General Assembly. (2013) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General*. UN Doc A/68/98. New York: United Nations. Paragraph 19. [online] Available from: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf?OpenElement [Accessed 20 August 2020].

[9] To the contrary see, however, Zemanek, K. (2013) Armed Attack. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law* (online edition), paragraph 15; Tsagourias, N. (2012) Cyber Attacks, Self-Defence and the Problem of Attribution. *Journal of Conflict and Security Law*, 17, p. 241.

of the three measures that we will focus on in this contribution, we will start with discussing it first.

2. ATTRIBUTION AND DUE DILIGENCE

Attribution, in general, is the act of *"identifying the agent responsible for the action"*.[10] Usually, experts differentiate between technical, political and legal attribution.[11] All three aspects of attribution need to be seriously taken into account when undertaking a hackback.

Regarding technical attribution, identifying the person acting behind the computer is extremely difficult.[12] The high degree of anonymity in the cyber context, the possibilities of conducting false-flag operations and the difficulties to identify the actors behind multi-stage attacks make it almost impossible to distinguish a particular actor in cyberspace.[13] However, identifying the specific natural person and its relationship to a state is the quintessential prerequisite of legal attribution.[14] Because only if a relationship with a state can be established, the targeted state can take action against the state from which the unlawful conduct originates.

For legal attribution, the *ILC Articles on Responsibility of States for Internationally Wrongful Acts* (hereinafter referred to as *ILC Articles*) are the primary source to determine whose conduct can be attributed

[10] Clark, D. D. and Landau, S. (2011) Untangling Attribution. *Harvard National Security Journal*, 2, p. 1.

[11] *Nicholas Tsagourias* is deemed to be the author of this differentiation, see Tsagourias, N. (2012) Cyber Attacks, Self-Defence and the Problem of Attribution. *Journal of Conflict and Security Law*, 17, p. 234: *"Attribution of cyber attacks is thus a multifaceted process; it has technical, legal and political aspects, with each aspect feeding into the other"*; see also Government of the Netherlands. (2019) *Appendix to the Letter to the Parliament on the International Legal Order in Cyberspace*. The Hague, p. 6. [online] Available from: https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace [Accessed 4 February 2020]: *"In the context of cyberspace, three forms of attribution can be distinguished: Technical attribution* […]*, Political attribution* […and] *Legal attribution* […]*"*.

[12] Antonopoulos, C. (2015) State Responsibility in Cyberspace. In: Nicholas Tsagourias and Russell Buchan (eds.). *Research Handbook on International Law and Cyberspace*. Cheltenham and Northampton: Edward Elgar Publishing, p. 62.

[13] Brunner, I., Dobric, M. and Pirker, V. (2019) Proving a State's Involvement in a Cyber-Attack: Evidentiary Standards Before the ICJ. *Finnish Yearbook of International Law*, 25, pp. 76–77.

[14] See Antonopoulos, C. (2015) State Responsibility in Cyberspace. In: Nicholas Tsagourias and Russell Buchan (eds.). *Research Handbook on International Law and Cyberspace*. Cheltenham and Northampton: Edward Elgar Publishing, p. 58.

to a state.[15] The rules of attribution contained therein are widely held to reflect customary international law.[16]

The ILC Articles follow their own legal definition of attribution, which they define as

> *"the operation of attaching a given action or omission to a State."*[17]

For that, the ILC Articles distinguish between conduct of state organs (including *de facto* state organs)[18], and conduct of non-state actors, who – in one way or the other – act for the state.[19] Thus, if there is no sufficient link between the natural person or group of persons and the state, attribution on the basis of the ILC Articles – which regulate the consequences of wrongful *state* behaviour – cannot be established.

However, as already noted above, the difficulty does not lie in the legal realm, it lies within *proving* the sufficient link to the state: If a cyber operation originates from an IP address situated within the territory of state A, this information still does not provide us with which actor is actually behind the wrongful cyber operation. With its press release of 4 January 2020, Austria seems to suggest that it was indeed able to identify the origins of the "attack".[20] Unfortunately, however, it did not release any further information – let alone evidence – that would back up its position that a state actor could be behind the operation.

Given the fact that attribution of a wrongful conduct to a state tends to be very difficult, some scholars suggest to apply the so-called "due diligence" principle also in the cyber context: If a direct link to a state cannot be established, but it can be proven that the cyber operation derives

---

[15] UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10. [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

[16] See e.g. Antonopoulos, C. (2015) State Responsibility in Cyberspace. In: Tsagourias, N. and Buchan, R. (eds.). *Research Handbook on International Law and Cyberspace*. Cheltenham and Northampton: Edward Elgar Publishing, p. 58.

[17] UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10. P. 36 (Commentary to Article 2, paragraph 12). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

[18] Cf. op. cit., Article 4.

[19] Cf. op. cit., Articles 5, 8 and 11.

[20] Austrian Press Agency. (2020) *Schwerwiegender Angriff auf IT-Systeme des Außenministeriums*. [press release] 4 January. Available from: https://www.ots.at/presseaussendung/OTS_20200104_OTS0020/schwerwiegender-angriff-auf-it-systeme-des-aussenministeriums [Accessed 19 August 2020].

from a specific location on the territory of another state, state responsibility should arise on the basis that that other State violated its due diligence obligation.[21] Here, it must be highlighted that the state can merely be held responsible for acting negligently, not for the initial malicious cyber operation itself.[22]

The *"due diligence principle"* was most famously referred to in the *Corfu Channel* judgment of the ICJ, which notes that it is

> *"every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States"*.[23]

Therefore, this means that states cannot escape international responsibility by merely noting that they did not do it if they knew that malicious conduct was exercised through some (non-state or foreign state) actor on their territory. They can thus at least be held responsible for knowing about the malicious conduct and not taking appropriate action to counter it.

Some scholars suggest that this principle constitutes a general principle of (international) law,[24] which also applies to cyber activities.[25] Both *Tallinn Manuals*[26] have included a due diligence rule similar to the *Corfu Channel dictum*.[27] Along the same lines, *Recommendation 13(c) of the 2015 Report of the United Nations Group of Governmental Experts on Developments*

---

[21] Cf. Henriksen, A. (2015) Lawful State Responses to Low-Level Cyber-Attacks. *Nordic Journal of International Law*, 84 (2), p. 335; we have not seen Austria claim a violation of "due diligence" (yet).

[22] There is a suggestion in the literature, however, that a state should be held responsible for the initial act if it acted negligently, see, *inter alia*, Chircop, L. (2018) A Due Diligence Standard of Attribution in Cyberspace. *International & Comparative Law Quarterly*, 67, p. 643. There is no basis in international law, however, which would support such an argument.

[23] Judgment of 9 April 1949, *Corfu Channel (United Kingdom v. Albania)* (Merits), ICJ Reports 4, p. 22; The due diligence principle is said to have its origins in the Island of Palmas Arbitration, which notes the following: *"Territorial sovereignty* […] *involves the exclusive right to display the activities of a State. This right has as corollary a duty: the obligation to protect within the territory the rights of other States, in particular their right to integrity and inviolability in peace and in war"*, see Award of 4 April 1928, *Island of Palmas Case (Netherlands v. United States of America)*, Reports of International Arbitral Awards, United Nations, Vol. II, p. 839.

[24] See Bannelier-Christakis, K. (2014) Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?. *Baltic Yearbook of International Law*, 14, pp. 23, 27; Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 30; Koivurova, T. (2010) Due Diligence. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law* (online edition), paragraph 2 (*Bannelier-Christakis* and the *Tallinn Manual 2.0* call it a general principle of international law, *Koivurova* calls it a general principe of law).

[25] Schmitt, M. N. (2015) In Defense of Due Diligence in Cyberspace. *The Yale Law Journal Forum*, 125, p. 68; Bannelier-Christakis, K. (2014) Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?. *Baltic Yearbook of International Law*, 14, p. 27; Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 31.

in the Field of Information and Telecommunications in the Context of International Security (hereinafter referred to as *UNGGE*)[28] notes that

> *"States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs [Information and Communication Technologies]"*.[29]

This is significant, as the report reflects the opinion of governmental – and thus states' – experts on the application of international law to cyberspace. It is important to note, however, that the reference in the report is merely framed as a non-binding recommendation.[30] This suggests that it is far from clear that this principle is a stand-alone principle inducing obligations on states "in its own right" in the cyber context.[31] Austria has made it clear that it perceives the due diligence obligation to be *"a legally binding obligation under international law"*.[32] Given that we seek to shine light

---

[26] Both *Tallinn Manual 1.0* and *2.0* provide guidance for policy advisors and governmental legal experts on how international law applies to cyberspace. They contain cyber specific rules, which were agreed upon by an international group of experts and have been written under the auspices of the *NATO Cooperative Cyber Defence Centre of Excellence*.

[27] Schmitt, M. N. (ed.). (2013) *The Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, p. 26, Rule 5, stipulates that *"*[a] *State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States"*; Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 30, Rule 6, stipulates that *"*[a] *State must exercise due diligence in not allowing its territory, or territory or cyber infra-structure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States"*.

[28] The UNGGE is a group of governmental experts tasked with, *inter alia*, identifying how international law applies in cyberspace. It convened 5 times since 2004 and is currently convening for the 6th time until 2021.

[29] United Nations General Assembly. (2015) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General*. UN GAOR 70th Session, Item 93, UN Doc A/70/174. New York: United Nations, p. 8, paragraph 13(c). [online] Available from: https://undocs.org/A/70/174 [Accessed 20 August 2020].

[30] United Nations General Assembly. (2015) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General*. UN GAOR 70th Session, Item 93, UN Doc A/70/174. New York: United Nations, p. 8, paragraph 13.

[31] The Netherlands, e.g. *"regard the principle as an obligation in its own right, the violation of which may constitute an internationally wrongful act"*, but they also acknowledge that not all states share this view; see Government of the Netherlands. (2019) *Appendix to the Letter to the Parliament on the International Legal Order in Cyberspace*. The Hague, p. 4. [online] Available from: https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace [Accessed 4 February 2020].

[32] Government of Austria. (2020) *Austrian Statement on Rules, Norms and Principles for Responsible State Behaviour*, p. 2 (delivered on 17 June at the Informal OEWG June Consultations).

on Austria's perspective and also because we are convinced that this is the right decision, we will follow this assumption.

Next to that, there are a couple of other questions regarding the application of this principle to cyber operations:

Firstly, as the due diligence principle is an obligation of conduct, not result,[33] the content of the obligation needs to be assessed on a case-by-case basis.[34] For example, there seem to be differing views whether this obligation also contains an obligation to prevent.[35] While the *Tallinn Manual 2.0* notes that its experts agreed that

> *"the due diligence principle does not encompass an obligation to take material preventive steps"*,[36]

other scholars disagree. *Bannelier-Christakis*, for example, notes that the due diligence principle indeed also encompasses a duty of prevention.[37] Thus, it is not clear what kind of obligations are expected in the cyber context from each state in a given case.[38]

Secondly, questions remain regarding the knowledge requirement of the due diligence principle. On the one hand, how can an injured state prove that a state had knowledge about a specific cyber operation? It could be argued that as that latter state exercises exclusive control over its territory, it will be almost impossible for the injured state to establish enough evidence that that state knew about the situation.[39] On the other hand, does "constructive knowledge" (i.e. the state *should* have known

---

[33] Bannelier-Christakis, K. (2014) Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?. *Baltic Yearbook of International Law*, 14, p. 26; Koivurova, T. (2010) Due Diligence. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law* (online edition), paragraph 8; Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 49.

[34] See Kolb, R. (2015) Reflections on Due Diligence Duties and Cyberspace. *German Yearbook of International Law*, 58, p. 116: *"*[D]*ue diligence is a standard of care, a general clause, not a specific rule to be immediately applied; it requires a judgement of value of what could and should have reasonably be done under the circumstances* [… It] *is a relative and circumstantial term, since the judgement on it must take account of all the circumstances of the particular case; judgment thus always takes place in concreto; the judgment is also necessarily flexible"*.

[35] See Bannelier-Christakis, K. (2014) Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?. *Baltic Yearbook of International Law*, 14, p. 32; Kolb, R. (2015) Reflections on Due Diligence Duties and Cyberspace. *German Yearbook of International Law*, 58, p. 123; on the other hand, denying a duty of prevention, see Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 32.

[36] Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 32, paragraph 5.

[37] Bannelier-Christakis, K. (2014) Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?. *Baltic Yearbook of International Law*, 14, pp. 23, 30.

about the situation) suffice in order to claim a violation of the due diligence principle? Here, again, there seem to be diverging views.[40]

While Austria seems convinced of the principle's binding nature, it has not (yet) clarified its view on the specific questions raised above. It has, however, endorsed South Korea's proposal on the implementation of *Recommendation 13(c) of the 2015 GGE Report* in its statement in June 2020 at informal consultations of the OEWG, noting that

> *"a state which has been notified by another state about an ICT incident on its territory and has thus knowledge about it must take all reasonable steps to cease the incident and mitigate its adverse consequences for other states."*[41]

To conclude, the due diligence principle appears to be a useful tool to establish responsibility for those acts which occurred on a state's territory and of whose harmful nature the state knew about. Austria itself has not made use of this principle for the January 2020 incident. However, if a state succeeds in establishing the responsibility of another state for a malicious

---

[38] France, the Netherlands and Estonia advocate a "reasonability test", but do not specify what can be seen as "reasonable" and what not; see Ministère des Armées. (2019) *Droit International Appliqué Aux Operations Dans Le Cyberespace*. Paris, p. 10. [online] Available from: https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-du-ministere-des-armees/communique_la-france-s-engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international [Accessed 4 February 2020]; Government of the Netherlands. (2019) *Appendix to the Letter to the Parliament on the International Legal Order in Cyberspace*. The Hague, p. 4. [online] Available from: https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace [Accessed 4 February 2020]; Government of Estonia. (2019) *President of the Republic at the Opening of CyCon 2019*. Tallinn. [online] Available from: https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html [Accessed 20 August 2020].

[39] Bannelier-Christakis, K. (2014) Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?. *Baltic Yearbook of International Law*, 14, p. 29, who terms this a "probatio diabolica".

[40] See e.g. Schmitt, M. N. (ed.). (2013) *The Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, p. 28, paragraph 11: *"The International Group of Experts could not achieve consensus as whether this rule applies if the respective State has only constructive ('should have known') knowledge"*; see, however, Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 41, which says that *"*[t]*he International Group of Experts agreed that knowledge encompasses constructive knowledge for the purposes of this Rule"*; see also Bannelier-Christakis, K. (2014) Cyber Diligence: A Low--Intensity Due Diligence Principle for Low-Intensity Cyber Operations?. *Baltic Yearbook of International Law*, 14, pp. 29f, arguing in favour of the "constructive knowledge" theory; see also Kolb, R. (2015) Reflections on Due Diligence Duties and Cyberspace. *German Yearbook of International Law*, 58, pp. 123–124.

[41] Government of Austria. (2020) *Austrian Statement on Rules, Norms and Principles for Responsible State Behaviour*, p. 2 (delivered on 17 June at the Informal OEWG June Consultations).

cyber operation – be it through attributing the wrongful conduct directly to the state or through proving the state's violation of the due diligence principle, the question now is how the targeted state can react to it. As explained above, international law allows specific measures.

In principle, in the case of countermeasures and measures taken in self-defence the targeted State must know *who* is the perpetrator of the wrongful act (note, that in case of a violation of the due diligence principle, the wrongfulness relates to the state acting in negligence, and not in committing the wrongful act itself).

Thus, we will first start with addressing countermeasures (as the least "intervention-intensive" measure), followed by self-defense and end with the measure for which attribution to a state is not necessary: the exceptional plea of necessity.

3. HACKBACK AS A COUNTERMEASURE

A state may take a countermeasure against a state who has committed an internationally wrongful act, in order to induce the state to comply with its international obligations.[42] These countermeasures would be, in general, unlawful, if they were not undertaken as a reactive measure to the initial wrongful act.[43] Thus, in order to take a countermeasure, the initial act must be in violation of international law.

Countermeasures need to be distinguished from retorsions: Retorsions are lawful, but unfriendly acts, whereas countermeasures are unlawful acts,

[42] See UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10. Article 49. [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

[43] See UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10, p. 128 (Commentary to Part Three, Chapter II, paragraph 1). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020]; note that if a state wrongfully assumes that, let's say, state A was behind an operation and takes a counter-measure against state A, but it turns out that state B was actually behind the act, the injured state has committed an internationally wrongful act whose wrongfulness would not be precluded; see UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10, p. 130 (Commentary to Article 49, paragraph 3). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

whose unlawfulness is, however, precluded if they are a reaction to another violation of international law.[44]

In the context of hackbacks, three violations are of particular interest: 1) the violation of the prohibition to use force, 2) the violation of the prohibition of intervention and 3) the violation of the rule of sovereignty [in case one assumes that this is a stand-alone rule of international law applicable in cyberspace.[45] Austria has made it clear in its speech on international law at the February session of the so-called *Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security* (hereinafter referred to as *OEWG*) that it believes that it is a rule, and not merely a principle, and also suggested that the cyber operation against the *Foreign Ministry* might be a violation of sovereignty[46]]. Other works have dealt with these questions in detail, thus the focus of this paper is on the reactions to the *violation* of these primary obligations.[47]

There are certain procedural and substantive conditions that need to be fulfilled in order for a state to be entitled to undertake a countermeasure. First and foremost, if we follow the traditional view on countermeasures as stipulated by the ILC Articles, they are "non-forcible"[48], meaning that any countermeasure must not cross the threshold of use of force.[49] Within

---

[44] See UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10, p. 128 (Commentary to Part Three, Chapter II, paragraph 3). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

[45] To the contrary see the speech by UK Attorney General *Jeremy Wright*, noting that there is no principle of sovereignty in cyberspace. Wright, J. (2018) *Cyber and International Law in the 21st Century*. London. [online] Available from: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century [Accessed 20 August 2020].

[46] See Government of Austria. (2020) *OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security: Statement by Austria on International Law*. New York, p. 1 (delivered on 11 February at the second substantive session of the OEWG).

[47] See e.g. Roscini, M. (2014) *Cyber Operations and the Use of Force*. Oxford: Oxford University Press; Brunner, I., Dobric, M. and Pirker, V. (2019) Proving a State's Involvement in a Cyber--Attack: Evidentiary Standards Before the ICJ. *Finnish Yearbook of International Law*, 25; Schmitt, M. (2014) "Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law. *Virginia Journal of International Law*, 54.

[48] See UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10, p. 129 (Commentary to Part Three, Chapter II, paragraph 6). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

[49] See op. cit., Article 50(1)(a): *"Countermeasures shall not affect: (a) the obligation to refrain from the threat or use of force as embodied in the Charter of the United Nations"*; additionally, countermeasures must also not violate fundamental human rights obligations of the state, see op. cit., Article 50(1)(b).

the literature different approaches exist on how to determine what measures can be considered "forcible" and are therefore prohibited by Article 2(4) UN Charter.[50] A very reasonable approach by *Dinniss* is to assess whether the act in question resulted in a "physical consequence" – hence, in *"destruction of physical property, injury or loss of lives"*.[51] In that case, the act is to be considered a use of force. *Schmitt* also includes a *"serious loss of functionality"*,[52] which is helpful in case a massive amount of data is deleted and can only be recovered with great difficulty and immense technical skill. Otherwise, or when the

> *"physical results are too minimal or too removed from the chain of causation"*,

it cannot be presumed that Article 2(4) UN Charter is violated.[53] If a state were thus to defend itself against DDoS attacks without causing any physical consequences against the wrongful state (such as by blocking IP addresses from which the attacks are held to originate) this will not constitute a use of force.

The *Tallinn Manual 2.0*, on the other hand, viewed the limitation not to use force when responding with a countermeasure a "contentious issue" and thus decided not to address this limitation in a Rule.[54] Given the explicit wording of the ILC Articles, the note in the ILC Articles' Commentary that the obligation to refrain from the threat or use of force when taking countermeasures is "sacrosanct",[55] and the lack of state practice[56] in favour to digress from this obligation, we stick to the ILC Articles' assessment

---

[50] See Shackelford, S. J., and Andres, R. B. (2011) State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. *Georgetown Journal of International Law*, 42, p. 993.

[51] Dinniss, H. (2014) *Cyber Warfare and the Laws of War*. Cambridge: Cambridge University Press, p. 74.

[52] Schmitt, M. (2020) *Cyber Operations Against Vaccine R & D: Key International Law Prohibitions and Obligations*. [blog entry] 10 August. EJIL:Talk!. Available from: www.ejiltalk.org/cyber-operations-against-vaccine-r-d-key-international-law-prohibitions-and-obligations/ [Accessed 20 August 2020].

[53] Dinniss, H. (2014) *Cyber Warfare and the Laws of War*. Cambridge: Cambridge University Press, p. 74.

[54] See Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 125.

[55] See UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10, p. 131 (Commentary to Article 50, paragraph 1). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

rather than the *Tallinn Manual's*. Moreover, the ICJ explicitly noted in its *Nicaragua* judgment, that

> *"a use of force of a lesser degree of gravity* [as an armed attack] *cannot* […] *produce any entitlement to take* [collective] *countermeasures involving the use of force."*[57]

Admittedly, however, the opinion that forcible countermeasures are lawful was only shared by the minority of the experts of the *Tallinn Manual*.[58]

Second, Article 52(1)(b) ILC Articles foresees a notification requirement of the injured state to the responsible state that it decides to take countermeasures and a requirement to offer negotiations with the latter state.[59] In case of urgent countermeasures, however, there is no such requirement according to Article 52(2) ILC Articles.[60] The question is what constitutes *urgency* in that context. France seems to interpret *urgency* quite broadly, arguing that urgent countermeasures may be taken whenever

> *"there is a need to protect* [the victim state's] *rights"*.[61]

---

[56] Rather to the contrary, see Ministère des Armées. (2019) *Droit International Appliqué Aux Operations Dans Le Cyberespace*. Paris, p. 8. [online] Available from: https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-du-ministere-des-armees/communique_la-france-s-engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international [Accessed 4 February 2020]; Wright, J. (2018) *Cyber and International Law in the 21st Century*. London. [online] Available from: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century [Accessed 20 August 2020]; Government of Estonia. (2019) *President of the Republic at the Opening of CyCon 2019*. Tallinn. [online] Available from: https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html [Accessed 20 August 2020]; Government of the Netherlands. (2019) *Appendix to the Letter to the Parliament on the International Legal Order in Cyberspace*. The Hague, p. 7. [online] Available from: https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace [Accessed 4 February 2020].

[57] Judgment of 27 June 1986, *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)* (Merits), ICJ Reports 14, p. 117, paragraph 249; UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10, p. 132 (Commentary to Article 50, paragraph 5). [online] Available from: https://legal.un.org/ilc/texts/instrument/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

[58] Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, pp. 125–126, paragraph 12.

[59] UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10. Article 52(1)(b). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

[60] Op. cit., Article 52(2) notes: *"Notwithstanding paragraph 1 (b), the injured State may take such urgent countermeasures as are necessary to preserve its rights."*

The *Tallinn Manual 2.0* notes that

> *"if notification of intent to take a countermeasure would likely render that measure meaningless"*

there is also no requirement to notify. The Group of Experts argued that such a case, despite not being urgent *per se*, would be analogous to urgent countermeasures.[62] Also, the majority of experts rejected the existence of a requirement to offer negotiation before conducting the countermeasure.[63]

Another important aspect to bear in mind is the proportionality requirement as stipulated in Article 51 ILC Articles. It poses an "essential limit" for states wishing to react to an internationally wrongful act through countermeasures.[64] The proportionality requirement is particularly important to consider when a victim state is taking countermeasures against a state which has violated its due diligence obligation but did not itself commit the internationally wrongful act (concerning the debate whether the due diligence principle poses a legal obligation on states, see above). Article 51 ILC Articles clearly stipulates in this context that both the gravity of the act and the rights in question need to be taken into account when assessing which countermeasure would be proportionate to the act. Thus, the way a state is able to react to the violation of a state's obligation to act with due diligence obviously differs compared to a state's reaction to a violation of e.g. the prohibition of the use of force or intervention.

Closely linked to the proportionality requirement is the view of the legality of *collective* countermeasures. Estonia has recently voiced its opinion that it believes that states may also take such *collective*

---

[61] Ministère des Armées. (2019) *Droit International Appliqué Aux Operations Dans Le Cyberespace*. Paris, p. 8. [online] Available from: https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-du-ministere-des-armees/communique_la-france-s-engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international [Accessed 4 February 2020].

[62] See Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 120, para. 12.

[63] Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, pp. 120–121, para. 13.

[64] Cf. UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10, p. 134 (Commentary to Article 51, paragraph 1). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

countermeasures[65] – something the ILC Articles have left open to debate. France, to the contrary, notes that

> *"*[c]*ollective countermeasures are not authorised, which rules out the possibility of France taking such measures in response to an infringement of another State's rights."*[66]

The passage of the *Nicaragua* judgment cited above on the illegality of collective countermeasures involving the use of force may also point in a similar direction.[67] One could, however, interpret this statement as only relating to the question of use of force, while leaving the legality of collective countermeasures below the threshold of force unanswered. It also cannot be ruled out that states may agree on a new cyber-related rule which might allow collective countermeasures solely in the cyber context.

According to a statement made at the second substantive session of the OEWG in February 2020, Austria believes that the "severe cyber operation" targeting the country violated the rule of sovereignty and that a *"state may seek reparation under the law of state responsibility"* – if the act is attributable to a state.[68] Austria also noted that a

> *"target state may* […] *react through proportionate countermeasures"*.[69]

External sources revealed that a team of hackers managed to end the attacks within the IT system of the *Foreign Ministry* by putting the offending group in the "defensive".[70] Luckily, the hacking group only managed to get into the mail server and not into the intranet of the *Ministry*, making it easier

---

[65] Government of Estonia. (2019) *President of the Republic at the Opening of CyCon 2019*. Tallinn. [online] Available from: https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html [Accessed 20 August 2020].

[66] Ministère des Armées. (2019) *Droit International Appliqué Aux Operations Dans Le Cyberespace*. Paris, p. 7. [online] Available from: https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-du-ministere-des-armees/communique_la-france-s-engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international [Accessed 4 February 2020].

[67] Cf. Judgment of 27 June 1986, *Case Concerning Military and Paramilitary Activities in and Against Nicaragua* (*Nicaragua v. United States of America*) (Merits), ICJ Reports 14, para. 249.

[68] Government of Austria. (2020) *OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security: Statement by Austria on International Law*. New York, p. 1 (delivered on 11 February at the second substantive session of the OEWG).

[69] Ibid.

[70] Moechel, E. (2020) *Cyberhusarenstück Schlug Angreifer im Außenministerium.* [blog entry] 23 February. Radio FM4. Available from: https://fm4.orf.at/stories/2999042/ [Accessed 20 August 2020].

to kick the offenders out of the system.[71] Unfortunately, there is no further information as Austrian institutions declined to comment.[72] Based on the existing information, however, it can be assumed that the defence against the hacking group stayed below the use of force. It also seemed proportional and aimed at ceasing the initial wrongful conduct. There is, unfortunately, no information, whether the defenders had to intrude into the networks of another state or whether the defence stayed within the Austrian IT systems. If the latter case is true, the "hackback" by Austrian technicians could even have been a lawful retorsion and it could be assumed that Austria would have been capable to even go further than what it did.

To conclude, it is safe to say that there currently is an active debate about what states are allowed and not allowed to do when undertaking a "hackback" in the form of a countermeasure. But not only are there open questions with respect to countermeasures – also the traditional views on the right to self-defence raises new questions in the cyber context (even though the possibility to react in self-defence is very limited). Therefore, hackback as self-defence will be addressed in the next chapter.

4. HACKBACK AS SELF-DEFENCE

A "hackback" could also be a lawful exercise of the right of self-defence. The right of self-defence is enshrined in Article 51 UN Charter and states the following:

> *"Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security".*

This means that a lawful exercise of the right of self-defence must meet the following conditions:[73]

1. it must be a response to an armed attack;
2. the use of force, and the degree of force used, must be necessary and proportionate; and

[71] Ibid.

[72] Ibid.

[73] See Greenwood, C. (2011) Self-Defence. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law* (online edition), paragraph 8.

3. it must be reported to the *Security Council* and must cease when the *Security Council* has taken *"measures necessary to maintain international peace and security"*.

Another precondition that is, according to the present authors, implied is that of attribution to a state:[74] If a cyber operation reaches the threshold of an armed attack, the present authors argue that under current international law it would also be necessary to attribute the attack to a state in order to exercise the right to self-defence. While the ICJ has repeatedly found that only acts attributable to a state can constitute an armed attack, this view has been questioned by some scholars.[75] *Zemanek*, for example, argues that the ICJ would disregard resolutions adopted by the *Security Council* after the terrorist attacks of "9/11", especially resolutions *1368 (2001)* and *1373 (2001)*. According to *Zemanek*, these resolutions would implicitly recognize the terrorist attack as an "armed attack" in the sense of Article 51 UN Charter.[76]

However, the ICJ has since reiterated its position and stated that

> *"Article 51 of the Charter* […] *recognizes the existence of an inherent right of self-defence in the case of armed attack by one State against another State"*.[77]

In addition, the notion to extend the right to self-defence against non-state actors has been criticized within the literature.[78]

---

[74] See section 2.

[75] See Zemanek, K. (2013) Armed Attack. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law* (online edition), paragraph 15; Tsagourias, N. (2012) Cyber Attacks, Self-Defence and the Problem of Attribution. *Journal of Conflict and Security Law*, 17, p. 241.

[76] Zemanek, K. (2013) Armed Attack. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law* (online edition), paragraph 15; Judgment of 19 December 2005, *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)* (Separate Opinion Judge Simma), ICJ Reports 334, paragraph 11.

[77] Advisory Opinion of 9 July 2004, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, ICJ Reports 136, paragraph 139; see also Judgment of 19 December 2005, *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)* (Merits), ICJ Reports 168, paragraphs 146, 160.

[78] Gray, C. (2018) *International Law and the Use of Force*. 4th edition. Oxford: Oxford University Press, p. 210; Vidmar, J. (2017) The Use of Force as a Plea of Necessity. *American Journal of International Law Unbound*, 111, p. 302; see also Ministère des Armées. (2019) *Droit International Appliqué Aux Operations Dans Le Cyberespace*. Paris, p. 8. [online] Available from: https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-du-ministere-des-armees/communique_la-france-s-engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international [Accessed 4 February 2020]; see, however, Murphy, S. D. (2005) Self-Defense and the Israeli Wall Advisory Opinion: An Ipse Dixit from the ICJ?. *American Journal of International Law*, 99 (1).

As *Gray*, for example, points out, even if self-defence against non-state actors was permissible, it would still not allow a state to infringe the host state's rights.[79]

An armed attack constitutes a "use of force" within the meaning of Article 2(4) UN Charter. The ICJ stated in the *Nicaragua* case that "armed attacks" have to be distinguished as

> *"the most grave forms of the use of force from other less grave forms"*.[80]

Self-defence is permissible only in response to such armed attacks. The ICJ's original emphasis on differentiating an armed attack from a "mere frontier incident" has also been criticized in the literature.[81] However, the ICJ has since clarified that a single attack can also constitute an armed attack.[82] Nevertheless, it is obvious that not every use of force automatically justifies actions of self-defence.[83] To determine whether a use of force amounts to an armed attack, the ICJ considers the "scale and effects" of an attack.[84] The type of weapon used to reach the threshold of an attack is irrelevant: "armed attack" in the sense of Article 51 includes both kinetic and "cyber"weapons.[85]

According to *Constantinou*,

> "[an] *armed attack implies an act or the beginning of a series of acts of armed force of considerable magnitude and intensity (ie scale) which have as their consequence (ie effects) the infliction of substantial destruction upon important elements of the target State namely, upon its people, economic and security infrastructure, destruction of aspects of its governmental*

---

[79] See Gray, C. (2018) *International Law and the Use of Force*. 4th edition. Oxford: Oxford University Press, p. 210, with further references.

[80] Judgment of 27 June 1986, *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America*) (Merits), ICJ Reports 14.

[81] Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 341.

[82] Judgment of 6 November 2003, *Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America*) (Merits), ICJ Reports 161, paragraphs 57, 61; Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 342.

[83] Greenwood, C. (2011) Self-Defence. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law* (online edition), paragraph 12; Zemanek, K. (2013) Armed Attack. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law* (online edition), paragraph 7.

[84] Judgment of 27 June 1986, *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America*) (Merits), ICJ Reports 14, para. 195.

[85] Woltag, J. (2015) Cyber Warfare. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law* (online edition), paragraphs 8f.

> *authority, ie its political independence, as well as damage to or deprivation of its physical element namely, its territory".*[86]

While this definition (or other similar ones) could just as well be applied to cyber operations, the *Tallinn Group of Experts* could agree only to a very basic outline. According to them,

> *"a cyber operation that seriously injures or kills a number of persons or that causes significant damage to, or destruction of, property would satisfy the scale and effects requirement"*,

whereas

> *"acts of cyber intelligence gathering and cyber theft, as well as cyber operations that involve brief or periodic interruption of non-essential cyber services, do not qualify as armed attacks".*[87]

The *Tallinn Group of Experts* could, however, not agree on whether cyber operations can be considered "armed attacks" if they do not result in injury, death, damage, or destruction, but nonetheless have extensive negative effects.[88] It is generally difficult to determine the scale and effects of cyber operations, since cyber attacks do not always manifest in the "analogous" world and if they do, they only have an "indirect" impact.[89]

In view of the immense harm that a failure of "critical infrastructure" could potentially have, some focus on whether the target of the attack can be qualified as such, in order to assess whether an armed attack has occurred.[90] However, this is problematic for two reasons. First, there is no uniform definition of "critical infrastructure" and different understandings exist within each national legal framework. Second, the two concepts

---

[86] Constantinou, A. (2000) *The Right of Self-Defence under Customary International Law and Article 51 of the United Nations Charter*. Ant. N. Sakkoulas, p. 64; Zemanek, K. (2013) Armed Attack. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law*. (online edition), paragraph 9.

[87] Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 341.

[88] Op. cit., p. 342.

[89] Woltag, J. (2015) Cyber Warfare. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law* (online edition), paragraph 13.

[90] Ministère des Armées. (2019) *Droit International Appliqué Aux Operations Dans Le Cyberspace*. Paris. [online] Available from: https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-du-ministere-des-armees/communique_la-france-s-engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international [Accessed 4 February 2020].

of "critical infrastructure" and "armed attack" do not entirely correlate. The former issue could be solved in the near future. There are efforts within the European Union, for example, to harmonize the concept of critical infrastructure and measures that have to be taken to ensure their security. In this regard *Council Directive 2008/114/EC*[91] and the *Directive on Security of Network and Information Systems (NIS Directive)*[92] should be mentioned.

Council Directive 2008/114/EC defines critical infrastructure as

> *"an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions"*.[93]

This means that whether certain infrastructure can be considered "critical", depends on the individual circumstances of each Member State.

The NIS Directive especially concerns network security for "operators of essential services" and "digital service providers". Essential services are therein determined within specific economic sectors (e.g. energy, transport, health) as being essential for the maintenance of "critical societal and/or economic activities" and that an incident would have *"significant disruptive effects on the provision of that service"*.[94] In Austria, the NIS Directive has been implemented by the NIS Act.[95]

Regarding the latter issue (namely the fact that the two concepts of "armed attack" and "critical infrastructure" do not correlate): There are possible scenarios where a critical infrastructure is targeted, but where

---

[91] Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection. *Official Journal of the European Union* (2008/L-345/75), 23 December.

[92] 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. *Official Journal of the European Union* (2016/L-194/01) 19 July.

[93] Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection. *Official Journal of the European Union* (2008/L-345/75), 23 December. Article 2(a).

[94] Article 5(2) Directive 2016/1148/EU also requires the service to depend on network and informations systems, 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. *Official Journal of the European Union* (2016/L-194/01), 19 July.

[95] Federal Act on Ensuring a High Level of Security of Network and Information Systems 2018 (*Netz- und Informationssystemsicherheitsgesetz – NISG*) Austrian Federal Law Gazette I No. 111/2018.

the operation is not severe enough as to reach the scale and effects of an armed attack. On the other hand, a cyber attack that leads to the destruction of e.g. an apartment building (which does not constitute "critical infrastructure") could be considered to reach the threshold of an armed attack. This means that the use of the terms "critical infrastructure" or "essential service provider" could be more confusing than helpful in determining whether an armed attack has occurred.

Having said this, given the reportedly low scale and effect of the operation against the *Austrian Foreign Ministry* in January 2020, it can be ruled out that such a cyber operation amounted to an armed attack, even if the *Ministry* decided to classify such as a use of force and even though it falls within the scope of the NIS Act. It can, however, not be ruled out that a future attack could reach the threshold of an armed attack, especially if the cyber operation was aimed at destroying infrastructure or causing ("considerable") damage. In that case, it might be easier to argue for a right of self-defence if critical infrastructure, such as the *Austrian Foreign Ministry*, was the target.

We can therefore conclude that the cyber operation against the *Austrian Foreign Ministry* did not entitle Austria to "hackback" with a forceful strike in self-defence, as only "the most grave forms of the use of force"[96] are qualified as armed attacks. Even if – for some reason – it did, the attack would, in accordance with the ICJ case law, have to be attributed to a state in order to take measures of self-defence against the attacker without consent of the host state.

5. HACKBACK BASED ON THE PLEA OF NECESSITY

States may rely on the plea of necessity during a hackback, which is quite different from the other legal bases mentioned before (countermeasure, self--defence). The plea of necessity, as set forth in Article 25 of the ILC Articles, is not dependent on the prior conduct of the injured state.[97] In the authors' opinion, the most important difference to the two legal bases mentioned

[96] Judgment of 27 June 1986, *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America*) (Merits), ICJ Reports 14.

[97] UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10, p. 80 (Commentary to Article 25, paragraph 2). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020]: the "injured state" being the state against which measures on the basis of necessity are taken.

above is that no attribution to a state is required.[98] It "merely" suffices that the danger emanates from that state's territory. This section will elaborate on the extent to which a plea of necessity allows a hackback.

For a state to be able to invoke necessity, the conditions – narrowly defined in Article 25[99] – must be met. These are (1) the grave danger either to the essential interests of the state or of the international community as a whole and (2) that the conduct in question does not seriously impair an essential interest of the state or states towards which the obligation exists, or of the international community as a whole.[100]

Even if these conditions are met, necessity may not be invoked by a state as a ground for precluding wrongfulness if (a) the international obligation in question excludes the possibility of invoking necessity; or (b) the State has contributed to the situation of necessity.[101]

In the Commentary to the ILC Articles, the ILC cited various decisions and cases in which the plea of necessity was put forward (or its existence at least not denied) as justification for the fact that the plea of necessity is part of the applicable customary international law (*lex lata*).[102] Even though critical voices in the literature have argued that Article 25 of the ILC Articles should have been seen to be merely an aid to orientation and should not have been adopted verbatim,[103] it cannot be denied that the concept of necessity exists in customary international law. On the other hand, it is

---

[98] Ibid. See also Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, Rule 25, paragraph 10; Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*, 95, p. 1621; note, as already highlighted above, that some scholars argue that attribution is also not required for the exercise of self-defence.

[99] UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10, p. 80 (Commentary to Article 25, paragraph 1). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

[100] Op. cit., Article 25(1); on necessity and its applicability in a cyber context see also: Vidmar, J. (2017) The Use of Force as a Plea of Necessity. *American Journal of International Law Unbound*, 111, p. 302; Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*, 95, p. 1619; Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, Rule 26.

[101] Op. cit., Article 25(2).

[102] Op. cit. pp. 80ff (Commentary to Article 25, paragraphs 3ff).

[103] Sloane, R. D. (2012) On the Use and Abuse of Necessity in the Law of State Responsibility. *American Journal of International Law*, 106 (3), p. 447; see also Schaller, C. (2017) Beyond Self--Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*, 95, p. 1630 [questioning state practice regarding the requirement *"that the action must not seriously impair the essential interests of other States"*].

also apparent that the precise nature and scope of the plea of necessity remain controversial.[104]

What amounts to an "essential interest" is not unilaterally defined and therefore vague.[105] According to the ILC, the extent to which a given interest is "essential" depends on all the circumstances and therefore cannot be prejudged. It extends to particular interests of the state and its people, as well as of the international community as a whole.[106]

As has been elaborated in the context of self-defence (see above), the designation of certain parts of a state's infrastructure as "critical infrastructure" might be suggestive of their characterisation of an interest as essential, but not determinative.[107] *Schaller* argues that an essential interest within the meaning of Article 25 and Rule 26 of the *Tallinn Manual* should not be narrowed down solely to the concept of critical infrastructure.[108] As the *Tallinn Group of Experts* agreed, an essential interest

> *"is most clearly implicated when critical infrastructure is targeted in a manner that may have a severe negative impact on a state's security, economy, public health, safety, or environment"*.[109]

Similar to the determination whether a cyber operation reaches the threshold of an armed attack, the involvement of critical infrastructure can be an indicative but not a decisive factor in determining if essential interests are in danger.

---

[104] UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10, p. 83 (Commentary to Article 25, paragraph 13). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020]; Schaller, C. (2017) Beyond Self--Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*, 95, p. 1636 [who promotes a necessity regime for cyber incidents, because the *"contours of the concept of necessity as applied in the cyber context are not yet sufficiently clear to dispel concerns* [of their abuse]*"*].

[105] Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, Rule 26, paragraph 2.

[106] UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10, p. 83 (Commentary to Article 25, paragraph 15). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

[107] Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, Rule 26, paragraph 2.

[108] Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*, 95, p. 1632.

[109] Schmitt, M. and Vihul, L. (eds.) (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, Rule 26, paragraph 5.

Similar to self-defence, however, focusing on the term "critical infrastructure" could lead to some confusion (see above). Particularly with regard to necessity, one has to be aware of circular reasoning. Since critical infrastructure is defined as concerning vital or essential interests of the state and/or the public and that damage of this infrastructure could seriously harm these interests, one cannot argue that there is a state of necessity just on the basis that a cyber operation is targeting critical infrastructure.

The examples given in the *Tallinn Manual* illustrate (according to most of the experts) situations in which essential interests are gravely and imminently threatened. Such situations would include

> *"a cyber-operation that would debilitate the State's banking system, cause a dramatic loss of confidence in its stock market, ground flights nation-wide, halt all rail traffic, stop national pension and other social benefits, alter national health records in a manner endangering the health of the population, cause a major environmental disaster, shut down a large electrical grid, seriously disrupt the national food distribution network, or shut down the integrated air defence system would provide the basis for the application of this rule"*.[110]

To invoke the plea of necessity, such essential interests of a State must face a grave and imminent peril. A peril can, in accordance with the expert group of the *Tallinn Manual*, be seen as "grave", when the threat is especially severe, if the interest is interfered with in a fundamental way, like destroying the interest or rendering it largely dysfunctional.[111]

With regard to the "imminence" of such peril, the Commentary to the ILC Articles states that such imminence must be

> *"objectively established and not merely apprehended as possible"*,[112]

and the decision that measures must be taken must be

---

[110] Ibid.

[111] Op. cit., Article 25, paragraph 4.

[112] UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10, p. 83 (Commentary to Article 25, paragraph 15). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

> *"clearly established on the basis of the evidence reasonably available at the time".*[113]

It should not be understood solely as a temporal issue.

The *Tallinn Group of Experts* agreed that peril should always be imminent when the "last window of opportunity" to take action to prevent it is about to close.[114] The last window of opportunity is familiar from the debate surrounding the right to anticipatory self-defence.[115] There, it is argued that

> *"restrictive approaches to imminency run counter to the purposes animating the right of self-defence"*[116]

and that

> *"the correct standard for evaluating a preemptive operation must be whether or not it occurred during the last possible window of opportunity in the face of an attack that was almost certainly going to occur".*[117]

One has to keep in mind that this last window of opportunity standard would generally provide States with considerable leeway for action whether invoking the right to self-defence or the plea of necessity.[118] From its meaning, the "last window of opportunity" standard should rather be applied to test whether a certain measure is "the only way" to protect essential interests from a grave and imminent peril, than to test if that peril is "imminent".

In conclusion, reacting based on necessity remains an exceptional measure.[119] Therefore, the wrongfulness of measures can only be precluded on the basis of necessity, if they are – based on reasonable certainty[120] – the only way for a state to safeguard essential interests from a grave and imminent danger. When determining essential interests, states will most

---

[113] Op. cit., p. 83 (Commentary to Article 25, paragraph 16).

[114] Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 139.

[115] Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*, 95, p. 1635.

[116] Schmitt, M. N. (2003) Preemptive Strategies in International Law. *Michigan Journal of International Law*, 24 (2), p. 534; see also references in Schaller, C. (2017) Beyond Self--Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*, 95, pp. 1619, 1635 (fn. 115).

[117] Schmitt, M. N. (2003) Preemptive Strategies in International Law. *Michigan Journal of International Law*, 24 (2), p. 535.

[118] Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*, 95, p. 1635.

likely resort to their definition of critical infrastructure, although it should be kept in mind that necessity is not restricted to critical infrastructure. In addition, the main focus should be to determine 1) if it is a "grave peril" that threatens essential interests and 2) if other measures (e.g. [cyber] diplomacy) that do not affect the rights of other states could be taken (arg. "the only way"). The present authors argue, however, that if a peril to an essential interest is imminent, there might be a lower standard with regard to what is reasonable to expect on the "gravity" of the attack if the window of opportunity is about to close (e.g. in the moment before a malware is inserted to or data is extracted from a critical system).

So even though the recent cyber operation was directed against the *Austrian Foreign Ministry* (and therefore, arguably, against a critical infrastructure) it would not allow Austria to react out of necessity. Only if essential interests (like water supply, power supply or general matters of internal security) are threatened in a way that would render them largely dysfunctional would it be permissible to invoke necessity. Therefore, not every cyber operation against networks of critical infrastructure allows for measures taken in necessity, but only those attacks that also threaten the essential interest that such infrastructure is "critical" to maintain. In other words: This exceptional rule should rather apply in cases like an imminent power outage ("black-out") or other events with grave consequences that similarly effect essential interests of the state and/or the population.

6. CONCLUSION

This contribution has demonstrated that international law allows certain ways to react to malicious cyber operations. States can either react through

[119] Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, Rule 26, paragraph 17; UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10, p. 80 (Commentary to Article 25, paragraph 1). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

[120] Schmitt, M. and Vihul, L. (eds.) (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, Rule 26, paragraph 14; UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10, p. 83 (Commentary to Article 25, paragraph 16). [online] Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

countermeasures, self-defence or out of necessity. The purpose of this contribution was to elaborate on these three ways in more detail.

Austrian news reports and press releases suggest that the cyber operation against the *Austrian Foreign Ministry* did not cause major damage. Thus, it most likely cannot be classified as a use of force according to Article 2(4) UN Charter, but it might be severe enough to constitute a violation of Austria's sovereignty. Austria has remained silent as to the territorial origins of the operation. However, in case the whereabouts are known, it could also be argued that the host state, from which the operation originated – acted in violation of the due diligence principle. In these cases, Austria would be permitted to take countermeasures against the state to which the wrongful conduct (in the former instance) or the negligence (in the latter instance) could be attributed. Such countermeasures could be any type of activity aimed at ceasing the wrongful conduct, as long as it does not amount to force and is necessary and proportionate.

Given the low-level nature of the cyber operation, the possibility to act in self-defence or out of necessity seems out of question. However, it cannot be ruled out that Austria (or any other state) may be able to rely on these measures in case it will be the target of a more severe cyber operation in the future.

To conclude, even when applying a more "traditional" approach by applying existing customary international law as expressed in the ILC Articles and by ICJ case law, many questions as to what the concrete response options are, remain. These questions will likely only be solved if more states come forward with their national views about how international law applies to cyber operations. With its press releases and statements at UN level, Austria finally entered this discussion. There is no doubt that the cyber operation against the *Foreign Ministry* has acted as a stimulus for this debate.

LIST OF REFERENCES

[1] Advisory Opinion of 9 July 2004. *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory.* ICJ Reports 2004, 136.

[2] Antonopoulos, C. (2015) State Responsibility in Cyberspace. In: Nicholas Tsagourias and Russell Buchan (eds.). *Research Handbook on International Law and Cyberspace.* Cheltenham and Northampton: Edward Elgar Publishing.

[3] Austrian Federal Ministry for European and International Affairs. (2020) *Cyber Attack on the Foreign Ministry is Over.* [press release] 13 February. Available from: www.bmeia.gv.at/en/the-ministry/press/announcements/2020/02/cyber-attack-on-the-foreign-ministry-is-over/ [Accessed 19 August 2020].

[4] Austrian Press Agency. (2020) *Schwerwiegender Angriff auf IT-Systeme des Außenministeriums.* [press release] 4 January. Available from: https://www.ots.at/presseaussendung/OTS_20200104_OTS0020/schwerwiegender-angriff-auf-it-systeme-des-aussenministeriums [Accessed 19 August 2020].

[5] Award of 4 April 1928. *Island of Palmas Case (Netherlands v. United States of America).* Reports of International Arbitral Awards, United Nations, Vol. II.

[6] Bannelier-Christakis, K. (2014) Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?. *Baltic Yearbook of International Law*, 14.

[7] Brunner, I., Dobric, M. and Pirker, V. (2019) Proving a State's Involvement in a Cyber--Attack: Evidentiary Standards Before the ICJ. *Finnish Yearbook of International Law*, 25.

[8] Charter of the United Nations and Statute of the International Court of Justice, 26 June 1945 (1 UNTS XVI).

[9] Clark, D. D. and Landau, S. (2011) Untangling Attribution. *Harvard National Security Journal*, 2.

[10] Constantinou, A. (2000) *The Right of Self-Defence under Customary International Law and Article 51 of the United Nations Charter*. Ant. N. Sakkoulas.

[11] Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection. *Official Journal of the European Union* (2008/L-345/75), 23 December.

[12] Dinniss, H. (2014) *Cyber Warfare and the Laws of War*. Cambridge: Cambridge University Press.

[13] 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. *Official Journal of the European Union* (2016/L-194/01) 19 July.

[14] Federal Act on Ensuring a High Level of Security of Network and Information Systems 2018 *(Netz- und Informationssystemsicherheitsgesetz – NISG)* Austrian Federal Law Gazette I No. 111/2018.

[15] Government of Austria. (2020) *Austrian Statement on Rules, Norms and Principles for Responsible State Behaviour* (delivered on 17 June at the Informal OEWG June Consultations).

[16] Government of Austria. (2020) *OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security: Statement by Austria on International Law*. New York (delivered on 11 February at the second substantive session of the OEWG).

[17] Government of Estonia. (2019) *President of the Republic at the Opening of CyCon 2019*. Tallinn. [online] Available from: https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html [Accessed 20 August 2020].

[18] Government of the Netherlands. (2019) *Appendix to the Letter to the Parliament on the International Legal Order in Cyberspace*. The Hague. [online] Available from: https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace [Accessed 4 February 2020].

[19] Gray, C. (2018) *International Law and the Use of Force*. 4th ed. Oxford: Oxford University Press.

[20] Greenwood, C. (2011) Self-Defence. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law.* Online ed.

[21] Guitton, C. (2017) *Inside the Enemy's Computer: Identifying Cyber-Attackers.* London: Hurst & Company.

[22] Henriksen, A. (2015) Lawful State Responses to Low-Level Cyber-Attacks. *Nordic Journal of International Law*, 84 (2).

[23] Judgment of 9 April 1949. *Corfu Channel (United Kingdom v. Albania).* ICJ Reports 1949, 4.

[24] Judgment of 27 June 1986. *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)*. ICJ Reports 1989, 14.

[25] Judgment of 6 November 2003. *Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America).* ICJ Reports 2003, 161.

[26] Judgment of 19 December 2005. *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda).* ICJ Reports 2005, 334.

[27] Koivurova, T. (2010) Due Diligence. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law.* Online ed.

[28] Kolb, R. (2015) Reflections on Due Diligence Duties and Cyberspace. *German Yearbook of International Law*, 58.

[29] Ministère des Armées. (2019) *Droit International Appliqué Aux Operations Dans Le Cyberespace*. Paris. [online] Available from: https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-du-ministere-des-armees/communique_la-france-s-

engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international [Accessed 4 February 2020].

[30] Moechel, E. (2020) *Cyberhusarenstück Schlug Angreifer im Außenministerium*. [blog entry] 23 February. Radio FM4. Available from: https://fm4.orf.at/stories/2999042/ [Accessed 20 August 2020].

[31] Moechel. E. (2020) *Vorläufige Bilanz des Cyberangriffs auf das Außenministerium.* [blog entry] 16 February. Radio FM4. Available from: https://fm4.orf.at/stories/2998771/ [Accessed 20 August 2020].

[32] Murphy, S. D. (2005) Self-Defense and the Israeli Wall Advisory Opinion: An Ipse Dixit from the ICJ?. *American Journal of International Law*, 99 (1).

[33] Roscini, M. (2014) *Cyber Operations and the Use of Force.* Oxford: Oxford University Press.

[34] Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*, 95.

[35] Schmitt, M. (2003) Preemptive Strategies in International Law. *Michigan Journal of International Law*, 24 (2).

[36] Schmitt, M. (2014) "Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law. *Virginia Journal of International Law,* 54.

[37] Schmitt, M. (ed.). (2013) *The Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge: Cambridge University Press.

[38] Schmitt, M. (2015) In Defense of Due Diligence in Cyberspace. *The Yale Law Journal Forum*, 125.

[39] Schmitt, M. and Vihul, L. (eds.). (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge: Cambridge University Press.

[40] Schmitt, M. (2020) *Cyber Operations Against Vaccine R & D: Key International Law Prohibitions and Obligations*. [blog entry] 10 August. EJIL:Talk!. Available from: www.ejiltalk.org/cyber-operations-against-vaccine-r-d-key-international-law-prohibitions-and-obligations/ [Accessed 20 August 2020].

[41] Shackelford, S. J., and Andres, R. B. (2011) State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. *Georgetown Journal of International Law*, 42.

[42] Sloane, R. D. (2012) On the Use and Abuse of Necessity in the Law of State Responsibility. *American Journal of International Law,* 106 (3).

[43] Tsagourias, N. (2012) Cyber Attacks, Self-Defence and the Problem of Attribution. *Journal of Conflict and Security Law*, 17.

[44] United Nations General Assembly. (2013) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General*. UN Doc A/68/98. New York: United Nations. Available from: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf?OpenElement [Accessed 20 August 2020].

[45] United Nations General Assembly. (2014) *Developments in the Field of Information and Telecommunications in the Context of International Security.* UN Doc A/RES/68/243. New York: United Nations. Available from: https://undocs.org/A/RES/68/243 [Accessed 20 August 2020].

[46] United Nations General Assembly. (2015) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General*. UN GAOR 70th Session, Item 93, UN Doc A/70/174. New York: United Nations. Available from: https://undocs.org/A/70/174 [Accessed 20 August 2020].

[47] UN International Law Commission. (2001) *Report of the International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. UN GAOR, 53rd Sess., Supp. No. 10, UN Doc. A/56/10. Available from: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 20 August 2020].

[48] Vidmar, J. (2017) The Use of Force as a Plea of Necessity. *AJIL Unbound*, 111.

[49] Woltag, J. (2015) Cyber Warfare. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law.* Online ed.

[50] Wright, J. (2018) *Cyber and International Law in the 21st Century.* London. [online] Available from: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century [Accessed 20 August 2020].

[51] Zemanek, K. (2013) Armed Attack. In: Rüdiger Wolfrum (ed.). *Max Planck Encyclopedia of Public International Law.* Online ed.

DOI 10.5817/MUJLT2020-2-5

MISUSE OF CONTACTLESS PAYMENT CARDS WITH RADIO-FREQUENCY IDENTIFICATION

by

LIBOR KLIMEK*

Counterfeiting of means of payment is one of European crimes. The Treaty on the Functioning of the European Union lists counterfeiting of means of payment as one of the areas of particularly serious crime with a cross-border dimension. At the European Union level a brand-new legislative instrument harmonising counterfeiting of means of payment has been adopted – the Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment. This Directive establishes minimum rules concerning the definition of criminal offences and sanctions in the areas of fraud and counterfeiting of non-cash means of payment. Moreover, it facilitates the prevention of such offences, and the provision of assistance to and support for victims. The Directive is addressed to the Member States of the European Union. They shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 31st May 2021.

The contribution deals with criminalisation of the misuse of contactless payment cards with Radio-Frequency Identification (RFID) technology. It is divided into three sections. The first section focuses on definition of Radio--Frequency Identification and payment cards with Radio-Frequency Identification. The second section focuses in detail on a new European Union approach to combat counterfeiting of means of payment addressed to its Member States – i.e. the Directive (EU) 2019/713 on combating fraud and counterfeiting of non--cash means of payment. The last third section is focused on non-legislative prevention possibilities.

* libor.klimek@umb.sk, Associate Professor at the Department of Criminal Law, director of the Criminology and Criminalistics Research Centre at the Faculty of Law, Matej Bel University in Banská Bystrica, Slovak Republic. Visiting Professor at the Faculty of Law, Leipzig University, Germany. Advisor of the Constitutional Court of the Slovak Republic.

KEY WORDS

Criminal Offences, Criminalisation, Directive (EU) 2019/713 on Combating Fraud and Counterfeiting of Non-Cash Means of Payment, Payment Cards with Radio--Frequency Identification, Prevention, Radio-Frequency Identification (RFID), Sanctions

1. INTRODUCTION

Payment cards have become very popular among people. Moreover, contactless payments by payments cards, introduced in 2007, have become popular as well. These days one in three card payments is contactless. Contactless payments are payments made by waving or tapping such card over a reader, which accepts the payment (if there are no barriers, for example, if payment limit of card is exceeded or if the validity of card has expired).

Payment cards have a chip inside them that recognises radio waves, if a card holder wishes to pay contactless. It is based on *Radio-Frequency Identification technology* – known as *RFID*. On the one hand, such a payment method is very useful method in case of small payments, for example, payments up to 20 EUR. On the other hand, there are many ways to misuse cards. In October 2016 the *Daily Mail*[1] revealed that criminals can swipe money off RFID cards – i.e. payment cards using contactless payments – as people are walking down the street, sitting in a restaurant or browsing in shops.

2. RADIO-FREQUENCY IDENTIFICATION AND PAYMENT CARDS WITH RFID

RFID uses wireless communication to establish the identity of a physical object. Automatic identification is the primary functionality provided by RFID technology, enabling recognition of tagged objects. Consequently, RFID tagged objects or persons can be easily recognised.[2] RFID is a system that transmits the identity of an object wirelessly, using radio waves. RFID tag is attached to an object and contains information about it.

---

[1] Could you fall prey to a contactless conman? How thieves can take money from your card as you're walking down the street. [online] Available from: https://www.dailymail.co.uk/news/article-3849368/Could-fall-prey-contactless-conman-thieves-money-card-walking-street.html [Accessed 18 October 2016].

[2] Ahson, S. A., Ilyas, M. (2008) *RFID Handbook: Applications, Technology, Security, and Privacy*. Boca Raton: CRC Press, p. 644.

Since the recent past RFID is understood as advanced automatic identification technology.[3] The basic technologies for RFID have been around for long time. Its root can be traced back to an espionage device designed in 1954 by *Léon Theremin* (*Lev Sergeyevich Termen*, Russian: *Лев Сергеевич Термéн*) of the Soviet Union, which retransmitted incident radio waves modulated with audio information.[4]

There are several versions of RFID that operate at different radio frequencies. Three primary frequency bands are used for RFID:

- *Low-Frequency* – 125/134 Khz – most commonly used for attendance and access control;
- *High-Frequency* – 13,56 MHz – used where medium data rate and read ranges up to about 1,5 meters are acceptable; it is used in case of contactless payment cards; and
- *Ultra-High-Frequency* – 850 to 950 MHz – offers the longest read ranges of up to approximately 3 meters and high reading speeds.

These days we use payment cards (also known as, for example, bank cards, ATM cards, client cards or cash cards). The most common payments cards are *debit cards*[5] and *credit cards*[6], provided by, for example, *Visa*, *Mastercard* or *Maestro*. They offer also contactless payments, since they have a small microchip inside that is capable of emitting radio waves. The antenna and chip are both built into the plastic. Such contactless cards operate at only a short range – 1–5 centimetres (or more) and work on RFID technology.

---

[3] Nof, S. Y. (2009) *Springer Handbook of Automation*. Berlin – Heidelberg: Springer, p. 865; Han, Z., Xu, Y., Wang, R. (2014) The Summarize of Medium Access Control Protocol in RFID. In: Xue Wang, Li Cui, Zhongwen Guo (eds.). *Advanced Technologies in Ad Hoc and Sensor Networks: Proceedings of the 7th China Conference on Wireless Sensor Networks*. Heidelberg – New York – Dordrecht – London, Springer, p. 336.

[4] Qiao, Y., Chen, S., Li, T. (2012) *RFID as an Infrastructure*. New York – Heidelberg – Dordrecht – London: Springer, p. 1.

[5] A *debit card* is a payment card made of plastic that contains chips. It is commonly used instead of cash in order to make payment(s). The money is transferred directly from the cardholder's bank account to merchant's bank account.

[6] A *credit card* is a payment card made of plastic that contains chips. It is commonly used instead of cash in order to make payment(s). It enables the cardholder to pay a merchant based on the cardholder's promise to the card issuer to pay for the amounts (plus the other agreed financial charges). The card issuer creates a revolving account and grants a line of credit to the cardholder. It means that the money is not transferred directly from the cardholder's bank account to merchant's bank account, but the cardholder "borrows" money for payment(s) in order to pay a merchant.

To pay with a contactless payment card, for example, in a supermarket or in a restaurant, the customer holds their card near to the reader, i.e. RFID reader. Consequently, the reader can communicate with the card's microchip. Further, the reader sends to the card the details regarding transaction, the card sends back the payment details and then the payment processor processes the contactless payment. Such understanding of using contactless payments can be illustrated in the more expanded series of events:[7]

- the RFID reader establishes a connection with the card;
- the RFID reader sends the card an encryption key;
- the card decrypts the encryption key, which allows all future communication to be encrypted using that key;
- the card reader sends the card the proposed transaction;
- the card creates a transaction document, including payment details;
- the card "signs" the transaction document using its private key;
- the card sends the transaction document to the card reader; and
- the card reader sends a receipt to the card.

The very first advantage of RFID technology is that it is convenient method of payment. An RFID reader sends needed information to the card. Card holder does not need to know all details of payment(s). This allows faster processing of payments. In general, unlike *bar code readers*[8] or *QR code readers*[9] that can only scan a single code at once, RFID readers are able to communicate with multiple tags at once.

RFID chips are small enough that they could be placed in payment card. Indeed, the card holder on the first touch does not know that the card has extra chip inside. These days the payment cards include such a chip quite commonly. Such a chip is placed commonly on the corner of the card, what is indicated by special symbol on the card.

---

[7] How Do RFID Contactless Payments Work? [online] Available from: https://www.cards witcher.co.uk/2019/03/rfid-contactless-payments/ [Accessed 8 November 2019].

[8] A *bar code* is a method of representing data in a visual form, which is machine-readable. It was invented in the United States of America in 1951. Today, bar codes are used in many contexts, especially when shopping. They are pre-printed on most items in shops. This speed up processing at check-outs.

[9] A *QR code* – abbreviated from *Quick Response code* – is a label, which is machine-readable, that contains information about the item to which it is attached. It was first designed in 1994 in Japan. The QR system became popular due to its fast readability and greater storage capacity compared to bar code.

RFID technology allows real-time usage of payments. If the card is close RFID reader, the payment does not require more than a few seconds. It is faster than using payment with PIN (personal identification number) and much faster than payment by cash. The reason is that it is not needed to calculate the value of banknotes and coins before payment.

As seen, the advantages of using RFID technology are persuasive. On the other hand, it is important to note that RFID technology has disadvantages as well.

It is easy to misuse RFID chip in payment card. Anyone with a fake RFID scanner, even homemade scanner, can "send" signal. That means that anyone with a scanner can walk down the street and "scan" cards of people without realising it. Of course, PIN technology can reduce such danger, but it is not always working. Many cards using RFID technology have set limits for automatic approvals of payments, for example, up to 20 EUR.

Any wireless or contactless technology has the chance to be hacked, including RFID. If it is for payment purposes, it could create an identity theft issue. RFID readers could record the data of the card without permission of the card holder. If information is "stolen", RFID chips are very easy to clone and to be counterfeited.

RFID identity theft, sometimes called *RFID skimming*[10], occurred. Like most technologies and networks, RFID systems are also vulnerable to physical and electronic attacks, namely reverse engineering, power analysis, eavesdropping, sniffing, denial of service, cloning, spoofing and viruses. As this technology matures and finds numerous applications, hackers will continue to seek novel methods to access private information, infiltrate secure networks, and take the system down for their own gains.[11]

It should be noted that, fraud on contactless payment cards remains low. Available data are from the United Kingdom, for example. According to *UK Finance*[12] fraud using the contactless technology on payment cards and

[10] See, for example: Walker, M. (2019) *CEH Certified Ethical Hacker All-in-One Exam Guide*. 4th ed. New York: McGraw Hill Professional, p. 430; Fernándes-Caramés, T. M., Fraga--Lamas, P., Suárez-Albera, M., Castedo, L. (2017) A Methodology for Evaluating Security in Commercial. In: Paulo Crepaldi, Tales Pimenta (eds.). *Radio Frequency Identification*. Rijeka: InTech, p. 39.

[11] What Is RFID Skimming? [online] Available from: https://www.tripwire.com/state-of-security/featured/what-rfid-skimming/ [Accessed 8 November 2019].

[12] *UK Finance* is the collective voice for the banking and finance industry. Representing more than 250 firms across the industry, it seeks to enhance competitiveness, support customers and facilitate innovation. The Economic Crime team within *UK Finance* is responsible for leading the industry's collective fight against economic crime in the United Kingdom, including fraud, anti-money laundering, sanctions, anti-bribery, corruption and cybercrime.

devices remains low, with 19,5 million GBP of losses during 2018, compared to spending of 69 billion GBP over the same period. This is equivalent to 2,7p in every 100 GBP spent using contactless technology, the same level recorded in 2016 and 2017. Fraud using the contactless technology on payment cards and devices represents just 2,9 % of overall card fraud losses.[13]

3. EUROPEAN UNION APPROACH TO COMBAT COUNTERFEITING OF MEANS OF PAYMENT

3.1. COUNTERFEITING OF MEANS OF PAYMENT AS EUROPEAN CRIME

The general policy objective of the European Union is to ensure a high level of security through measures to prevent and combat crime.[14] At the European Union level some of criminal offences are considered as European crimes or so-called Euro crimes[15] (in literature there can be observed also the terms Euro-crimes[16] and Eurocrimes[17]).

Specific offences are recognised as offences which are within the legislative competence of the European Union. The *Treaty on the Functioning of the European Union* lists *counterfeiting of means of payment* as one of the areas of particularly serious crime with a cross--border dimension. It stipulates that

> *"*[t]*he European Parliament and the Council* [of the European Union] *may, by means of* directives *adopted in accordance with the ordinary*

[13] UK Finance. (2019) *Fraud the Facts 2019: The definitive overview of payment industry fraud*, p. 23. [online] Available from: https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202019%20-%20FINAL%20ONLINE.pdf [Accessed 8 November 2019].

[14] Article 67(3) of the Treaty on the Functioning of the European Union as amended by the Treaty of Lisbon. 26 October 2012 (C 326/47). Available from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:EN:PDF [Accessed 8 November 2019].

[15] It should be noted that the *Treaty on the Functioning of the European Union* does not use the wording *Euro crimes*. It is used by the *European Commission* – see: European Commission. (2011) *Towards an EU Criminal Policy: Ensuring the effective implementation of EU policies through criminal law*. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2011) 573 final, p. 5. Available from: https://db.eurocrim.org/db/en/doc/1626.pdf. [Accessed 8 November 2019].

[16] See: Cools, M. et al. (2009) *Readings on Criminal Justice, Criminal Law & Policing*. Antwerpen – Apeldoorn: Maklu, p. 100; Miettinen, S. (2013) Criminal Law and Policy in the European Union. Abingdon – New York: Routledge, p. 145; Body-Gendrot, S. et al. (2014) *The Routledge Handbook of European Criminology*. Abingdon – New York: Routledge, p. 65; Chalmers, D., Davies, G., Monti, G. (2014) *European Union Law*. 3rd ed. Cambridge: Cambridge University Press, p. 657.

[17] See: Klip, A. (2012) *European Criminal Law: An Integrative Approach*. 2nd ed. Cambridge – Antwerp – Portland: Intersentia, p. 211.

> *legislative procedure, establish minimum rules concerning the* definition of criminal offences and sanctions *in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis. These areas of crime are the following: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption,* counterfeiting of means of payment, *computer crime and organised crime* […]"[18] (emphasis added).

It should be noted that the *United Nations* and the *Council of Europe* have introduced conventions harmonising almost all of European crimes, generally even before the EU. Thus, taking into account legislation of the European Union and the conventions of the *United Nations* and the *Council of Europe*, one could observe "double criminalising" or even "triple criminalising" of some offences.

Within the European Union have been adopted legislative instruments regulating European crimes. There is no need to introduce their in-depth analysis, since this article is focused on *counterfeiting of means of payment*. The text below analyses the leading legislative instrument harmonising counterfeiting of means of payment – the Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment.

3.2. DEFINITION OF CRIMINAL OFFENCES AND SANCTIONS: DIRECTIVE (EU) 2019/713

At the European Union level the leading legislative instrument harmonising counterfeiting of means of payment is the *Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment*[19] (hereinafter referred to as "Directive (EU) 2019/713"). This Directive establishes minimum rules concerning the definition of criminal offences and sanctions in the areas of fraud and counterfeiting of non-cash means

[18] Article 83(1) of the Treaty on the Functioning of the European Union as amended by the Treaty of Lisbon. 26 October 2012 (C 326/47). Available from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:EN:PDF [Accessed 8 November 2019].

[19] Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA. *Official Journal of the European Union* (L 123/18) 10 May. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0713&from=EN [Accessed 8 November 2019].

of payment. Moreover, it facilitates the prevention of such offences, and the provision of assistance to and support for victims.[20]

The Directive (EU) 2019/713 repealed its predecessor – the Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment.[21] It no longer reflected today's realities and insufficiently addresses new challenges and technological developments such as virtual currencies and mobile payments.[22] It was adopted in 2001, however, in 2013, fraud using cards issued in the *Single European Payment Area (SEPA)* reached 1,44 billion EUR, representing growth of 8 % on the previous year. An evaluation of the Framework Decision 2001/413/JHA identified three main problems that were driving the current situation concerning non-cash payment fraud in the European Union. First, some crimes could not be effectively investigated and prosecuted. Second, some crimes could not be effectively investigated and prosecuted due to operational obstacles. Third, criminals took advantage of gaps in prevention to commit fraud.[23] The *European Commission* introduced a proposal for a new legislation[24] addressed to the Member States of the European Union. It introduced three specific objectives that addressed the problems identified. First, to ensure that a clear, robust and technology neutral policy/legal framework is in place. Second, to eliminate operational obstacles that hamper investigation and prosecution and. Third, to enhance prevention.

---

[20] Article 1 of the Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment.

[21] Council Framework Decision 2001/413/JHA of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment. *Official Journal of the European Communities* (L 149/1) 2 July. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32001F0413 [Accessed 8 November 2019].

[22] See: Funta, R. (2019) *Úvod do počítačového práva*. Brno, MSD, p. 67 *et seq.*; Ivor, J., Polák, P., Záhora, J. (2017) *Trestné právo hmotné II: Osobitná časť*. Bratislava: Wolters Kluwer, p. 212.

[23] For details see: European Commission. (2017) *Proposal for a Directive of the European Parliament and of the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA*, COM(2017) 489 final. Available from: https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-489-F1-EN-MAIN-PART-1.PDF [Accessed 8 November 2019]; European Commission. (2017) *Impact assessment accompanying the Proposal for a Directive of the European Parliament and the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, Commission staff working document*, SWD(2017) 298 final. Available from: https://ec.europa.eu/transparency/regdoc/rep/10102/2017/EN/SWD-2017-298-F1-EN-MAIN-PART-1.PDF [Accessed 8 November 2019].

[24] European Commission. (2017) *Proposal for a Directive of the European Parliament and of the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA*, COM(2017) 489 final. Available from: https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-489-F1-EN-MAIN-PART-1.PDF [Accessed 8 November 2019].

As seen, the Directive (EU) 2019/713 is addressed to the Member States of the European Union. They shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 31st May 2021.

The Directive (EU) 2019/713 contains own legal definitions. For the purpose of the Directive, non-cash payment instrument shall mean a non-corporeal or corporeal protected device, object or record, or a combination thereof, other than legal tender, and which, alone or in conjunction with a procedure or a set of procedures, enables the holder or user to transfer money or monetary value, including through digital means of exchange.[25]

3.3. CRIMINAL OFFENCES

The Directive (EU) 2019/713 obliges the Member States of the European Union to introduce specific provisions into their criminal law or to modify existing provisions in this field. It establishes as criminal offences a number of acts committed intentionally, namely:

- fraudulent use of non-cash payment instruments;
- offences related to the fraudulent use of corporeal non-cash payment instruments;
- offences related to the fraudulent use of non-corporeal non-cash payment instruments; and
- fraud related to information systems.

As regards the misuse of contactless payment cards, relevant is the first group of above-mentioned offences, i.e. *fraudulent use of non-cash payment instruments*. The Directive (EU) 2019/713 stipulates that the Member States of the European Union shall ensure that, when committed *intentionally*, the following conduct is punishable as a criminal offence:

> *"the fraudulent use of a stolen or otherwise unlawfully appropriated or obtained non-cash payment instrument"*.[26]

---

[25] Article 2(a) of the Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment.

[26] Article 3 of the Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment. In addition, the act of inciting or aiding or abetting a person to mentioned offence may also lead to criminal liability.

In fact, the perpetrator of the offence does not use (misuse) the contactless card by his hand(s), since (s)he does not holds it. However, using fake RFID reader, (s)he sends the card an encryption key, subsequently the card decrypts the encryption key, which allows all future communication to be encrypted using that key, the card reader sends the card the proposed transaction, the card "signs" the transaction. On the one hand, the regular using of contactless payments operate at only a short range – 1-5 centimetres (or more). On the other hand, fake RFID reader can operate at longer distance, for example, a few meters.

As regards liability, the Directive (EU) 2019/713 defines the concept of criminal liability of natural persons as well as legal persons. Indeed, the Directive takes into account also corporate criminal liability.[27] On the other hand, the question which begs consideration is whether legal persons are interested in such a criminal offence.

It should be noted that criminal liability of legal persons for offences is an issue which has been coming and going on the political agenda of the European Union.[28] Another question which begs consideration in this context is whether liability of legal persons should be governed by civil or criminal controls. In the European Union the criminal law approach has evolved. Besides harmonisation of elements of crimes (European crimes) and sanctions for naturals, European Union law has repeatedly confirmed the liability of legal persons.[29] It became a common approach of legal framework regulating European crimes, including counterfeiting of means of payment.

---

[27] Article 10 of the Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment.

[28] Vermeulen, G., De Bondt, W., Ryckman, Ch. (2012) *Liability of Legal Persons for Offences in the EU*. Antwerpen – Apeldoorn – Portland: Maklu, p. 9; Maďar, M. (2016) Trestná zodpovednosť právnických osôb – historické aspekty. In: Dominika Cevárová (ed.). *Interpolis '16. Zborník vedeckých prác z XIII. medzinárodnej vedeckej konferencie doktorandov a mladých vedeckých pracovníkov konanej dňa 10. novembra 2016 v Banskej Bystrici*. Banská Bystrica: Belianum, pp. 452–461.

[29] See, for example: Article 16 of the Directive (EU) 2017/541 on combating terrorism; Article 6 of the Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims; Article 13 of the Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography; Article 7 of the Framework Decision 2004/757/JHA laying down minimum provisions on the constituent elements of criminal acts and penalties in the field of illicit drug trafficking; Article 6 of the Framework Decision 2003/568/JHA on combating corruption in the private sector; Article 11 of the Directive 2013/40/EU on attacks against information systems; Article 6 of the Framework Decision 2008/841/JHA on the fight against organised crime.

3.4. SANCTIONS FOR OFFENCES

The Directive (EU) 2019/713 defines serious environmental offences which should be made punishable under criminal law (see above). It obliges explicitly the States to provide for criminal sanctions in their criminal laws (see below).

The Directive stipulates, as regards sanctions for natural persons, that the Member States of the European Union shall ensure that the above--mentioned offences are punishable by *effective, proportionate and dissuasive criminal penalties*.[30] On the one hand, the Directive requires the Member States of the European Union to take *effective, proportionate and dissuasive sanctions*. On the other hand, it does not define this approach. According to the *European Commission*, *effectiveness* requires that the sanction is suitable to achieve the desired goal, i.e. observance of the rules; *proportionality* requires that the sanction must be commensurate with the gravity of the conduct and its effects and must not exceed what is necessary to achieve the aim; *dissuasiveness* requires that the sanctions constitute an adequate deterrent for potential future perpetrators.[31]

The Member States shall ensure that the some offences are punishable by a maximum term of imprisonment of at least one year, some at least two years and some at least three years.[32] In addition to that, the offences shall be punishable by a maximum term of imprisonment of at least five years if they are committed within the framework of a criminal organisation as defined in the Framework Decision 2008/841/JHA on the fight against organised crime[33] (irrespective of the penalty provided for in that Decision).

---

[30] Article 9(1) of the Directive (EU) 2019/713 on combating fraud and counterfeiting of non--cash means of payment.

[31] European Commission. (2011) *Towards an EU Criminal Policy: Ensuring the effective implementation of EU policies through criminal law.* Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2011) 573 final, p. 9. Available from: https://db.eurocrim.org/db/en/doc/1626.pdf [Accessed 8 November 2019].

[32] For details, see: Article 9(2)(3)(4)(5) of the Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment.

[33] Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime. *Official Journal of the European Union* (L 300/42) 11 November. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008F0841 [Accessed 8 November 2019]. The objective of the Framework Decision is to harmonise Member States' definitions of crimes related to a criminal organisation and to lay down corresponding penalties for these offences. See: Calderoni, F. (2010) *Organized Crime Legislation in the European Union: Harmonization and Approximation of Criminal Law, National Legislations and the EU Framework Decision on the Fight Against Organized Crime*. Heidelberg – Dordrecht – London – New York, Springer.

The Directive (EU) 2019/713 stipulates, as regards sanctions for legal persons, that the Member States of the European Union shall ensure that a legal person is subject to – again – *effective, proportionate and dissuasive sanctions*, which shall include criminal or non-criminal fines.[34]

4. NON-LEGISLATIVE PREVENTION

The prevention against misuse of payment cards with RFID chip is very simple. One could say that using of cash is the best protection. However, how about people constantly using payment cards, including contactless RFID payments.

RFID technology does not work through metal. One could pack their card in aluminium foil, but it is not comfortable. There is a possibility to use RFID-blocking products, for example, RFID card protector made of aluminium. It is small aluminium foil, where you can put your payment card. You can remove your card before payment and put it in the foil after payment. The price of such a foil is surprising – you can buy it just a few cents. For example, a pack of 10 aluminium foils costs about 1–5 EUR. On the other hand, there is opinion that RFID-blocking products are practically worthless. According to *Digital Trends*[35] a card transmits a one--time transaction code that is encrypted. It does not give name or billing address of its holder and crucially it does not include the three-digit code on the back of the card that is needed for online transactions. The information that can be skimmed is simply not enough to enable the thief to commit another crime. As regards RFID-blocking products,

> *"No, they're a waste of money,"*

Roger Grimes, data-driven defense evangelist at *KnowBe4*[36], told the *Digital Trends.*

> *"You shouldn't spend one cent. There has still to this day not been a report of a single real-world crime that an RFID blocking product would have stopped."*

[34] For details, see: Article 11 of the Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment.

[35] RFID-blocking products are practically worthless. Here's why. [online] Available from: https://www.digitaltrends.com/cool-tech/are-rfid-blocking-products-worth-your-money-we-asked-an-expert/ [Accessed 8 November 2019].

[36] *KnowBe4* provides *Security Awareness Training* to help manage the IT security problems of social engineering, spear phishing and ransomware attacks. See: https://www.knowbe4.com

In personal banking, using two bank accounts is recommended – primary bank account and secondary bank account. While the primary bank account should be account for incomes, the secondary bank account should be used for outgoings – in case of credit cards all costs are paid via revolving account. It is good choice to send needed amount of money to secondary bank account and use payment card(s) issued to secondary bank account – not only for card payments by RFID and PIN, but also for all transactions – withdrawing money from an ATM (automated teller machine), online payments, mobile payments (for example, by *Masterpass*[37]), etc. If the card is misused (not only misuse for purposes of contactless payments), only limited amount of money will be lost.

5. CONCLUSION

Since the recent past RFID technology is understood as advanced automatic identification technology. As regards usage of this technology in banking, the very first advantage of this technology is convenience of payment. On the other hand, it is easy to misuse RFID chip in payment card. Anyone with a fake RFID scanner, even homemade scanner, can "send" signal. That means that anyone with a scanner can walk down the street and "scan" cards of people without realising it. Moreover, if information is "stolen", RFID chips are very easy to clone and to be counterfeited.

Specific offences are recognised as offences which are within the legislative competence of the European Union. The *Treaty on the Functioning of the European Union* lists *counterfeiting of means of payment* as one of the areas of particularly serious crime with a cross--border dimension. At the European Union level the leading legislative instrument harmonising counterfeiting of means of payment is the Directive (EU) 2019/713. This Directive establishes *minimum rules* concerning the definition of criminal offences and sanctions in the areas of fraud and counterfeiting of non-cash means of payment. The Directive (EU) 2019/713 is addressed to the Member States of the European Union. They shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 31st May 2021.

[37] A *Masterpass* is a digital wallet offered by *Mastercard* to provide the consumers with a faster checkout process by storing the payment and shipping information at a secured location. See: https://www.masterpass.com

The Directive (EU) 2019/713 stipulates that the Member States of the European Union shall ensure that, when committed *intentionally*, the fraudulent use of a stolen or otherwise unlawfully appropriated or obtained non-cash payment instrument is punishable as a criminal offence.

As regards prevention against misuse of payment cards with RFID chip, it is very simple. RFID technology does not work through metal. One could pack their card in aluminium foil, but it is not comfortable. There is a possibility to use RFID-blocking products, for example, RFID card protector made of aluminium. It is small aluminium foil, where you can put your payment card. In personal banking, using two bank accounts is recommended. While the primary bank account should be account for incomes, the secondary bank account should be used for outgoings.

LIST OF REFERENCES

[1] Ahson, S. A., Ilyas, M. (2008) *RFID Handbook: Applications, Technology, Security, and Privacy*. Boca Raton: CRC Press.

[2] Could you fall prey to a contactless conman? How thieves can take money from your card as you're walking down the street. [online] Available from: https://www.dailymail.co.uk/news/article-3849368/Could-fall-prey-contactless-conman-thieves-money-card-walking-street.html [Accessed 18 October 2016].

[3] Council Framework Decision 2001/413/JHA of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment. *Official Journal of the European Communities* (L 149/1) 2 July. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32001F0413 [Accessed 8 November 2019].

[4] Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime. *Official Journal of the European Union* (L 300/42) 11 November. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008F0841 [Accessed 8 November 2019].

[5] Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA. *Official Journal of the European Union* (L 123/18) 10 May. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0713&from=EN [Accessed 8 November 2019].

[6] European Commission. (2011) *Towards an EU Criminal Policy: Ensuring the effective implementation of EU policies through criminal law*. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2011) 573 final. Available from: https://db.eurocrim.org/db/en/doc/1626.pdf [Accessed 8 November 2019].

[7] European Commission. (2017) *Proposal for a Directive of the European Parliament and of the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA*, COM(2017) 489 final. Available from: https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-489-F1-EN-MAIN-PART-1.PDF [Accessed 8 November 2019].

[8] Fernándes-Caramés, T. M., Fraga-Lamas, P., Suárez-Albera, M., Castedo, L. (2017). A Methodology for Evaluating Security in Commercial. In: Paulo Crepaldi, Tales Pimenta (eds.). *Radio Frequency Identification*. Rijeka: InTech.

[9] Funta, R. (2019) *Úvod do počítačového práva*. Brno, MSD.

[10] Han, Z., Xu, Y., Wang, R. (2014) The Summarize of Medium Access Control Protocol in RFID. In: Xue Wang, Li Cui, Zhongwen Guo (eds.). *Advanced Technologies in Ad Hoc and Sensor Networks: Proceedings of the 7th China Conference on Wireless Sensor Networks*. Heidelberg – New York – Dordrecht – London, Springer.

[11] How Do RFID Contactless Payments Work? [online] Available from: https://www.cardswitcher.co.uk/2019/03/rfid-contactless-payments/ [Accessed 8 November 2019].

[12] Ivor, J., Polák, P., Záhora, J. (2017) *Trestné právo hmotné II: Osobitná časť*. Bratislava: Wolters Kluwer.

[13] Maďar, M. (2016) Trestná zodpovednosť právnických osôb – historické aspekty. In: Dominika Cevárová (ed.). *Interpolis '16. Zborník vedeckých prác z XIII. Medzinárodnej vedeckej konferencie doktorandov a mladých vedeckých pracovníkov konanej dňa 10. novembra 2016 v Banskej Bystrici*. Banská Bystrica: Belianum.

[14] Nof, S. Y. (2009) *Springer Handbook of Automation*. Berlin – Heidelberg: Springer.

[15] Qiao, Y., Chen, S., Li, T. (2012) *RFID as an Infrastructure*. New York – Heidelberg – Dordrecht – London: Springer.

[16] RFID-blocking products are practically worthless. Here's why. [online] Available from: https://www.digitaltrends.com/cool-tech/are-rfid-blocking-products-worth-your-money-we-asked-an-expert/ [Accessed 8 November 2019].

[17] Treaty on the Functioning of the European Union as amended by the Treaty of Lisbon. 26 October 2012 (C 326/47). Available from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:EN:PDF [Accessed 8 November 2019].

[18] UK Finance. (2019) *Fraud the Facts 2019: The definitive overview of payment industry fraud*. [online] Available from: https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202019%20-%20FINAL%20ONLINE.pdf [Accessed 8 November 2019].

[19] Vermeulen, G., De Bondt, W., Ryckman, Ch. (2012) *Liability of Legal Persons for Offences in the EU*. Antwerpen – Apeldoorn – Portland: Maklu.

[20] Walker, M. (2019) *CEH Certified Ethical Hacker All-in-One Exam Guide*. 4th ed. New York: McGraw Hill Professional.

[21] What Is RFID – Radio Frequency Identification? [online] Available from: https://www.iitms.co.in/rfid-based-attendance-system/what-is-rfid/ [Accessed 8 November 2019].

[22] What Is RFID Skimming? [online] Available from: https://www.tripwire.com/state-of-security/featured/what-rfid-skimming/ [Accessed 8 November 2019].

DOI 10.5817/MUJLT2020-2-6

COUNCIL OF EUROPE RECOMMENDATION CM/REC(2017)5 AND E-VOTING PROTOCOL DESIGN

by

ROBERT MÜLLER-TÖRÖK[*], DOMENICA BAGNATO[**], ALEXANDER PROSSER[***]

The Corona pandemic has created a push towards digitization in a number of fields, not least in the public sector including democratic processes. This of course includes an increased interest in e-voting via the Internet. The Council of Europe has a long-standing history of work in the field including two Recommendations – (2004)11 and (2017)5 – which have become the de facto yardstick against which every e-voting system is measured. Rec(2017)5 builds on a decade of experience with e-voting and particularly strengthens two concepts important in any electronic voting system: Voting secrecy and auditability/verifiability. This has distinct implications for the design of e-voting protocols.

The aim of this paper is to analyse the impact on what arguably are the most popular voting protocol families, envelope and token protocols. How does the modified Recommendation impact on the viability of protocols and protocol design? The paper first presents the Council of Europe Recommendation and the technical issues it addresses. Then a model is introduced to assess a voting protocol against the Recommendation; a typical envelope and a token protocol are assessed in view of the model and finally the two assessments are compared including policy recommendations for a path to e-voting implementation.

[*] mueller-toeroek@hs-ludwigsburg.de, University of Public Administration and Finance Ludwigsburg, Germany.

[**] domenica.bagnato@hierodiction.com, Hierodiction Software GmbH, Austria.

[***] alexander.prosser@wu.ac.at, Vienna University of Economics and Business Administration, Austria.

KEY WORDS
Council of Europe, Envelope Protocol, e-Voting, Token Protocol, Voting Principles

1. THE COUNCIL OF EUROPE AND ITS E-VOTING RECOMMENDATIONS

On the 30th of September 2004, the *Council of Europe* passed the *Recommendation for electronic voting, Rec(2004)11*[1]. It was the first attempt to define requirements for e-voting systems, which also includes remote voting and voting machines. Some points listed in the recommendation would prove to be irrelevant to the practical implementation for e-voting systems as they were of rather general nature equally concerning all voting channels and methods.[2] Yet it was the landmark attempt to define the legal, operational and technical standards an e-voting system has to follow (Appendices I–III). *The Explanatory Memorandum to Appendix III* on the technical standards was couched in *Common Criteria (CC)* terminology; CC is a global standard for the security evaluation and certification of IT systems.[3] Clear reference to CC terminology and structure indicates that the *Council of Europe* intended the Recommendation to become the basis for e-voting system certification.

Building on a decade of practical experience of e-voting, *CM/Rec(2017)5*[4] provides an update that equally applies to voting machines and remote (typically internet) voting. This paper uniquely focusses on the latter. It has to be noted that there is no such thing as "e-voting", but that there are many systems in place, which also follow vastly different protocols and algorithms. It also has to be understood that the correct and meaningful

---

1 Recommendation Rec(2004)11 of the Committee of Ministers to member States on legal, operational and technical standards for e-voting, 30 September 2004. Available from: https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/Rec(2004)11_Eng_Evoting_and_Expl_Memo_en.pdf [Accessed 16 June 2020].

2 Example includes, *"Possible registration requirements for e-voting shall not pose an impediment to the voter participating in e-voting"*, ibid, Appendix I, A. 2.; *"E-voting systems shall prevent any voter from casting a vote by more than one voting channel"*, ibid, A.6.; *"The e-voting system shall not permit any manipulative influence to be exercised over the voter during the voting"* , ibid, Appendix III, 12.

3 Bagnato, D. (2019) The impact of the Council of Europe Recommendation CM/REC(2017)5 on eVoting protocols. In: Nemeslaki, A., Prosser, A., Scola, D., Szadeczky, T. (eds.). *Central and Eastern European eDem and eGov Days 2019*, Budapest, 2–3 May.

4 Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting, 14 June 2017 (CM/Rec(2017)5), p. 2. Available from: https://rm.coe.int/0900001680726f6f [Accessed 17 April 2019].

software implementation of the protocol has to be considered as well.[5] This paper focusses on the *protocol design* (not the intricacies of software implementation) of e-voting systems in view of the Recommendation.

After the release of the 2004 Recommendation several e-voting projects in European countries failed, including Austria,[6] United Kingdom[7] and Finland,[8] which led to a general feeling that more stringent recommendations were needed. The main issues surrounding the failed elections could be summarised as a lack of reproducibility, audibility, general verifiability, transparency, and voter secrecy. In the Austrian student elections 2009, the election committee was unable to perform its duties because electronic election data had been destroyed and there was no means to verify the election results. In Finland, electronic votes went missing, which clearly indicates a lack of audibility. In the UK, votes were manually edited in clear text to fit into the counting application[9] and the election committee could not follow the procedures for opening the ballot box and counting the votes. Furthermore, undocumented data transfers during an ongoing election were observed.[10] These and similar events clearly necessitated a new and more stringent Recommendation.

On the 14th of June 2017, the *Recommendation CM/Rec(2017)5 of the Committee of Ministers to Member States on standards for e-voting* and an explanatory memorandum[11] and guidelines[12] were passed. We hold that

---

5 Prosser, A. and Müller-Török, R. (2009) E-Voting: Lessons Learnt. In: Kaplan, B. and Aktan, D. (eds.). *International Conference on eGovernment and eGovernance*, Ankara, pp. 265–280.

6 Constitutional Court. (2011) V 85-96/11-15, 13 December.

7 Actica Consulting. (2007) *Summary of Technical Assessments of May 2007 e-voting Pilots*. [online] Available from: http://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0018/16191/Actica_Summary_27244-20136__E__N__S__W__.pdf [Accessed 31 May 2018].

8 Karhumäki, J. and Meskanen, T. (2008) *Audit Report on Pilot Electronic Voting in Municipal Elections*. University of Turku, Turku.

9 Actica Consulting. (2007) *Technical Evaluation of Rushmoor Borough Council e-voting Pilot 2007*. [online] Available from: http://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0019/16192/Actica_Rushmoor_27248-20137__E__N__S__W__.pdf [Accessed 31 May 2018].

10 Actica Consulting. (2007) *Summary of Technical Assessments of May 2007 e-voting Pilots*. [online] Available from: http://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0018/16191/Actica_Summary_27244-20136__E__N__S__W__.pdf [Accessed 31 May 2018].

11 Explanatory Memorandum to Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting, 14 June 2017 (CM(2017)50-add1 final). Available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168071bc84 [Accessed 17 April 2019].

12 Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting, 14 June 2017 (CM(2017)50-add2final). Available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680726c0b [Accessed 17 April 2019].

the Recommendation, for the most part, streamlines requirements for e-voting in the context of the practical application of an e-voting system, particularly in the field of voter secrecy as well as (individual and collective) verifiability.

2. COMPARATIVE ANALYSIS OF REC(2004)11 AND CM/REC(2017)5

The relevant recommendations that relate to the technical core functioning of e-voting are found in Appendix I, standards 1–26 of CM/Rec(2017)5. First and foremost, the document has been streamlined with the number of standards being reduced from 112 to 49. Below are a number of standards that were added to or expanded in CM/Rec(2017)5 as compared to the 2004 recommendation.

1) Defining the way in which voting information is to be presented. In terms of the user interface, this recommendation is crucial. Official voting information is to be presented in an equal way across voting channels [CM/Rec(2017)5, 5][13]. This may lead to unexpected results: Catering, for instance, for persons with disabilities, such as the visually impaired, by supporting a screen reader would mean that the way information is presented needs to be changed to make it accessible and this breaches CM/Rec(2017)5, 5. Furthermore, an e-voting system cannot reasonably be seen to maintain voter secrecy under these conditions and hence poses a security breach.
2) The voter registry and its requirements for e-voting is not controlled by the e-voting system, hence Rec(2004)11, 2 was rightfully omitted. CM/Rec(2017)5 expanded its requirements to enforce that the system authenticate a person as having the right to vote [CM/Rec(2017)5, 8] before accessing the e-voting system. This was indirectly addressed by Rec(2004)11, 80 and 94 but has been reworded to specifically apply to the voter.
3) The function of an electronic ballot box differs considerably to that of the physical ballot box in traditional voting. The electronic ballot box stores votes cast, including redundant votes created

[13] In the following, CM/Rec(2017)5, x refers to Standard x of the Recommendation. The same applies to Rec(2004)11. In accordance with *Council of Europe* practice we equally use CM/Rec and Rec.

through the voter's right to cast a vote up to an arbitrary number of times. During the vote-counting stage, the system sorts the votes discarding redundant votes and counts only the last vote cast per voter, irrespective of how many times a voter voted and includes only that last vote in the final election results [CM/Rec(2017)5, 9].

4) The e-voting system is required to alert the voter if he or she attempts to cast an invalid vote, giving the voter the option to cast a valid vote [CM/Rec(2017)5, 14]. This however means that "paper voters" and electronic voters are not treated the same way, as such an alert does not exist for postal or paper-based presence voting.
5) A requirement that presents itself in the 2017 recommendations is the need for collective verifiability in that each vote is accurately included in the election results and it must be verifiable independently from the e-voting system [CM/Rec(2017)5, 17 and 18].
6) The voter shall be able to verify that his or her intention is accurately represented in the vote [individual verifiability, CM/Rec(2017)5, 15]. Please note that individual verifiability reaches until the vote enters the ballot box and general verifiability reaches until the election result.
7) E-voting system stores only personal information that is necessary to conduct the election [CM/Rec(2017)5, 20]. Depending on the protocol, very little personal information is needed, because the system only needs to identify the user as having the right to vote, possibly assign a constituency (if any) and record that the user has voted at least once.
8) The recommendation on the confidentiality of the voter's register has been expanded slightly to allow for accessibility by authorised parties [compare Rec(2004)11, 78 and CM/Rec(2017)5, 22].
9) The 2004 recommendation did not take into account the possibility for a voter to vote several times and so the 2017 recommendations has included this requirement. It asks that

"E-voting shall ensure that the secrecy of previous choices recorded and erased by the voter before issuing his or her final vote is respected"

in CM/Rec(2017)5, 25. However, here the standard does not accurately correspond to the technical functioning of an e-voting system for no vote/choice is erased by the system, if it is to be secure and auditable. The previous choices are not included in the final election results but they are stored in the ballot box and nobody has the right to erase or change a vote cast at any stage of the election process for this would be a clear breach of security, cf. CM/Rec(2017)5, 24.

The essence of the improvements can be summarised by verifiability, Standards 15, 17, 18 and a strengthening of voting secrecy, Standards 19, 20, 25 and – most prominently – 26, with some emphasis on usability, recommendations 5 and 14.

3. HOW TO MEASURE AN E-VOTING SYSTEM'S VIABILITY

An e-voting system is defined by the protocol it implements. The protocol is the basis for its core functionality and determines to what extent the system will be able to fulfil the requirements of CM/Rec(2017)5. The first step is to define the dimensions and then to assess the extent to which an e-voting protocol fulfils the dimensional requirements. Using the recommendation of the *Council of Europe*, CM/Rec(2017)5, the following dimensions can be distinguished:[14]

A. Equal suffrage:

   1. The unique identification of voters [CM/Rec(2017)5, 7];
   2. Access granted only to authenticated voters [CM/Rec(2017)5, 8];
   3. Only the appropriate number of votes per voter are stored in the electronic ballot box [CM/Rec(2017)5, 9].

B. Individual verifiability includes:

   1. Verification by the voter that the voters' intention is accurately represented by the vote and that the "sealed vote" has entered the ballot box without being altered [CM/Rec(2017)5, 15];

[14] This section builds upon the general modelling method introduced in Prosser, A. (2014) Transparency in eVoting – Lessons learnt. *Transforming Government: People, Process and Policy*, 8 (2), pp. 171–184.

2. Voter confirmation that the vote has been cast successfully [CM/Rec(2017)5, 16].

C. General verifiability includes:

1. Sound evidence must be provided, *"that each authentic vote is accurately included in the* [...] *results"* and be independently verifiable from the e-voting system [CM/Rec(2017)5, 17];
2. Sound evidence must be provided that *"only eligible voters' votes have been included in the* [...] *result"* and be independently verifiable from the e-voting system [CM/Rec(2017)5, 18].

It should be noted that B and C cover protection against manipulation,[15] however distinguishes between the type of verification following the systematisation in CM/Rec(2017)5.

D. Secret suffrage includes:

1. Ensuring the secrecy of previous voting choices made by the voter before issuing his or her final vote [CM/Rec(2017) 5, 25];
2. Anonymity of votes, notably that the unsealed vote and the voter cannot be linked during counting. [CM/Rec(2017)5, 26];
3. Ensuring *"that the secrecy of the vote be respected at all stages of the voting procedure"* [CM/Rec(2017)5, 19].

E. Anti-coercion:

1. Not providing the voter with proof of the content of a vote cast *"for use by third parties"* [CM/Rec(2017)5, 23].

F. No premature disclosure of election results:

1. Secrecy of the number of votes for any voting option is to be maintained until after the closure of the electronic ballot box. [CM/Rec(2017)5, 24].

[15] Prosser, A. (2014) Transparency in eVoting – Lessons learnt. *Transforming Government: People, Process and Policy*, 8 (2), pp. 171–184.

Each of these dimensions may be protected by purely organisational or by technical means. The former means separation of control, data access restrictions in an application, usage of certified personnel, legal provisions etc. Organisational protection ultimately relies on people playing by the book; it relies on the fact that not a single individual or coalition of individuals may break the security of the system. Technical protection typically means cryptographic security that cannot be broken by any coalition of actors.[16] Therefore, the level up to which each of the above dimensions A–F is protected by technical means indicates a security frontier for an e-voting system.

It has to be understood that at some stage, organisational protection must be employed, there can be no 100 % technical security. However, the question is, when the organisational safeguards are needed. Two dimensions appear to be relevant in this context; both concern a violation of Dimensions A–F above (in a generalised way referred to as "violation" below):

1. How many votes may be violated by organisational means?

    a. The entire election (as far as conducted electronically);
    b. The content of one (virtual) ballot box, i.e. a ward;
    c. A single vote.

2. Who can violate successfully?

    a. A single person in whatever capacity ("hot" candidates would be a system administrator or members of the election committee);
    b. A coalition of persons without the voter, e.g. the election committee in its entirety;
    c. A coalition including the voter/s concerned.

Let us assign levels 1 to 3 to combinations of the two violation dimensions in as far as the e-voting system does not provide *technical* protection (for which organisational protection must apply). We operate

[16] Here we disregard the fact that over time key lengths may become obsolete and may be broken. This risk may be minimised by using cryptographic keys with a sufficiently large "buffer time" until their length becomes obsolete.

under the assumption that there is one (logical) electronic ballot box per ward, which is controlled by one election committee.

	How many votes?			
		Entire ward	Single vote	No vote
How many actors?	Single actor	1	1	3
	Coalition w/o v.	1	2	3
	Coalition /w v.[17]	2	2	3

Table 1: Levels of manipulation that the technical safeguards of the e-voting system allow

"Violation" in this context means the undetected (hence successful) and directed violation of any of the Dimensions A–F. *Detected* violation of a dimension does not count as violation in the above systematization as it may entail an enormous backlash including repetition of the election but does *not* imply the successful violation of the dimension and the underlying election principle. To assign a value to the dimension, the first line in *Table 1* (single actor) is analysed. If a single actor can violate the dimension for the ward or a single vote, a value of 1 is assigned to the dimension and the analysis of the dimension stops; otherwise ("no vote" in line one), line two (coalition of actors without a voter, e.g. the election committee or a subset thereof) is analysed the same way; if it also yields "no vote", line three is analysed. An example: Assume that Dimension D (voting secrecy) is completely (technically) protected against single actor violation and that a coalition without the voter can violate the dimension for the entire ward: Line one yields a value of 3, hence line two is analysed, which yields a value of 1 for the dimension and the analysis stops. This procedure is repeated for all dimensions. Summarising, *Figure 1* presents a model for mapping the resulting security frontier following a systematisation proposed by *Prosser*.[18] There are Dimensions A to F and values of 1 to 3 in each dimension.

Remark: The interested reader is invited to insert his or her own classification in the above systematisation. The model is also flexible enough to include additional or fewer dimensions or to provide for a finer distinction, for instance with a defined subgroup of votes cast in a ward

[17] Meaning with all the respective voter/s concerned.

[18] Prosser, A. (2014) Transparency in eVoting – Lessons learnt. *Transforming Government: People, Process and Policy*, 8 (2), pp. 171–184.

as additional level of compromising votes. The values in *Table 1* represent our take of the severity of violations and will be suitable for the following discussion of the two protocol families.

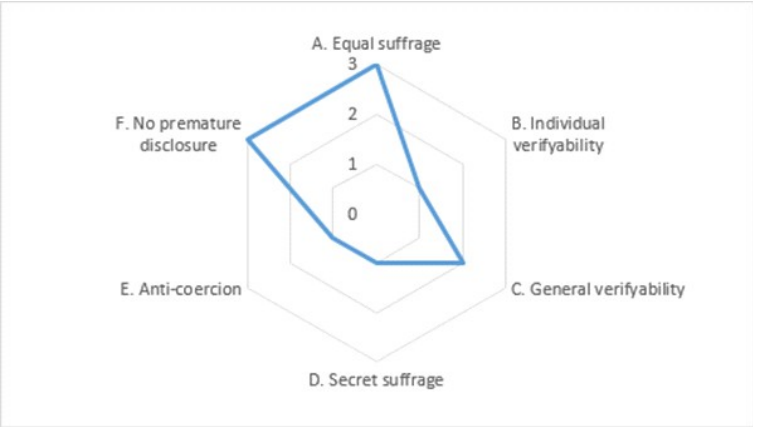

Figure 1: Model of the aims of an e-voting system – hypothetical example

The hypothetical system depicted in *Figure 1* provides high protection of equal suffrage, for instance by using a citizen card for voter identification and cryptographic protection for the data link between voter and constituency assignment. Individual verifiability is on a low level, for instance, a single person could fool voters into believing that their vote reached the ballot box correctly, where in fact it was altered. General verifiability is on a medium level, for instance the election committee of a ward could collude to provide a false audit trail for the correctness of the result of their ward with respect to an individual vote. Protection of voting secrecy is minimal, again a single person could break it for a ward. Anti-coercion protection is equally minimal, vote buying by a single person would effectively be possible. Premature disclosure of results however, has the highest protection level.

We hold that this model is (i) useful to quickly map the abilities of a voting protocol in view of the requirements set out in CM/Rec(2017)5 and (ii) flexible enough to be adapted and/or refined to more specific needs in this regard, for instance selection of an e-voting system in a tendering procedure.

4. TRADE-OFFS

4.1. INDIVIDUAL VERIFIABILITY AND WAYS TO DETER VOTE BUYING

The CM/Rec(2017)5, 19, recommends the secrecy of the vote be respected at all stages of the voting procedure. However, this presents a conflict with CM/Rec(2017)5, 15, which requires that the voter be able to verify the vote and verify that the vote has entered the ballot box without alteration. Finally, CM/Rec(2017)5, 23 contrasts in that

> *"An e-voting system shall not provide the voter with proof of the content of the vote cast for use by third parties".*

It becomes evident that these requirements create two goal conflicts, that of individual verifiability versus anti-coercion and individual verifiability versus secret suffrage. These conflicts have been realised very early on.[19] It should be understood that individual verifiability may create conflicts in terms of voting secrecy, for in order to verify the vote cast, the voter would need to receive confirmation of the actual vote cast to validate its correctness; this could be checked by a third party buying the vote or coercing the voter. However, this equally applies to postal voting.[20]

However, on a very general level, it is not possible to stop voters from recording in some format their vote; this also applies to polling booth voting as well. The moment a voter has the ability to check the authenticity of a vote, voter secrecy is compromised paving the way for voter coercion. Voter buying relies on proof in some format that the vote cast is the vote that was bought. In this light, measures could be taken in terms of system procedures that would question the authenticity of the vote recorded for use by third parties, by allowing only the ability to verify a vote when having the option to change it. So, one could never be sure if the verification recorded by the voter for use by third parties was the final vote actually cast or not.

The *Explanatory Memorandum to CM/Rec(2017)5* in relation to Standard 23 of the recommendation outlines concerns where voter secrecy could be

---

[19] Cf. Cohen, J. and Fischer, M. (1985) A robust and verifiable cryptographically secure election scheme. In: *26th Symposium on the Foundations of Computer Science*, October 21–23, IEEE, pp. 373–382.

[20] Müller-Török, R. (2019) The Principles Established by the Recommendation CM/Rec(2017)5 on Standards for E-Voting Applied to Other Channels of Remote Voting. *Masaryk University Journal of Law and Technology*, 13 (1), pp. 3–26.

compromised. From this list, compromised voting secrecy could be summarised:

1. Through some form of remote access to computers via the internet such as a computer virus to collect and record voter transactions;
2. The voter physically breaches voter secrecy by using some means to create a copy of the vote and distribute it.

It is very difficult to control every aspect of remote voting particularly internet connected computers and although the ability to disable printing and print screen functionalities, erasing user interaction through input and output devices such as keyboards, mice and screens, can be realised. Ultimately it is up to the voters to take responsibility for the security of their computers and in doing so voter secrecy. The same applies to postal voting, where the ballot should perhaps also not be filled in in public.

It must be understood that if one can see the vote, one can record the vote and the voting process via devices that are not physically connected to the voting device, such as photographing the screen and video recording the entire procedure. The same applies to paper-based voting, whereby, for instance, in Austria it is perfectly legal to take a photo of one's own vote and post it on social media.[21] At this stage, it is not possible to prevent this from happening, but to focus on defining e-voting procedures making vote buying or coercion more difficult. Here some technical suggestions we find useful from an implementation perspective:

1. Deter photographing and printing of votes, enable multiple vote casting

   Enable multiple voting, something that is impossible to realise in postal voting procedures. Furthermore, in voting multiple times, there should be no indication on the screen of the voting device as to how many times the voter has voted. Even if the voter took a photo of the screen or even a screen shot and printed it out to validate his vote, the information displayed should not give the viewer any indication as to whether the vote displayed is

[21] Pichler, G. (2019) Darf man seinen ausgefüllten Wahlzettel auf Instagram teilen? *Der Standard*, 25 May. [online] Available from: https://www.derstandard.at/story/2000103646954/darf-man-seinen-ausgefuellten-wahlzettel-auf-instagram-teilen [Accessed 16 June 2020].

the final vote cast. This would at least provide doubt as to the authenticity of the final vote shown to a third party.

2. Deter recording the voting process

   When recording the entire process via video camera for example, restrictions can be set requiring that before changing a vote, the voter must wait a certain number of hours before being allowed to change the vote, making the recording process difficult and tedious at best and the authenticity of the proof provided by the voter would still be questionable.

3. Deter bulk voting

   Restrictions could be placed on how many voters can access the voter registry and/or actually vote from any one computer or device. This could be done by recording the (physical) MAC address of the PC or device, separate from any identification information of the person voting. This would deter people from buying the right to vote on behalf of voters by having bought the identification needed to register and then voting for a group of people from any one PC. Also, this would be a huge improvement as compared to postal voting.[22]

4.2. SECRET SUFFRAGE VS. EQUAL SUFFRAGE

A system perfectly gauged to protect equal suffrage can be built but it would completely denigrate voting secrecy. An example would be the Austrian electronic citizens' initiative system, where supporters of a citizens' initiative sign with their electronic signature cards.[23] In contrast to hand-written signatures, these signatures can be reliably verified. Voter secrecy is not an issue here, as it is a citizens' initiative.

[22] Cf. the horrendous number of bulk voting cases documented in the U.K., cf. White, I. and Coleman, Ch. (2011) *Postal Voting & Electoral Fraud*, SN/PC/3667, House of Commons Library, and a recent case in Germany, cf. Landgericht Regensburg. (2018) *Strafverfahren wegen Verdachts der Wahlmanipulation in Geiselhöring*. [press release] 15 October. Available from: https://www.justiz.bayern.de/gerichte-und-behoerden/landgericht/regensburg/presse/2018/7.php [accessed 2 November 2018], all involving bulk postal voting.

[23] Stein, R. and Wenda, G. (2014) Das Zentrale Wählerregister – Ein skalierbares Instrument zur Bürgerbeteiligung mit 1:1-Verifikation. In: Plodereder, E., Grunske, L., Ull, D. and Schneider, E. (eds.). *44. Jahrestagung der Gesellschaft für Informatik.* INFORMATIK 2014, 22–26. September, Bonn, pp. 1427−1436. [online] Available from: https://subs.emis.de/LNI/Proceedings/Proceedings232/1427.pdf [Accessed 16 June 2020].

The essence of every e-voting protocol is to balance secrecy and reliable identification, which are clear trade-offs there.[24]

In the following sections, two voting protocol families are discussed with a view to the Recommendation and the security model in *Figure 1*. They can be distinguished by one "watershed" property, that is when the anonymization of the vote takes place – before or after the vote is put in the electronic ballot box.

5. ENVELOPING PROTOCOLS

Enveloping protocols have been widely implemented, probably because of their intuitive appeal due to the emulation of postal voting, and as an example we will take a look at the Estonian e-voting system,[25] which has been implemented in elections in Estonia since 2005.[26]

It should also be noted that the authors of CM/Rec(2017)5 due to some wording appear to have had an envelope protocol in mind when drafting the new recommendation, cf. for example Standard 15:

> *"The voter shall be able to verify that his or her intention is accurately represented in the vote and that the sealed vote has entered the electronic ballot box* […]*)"*;
>
> Standard 26:
>
> *"*[…] *in such a way that it is not possible to reconstruct a link between the unsealed vote and the voter* […]*)"*;
>
> or Standard 45:
>
> *"Votes and voter information shall be kept sealed until the counting process commences"*.

[24] Maaten, E. (2004) Towards remote e-voting: Estonian case. In: Prosser, A. and Krimmer, R. (eds.). *Electronic Voting in Europe – Technology, Law, Politics and Society*, GI-Edition, Lecture Notes in Informatics, pp. 83–90.

[25] Cf. State Electoral Office of Estonia. (2017) *General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia*, Document: IVXV-ÜK-1.0, Tallin. [online] Available from: https://www.valimised.ee/sites/default/files/uploads/eng/IVXV-UK-1.0-eng.pdf [Accessed 16 June 2020] and Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M. and Halderman, J.A. (2014) Security Analysis of the Estonian Internet Voting System. In: *CCS '14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ACM. [online] Available from: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf [Accessed 16 June 2020].

[26] Maaten, E. (2004) Towards remote e-voting: Estonian case. In: Prosser, A. and Krimmer, R. (eds.). *Electronic Voting in Europe – Technology, Law, Politics and Society*, GI-Edition, Lecture Notes in Informatics, pp. 83–90.

This is arguably due to the fact that enveloping protocols are comparatively easy to implement and have dominated the first wave of e-voting systems.

The envelope e-voting process can be split into three stages:

5.1. CASTING A VOTE

The voter authenticates him- or herself *vis à vis* the voting application using an eID. This is not part of the e-voting protocol proper.

The voter selects option/s on the ballot. The voting client selects a large random number *r* and constructs a pad from it, *pad(r)*.[27] The voter's vote and *pad(r)*, together as a "package", are encrypted using the public key of the election committee, and this creates the inner envelope.[28, 29] The voter then confirms his vote by digitally signing the inner envelope with his or her eID (digital signature card) creating a second layer known as the outer envelope.[30] The outer envelope containing the inner envelope is sent to the server and the voting client shows a QR-code containing the voter ID and *r*, which enables the voter to verify and/or change his vote a maximum of three times for up to 30 minutes after casting his initial vote.[31]

5.2. INDIVIDUAL VERIFICATION

To verify and/or to change the vote, the voter scans in the QR-code (that is his voter ID and random *r*) using a different device (typically a smart phone) from which he initially voted and the smart device sends the voter

---

[27] That is to ensure that even if two votes vote for the same option/s, they look different in encoded state.

[28] Cf. State Electoral Office of Estonia. (2017) *General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia*, Document: IVXV-ÜK-1.0, Tallin, p. 7. [online] Available from: https://www.valimised.ee/sites/default/files/uploads/eng/IVXV-UK-1.0-eng.pdf [Accessed 16 June 2020].

[29] Cf. Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M. and Halderman, J. A. (2014) Security Analysis of the Estonian Internet Voting System. In: *CCS '14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ACM, p. 705. [online] Available from: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf [Accessed 16 June 2020].

[30] Cf. State Electoral Office of Estonia. (2017) *General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia*, Document: IVXV-ÜK-1.0, Tallin, p. 7. [online] Available from: https://www.valimised.ee/sites/default/files/uploads/eng/IVXV-UK-1.0-eng.pdf [Accessed 16 June 2020].

[31] Cf. Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M. and Halderman, J. A. (2014) Security Analysis of the Estonian Internet Voting System. In: *CCS '14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ACM, p. 706. [online] Available from: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf [Accessed 16 June 2020].

ID to the electronic ballot box. From the ID, the ballot box identifies the vote stored in the system and sends it back. The encrypted vote as well as a list of all the possible voting options (parties, candidates or options at a referendum) are received by the smart device, which encrypts all the possible combinations for the options and the *pad(r)* with the original public key used to encrypt the vote and compares it with the voters' intended choice. If there is a match the option is displayed. This mechanism is used to verify what is in the encrypted inner envelope.[32]

5.3. COUNTING

First the digital signature in the outer envelope and whether the voter has already cast a vote are checked. Then outer and inner envelope are "separated" and the encrypted votes of the inner envelope are stored on a DVD and transferred to a separate machine that decrypts the vote using the private key of the election committee. Finally, the decrypted votes are counted.[33] *Figure 2* schematically depicts this process.

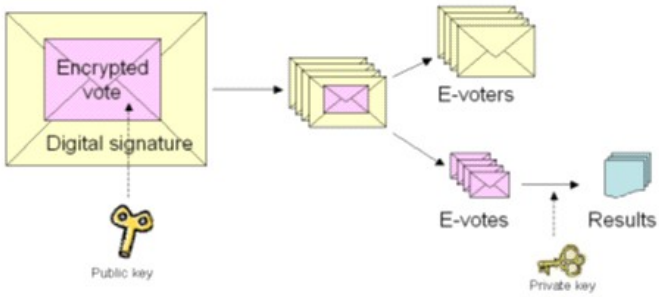

Figure 2: Envelope e-voting system[34]

[32] Estonian National Electoral Committee. (2010) *E-Voting System – General Overview*, Tallin, 2005–2010. [online] Available from: https://www.valimised.ee/sites/default/files/uploads/eng/General_Description_E-Voting_2010.pdf [Accessed 16 June 2020].

[33] Cf. Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M. and Halderman, J. A. (2014) Security Analysis of the Estonian Internet Voting System. In: *CCS '14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ACM, p. 706. [online] Available from: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf [Accessed 16 June 2020].

[34] Estonian National Electoral Committee. (2010) *E-Voting System – General Overview*, Tallin, 2005–2010, p. 10, Figure 2. [online] Available from: https://www.valimised.ee/sites/default/files/uploads/eng/General_Description_E-Voting_2010.pdf [Accessed 16 June 2020].

5.4. THE ENVELOPE PROTOCOL AND CM/REC(2017)5

Figure 3 depicts the enveloping protocol assessment according to the model in *Table 1* and *Figure 1*:

Equal suffrage is protected if an eID is used to authenticate voters. Thereby it is readily possibly to prevent voters from illegally casting multiple votes. This ID also determines the constituency for which the vote may be cast.

Individual verifiability is implemented in a rather roundabout way with the QR code and it should be clear that in the case of complex voting schemes with a large number of preferential votes, this mechanism does not scale well.[35] However, voters may check whether the vote reached the ballot box correctly; they may not check whether the vote stays there and enters the result correctly, which however is not required by CM/Rec(2017)5, 15! Therefore, the protocol gets a full score here.

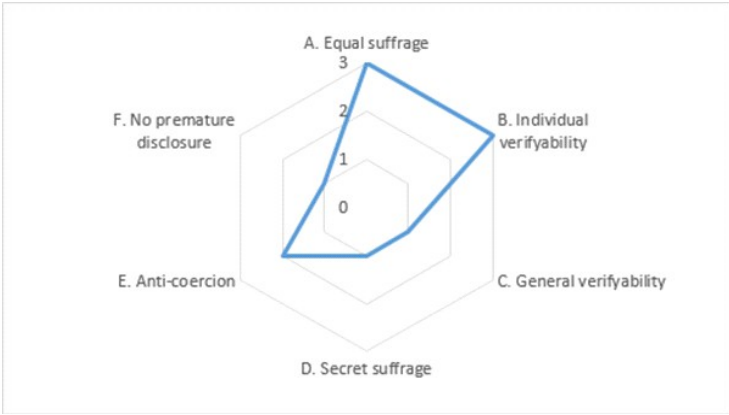

Figure 3: Enveloping protocol

General verifiability however cannot be guaranteed. The big weakness of this protocol family is that the ballot box contains the information how a voter voted (whereby the "how" is encrypted with the public key of the election committee). If the private key of the election committee and the ballot box with the votes containing the outer envelope were ever to be brought together, one could find out how every single voter voted. This could be done by a single person, e.g. a fraudulent administrator,

[35] Cf. Bagnato, D. (2019) The impact of the Council of Europe Recommendation CM/REC (2017)5 on eVoting protocols. In: Nemeslaki, A., Prosser, A., Scola, D., Szadeczky, T. (eds.). *Central and Eastern European eDem and eGov Days 2019*, Budapest, 2–3 May, pp. 59–69.

or a coalition without the voter, most notably a collusive election committee. This is also the reason why an independent recount is simply not possible:

- It would either mean to pass the ballot box plus private key of the election committee to an independent authority hoping that this authority does not misuse this information, or
- It would mean that the independent authority to conduct the recount gets the unsealed votes, which could also be manufactured by the election committee, part thereof or a fraudulent administrator (i.e. a single actor).

For the same reason, voting secrecy can only be guaranteed as long as the ballot box and the private key of the election committee are not joined. This has to be ascertained by organisational means. Therefore, Dimensions "general verifiability" and "secret suffrage" get the lowest score possible.

Anti-coercion is generally difficult to guarantee in remote voting procedures, electronic or paper-based, as discussed above. However, the QR code solution enables a coercer or vote buyer to check the "correct" vote. However, this is only possible for a single vote each time and involves cooperation by the voter, hence value 2 in *Figure 3*.

Premature disclosure of the ballot can be controlled to some extent by the application of the private key of the election committee, if a protocol of key decomposition is followed, where each election committee member holds a part of the key which is then assembled.[36, 37] Otherwise a single actor could apply the private key to "open" the ballots of the entire ward. However, in both cases the lowest value in *Table 1* applies.

6. TOKEN-BASED PROTOCOLS

A token protocol implements a two-staged process. The first stage is to attain a valid, signed voting card (token), which allows the voter to cast a vote at any stage during the voting period. The second stage is to vote via

[36] Cf. Blakley, R. (1979) Safeguarding cryptographic keys. In: IEEE (eds.). *International Workshop on Managing Requirements Knowledge (MARK)*, New York, 4–7 June, pp. 313–317.

[37] Cf. Prosser, A., Kofler, R., Krimmer, R. and Unger, M. K. (2004) Implementation of Quorum--Based Decisions in an Election Committee. In: Traunmüller, R. (ed.). *Proceedings of DEXA/EGOV 2004*, Lecture Notes in Computer Science LNCS 3183, Springer, Berlin, pp. 122–127.

an electronic ballot sheet using the token attained in the first stage. In the following the protocol presented in *Prosser and Müller-Török* (2002) is taken as a reference.[38]

6.1. CREATION OF THE TOKEN

The voter first identifies himself to the election system. This can be done by any current means of identification; in the context of political elections an eID would typically be used. The voting application then generates a very large random number as token *t* and submits it to the election system for a blind signature.[39] The blind signature gives an authentic signature on the token, nevertheless the server never sees the token it signs. In the physical world this would correspond to inserting a document to be signed into a carbon paper-lined envelope and sealing the envelope. The signor signs on the envelope and the signature imprints itself onto the document – there is an authentic signature by the signor, who nevertheless never sees what he signed. Blind signatures achieve this in the world of cryptography. However, in contrast to the physical envelope, the cryptographic "seal" cannot the broken. The election administration uses an asymmetric key pair (e.g. following the *RSA protocol*) of (e, d, m) with *e* being the external/public, *d* the domestic/private key and *m* the modulus.[40] The voter now has a voting card VC=[t, t^d].

The same process can be repeated with an election observer using a second RSA key pair (ε, δ, μ) adding another signature to the voting card. At the end of the first stage, the voter possesses a token validly signed by the election system and by the observer VC=[t, t^d, t^δ]. If several constituencies have to be served, the server maintains a key pair (e, d, m) per constituency and the constituency C is added to the VC=[t, $t^{d(C)}$,t^δ, C]. Of course, also several election observers could be used and the respective blind signatures concatenated in the token. To prevent misuse of the token

---

[38] Prosser, A. and Müller-Török, R. (2002) E-Democracy: Eine neue Qualität im demokratischen Entscheidungsprozess. *Wirtschaftsinformatik*, 44 (6), pp. 545–556.

[39] Chaum, D. (1981) Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24 (2), pp. 84–86.

[40] RSA signatures/encryption are done in a residue class ring modulo a very large number. Hence, a key "pair" always consists of private key, public key and modulus. For an introduction, we would recommend to directly go back to the classic [see Rivest, R. L., Shamir, A., Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21 (2)]. Please note that a blind signature according to *Chaum* (Ibid) is always executed on the full text not a hash of the full text as done in open (standard digital) signatures.

it can be saved symmetrically (=password) encrypted on the local file system, for instance using AES.[41]

6.2. VOTING

VC is the only means of identification the voter uses when casting a vote. Hence, anonymization happens before the vote is inserted in the ballot box. The ballot box (server) checks the voter authentication in VC by checking the digital signature/s (t, t^d) and, if used, (t, t^δ), by applying the public keys of the election authority e[42] and the observer ε. Also, the ballot box verifies whether the token *t* has already been used. After verification the voter gets the ballot sheet of the respective constituency. The ballot sheet is filled in and inextricably linked to the VC, for instance via a hash or other concatenation methods. The entire vote is then encrypted with the public key of the election committee and submitted to the ballot box.

6.3. COUNTING

The votes in the ballot box are already anonymous, and are only validated by a correctly signed VC to which they are concatenated. Counting therefore involves the following steps:[43]

1. Decrypting the ballots with the private key of the election committee;
2. Validating the concatenation of VC and ballot sheet;
3. Checking that the token was used only once;
4. Checking the signatures of election system and observer/s on the VC according to their public keys;
5. Checking the validity of the ballot and including it in the tally.

Since the electronic ballot box does not contain any information on the voter, it can be transferred to a third party for an independent recount. Moreover, the election authority could publish VCs and votes in a table (e.g. on a web site per ward) to enable verification containing

---

[41] National Institute of Standards and Technology. (2001) *Federal Information Processing Standards Publication 197*, ADVANCED ENCRYPTION STANDARD (AES). [online] Available from: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf [Accessed 16 June 2020].

[42] Note that a voter cannot fraudulently modify the constituency as then the public key *e* of the new (modified) constituency would not work anymore.

[43] Prosser, A (2014) Transparency in eVoting – Lessons learnt. *Transforming Government: People, Process and Policy,* 8 (2), pp. 171–184.

the authenticated voting card, the filled-in ballot sheet and the concatenation hash linking both as shown in *Table 2*.

$VC_1 = [t, t^{d(C)}, t^{\delta}, C]$	$Ballot_1$	$Hash_1$
$VC_2 = [t, t^{d(C)}, t^{\delta}, C]$	$Ballot_2$	$Hash_2$
$VC_3 = [t, t^{d(C)}, t^{\delta}, C]$	$Ballot_3$	$Hash_3$
...	...	...

Table 2: Publication of votes in a token protocol

6.4. THE TOKEN PROTOCOL AND CM/REC(2017)5

Figure 4 shows the degree to which the dimensions from the Recommendation are fulfilled.

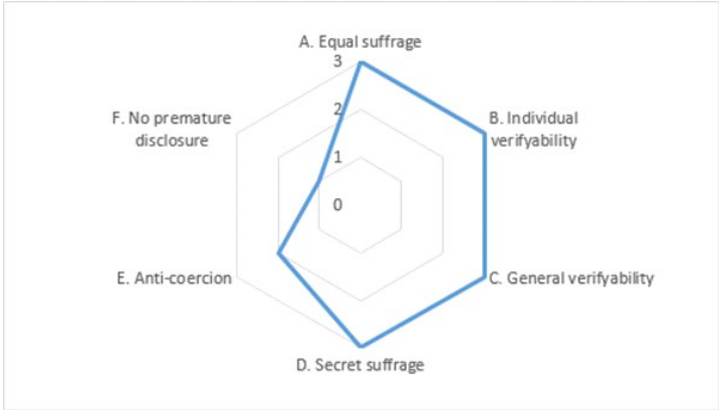

Figure 4: Token protocol score

If an eID or similar means of authentication is used, respect for the principle of equal suffrage is fulfilled; the discussion is the same as with the enveloping protocol.

The degree of individual verifiability of token systems indeed does not only fulfil the requirements of CM/Rec(2017)5, it goes way beyond. To see that consider *Table 2* and *Figure 5*. CM/Rec(2017)5 requires general verifiability as an "end-to-end" solution right to the election result. Individual verifiability, however, is only required until the ballot box, not the end result.[44] With a token protocol however, as votes are already anonymous when they reach the ballot box, the very content of the ballot box could be published on a website, probably organised by the ward

[44] Maybe having an envelope protocol type in mind, where such end-to-end individual verifiability would indeed be unthinkable.

to enable easier access by the voters. For each vote in the ballot box, VC, vote and concatenation information is published as depicted in *Table 2*. The voter can now readily access the web site and search for his or her token and verify, whether it entered the tally correctly. This can be done without compromising voting secrecy only using the token as a means of identifying the vote.[45] In this context token protocols reach a degree of individual verifiability that is not only higher than that of postal voting, but also than that of conventional polling station voting.

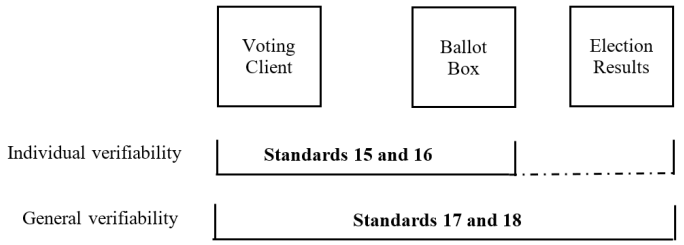

Figure 5: Individual vs. general verifiability in Rec(2017)5

In this list of published votes, individual verifiability is the "row-wise check" each individual voter can perform. General verifiability would be the "column-wise check" verifying all votes in the ward published with the following verification steps:

a. Each token entered the tally once;
b. Each token is properly authenticated by the election authority and, if used, by the observer/s;
c. Each vote is concatenated with a valid token;
d. The vote count published by the election authority can be reproduced with this published list and therefore be verified;
e. Comparison between the number of authenticated tokens and the number of tokens issued by the election authority and the observer/s ensures that no tokens/votes have been suppressed or inserted.

In contrast to envelope procedures an independent recount is possible because publishing the ballot box does not contain the information how voters voted and hence does not compromise voting secrecy. Every

[45] This could be offered in a "pure" function using *Ctrl+F* search for one's token on the web site and/or with a more amenable search functionality.

organisation interested and "civil society" in general may do that with a comparatively modest cryptographic toolset being necessary. Of course, open source tools for independent recounts can also be expected to emerge. In both verifiability dimensions the score is hence 3.

Secret suffrage is protected by the fact that nowhere in the server landscape of the election system the information how a voter voted is stored. The basis of authentication is the token signed by the election authority and the observer/s. No organisational means are necessary to protect secrecy. The only time, when the system "sees" voter information and token in the same transaction, the token is cryptographically (therefore technically, not organisationally) protected by the blind signature algorithm. The token is authentically signed without the signor ever seeing the token. That is also the reason why the ballot box as well as the private key of the election committee can be passed on after the election without compromising voting secrecy.

Anti-coercion is only moderately protected as with any remote voting scheme. However, the token may be used several times to cast a vote depending on the legal framework of the election. Each vote cast upon the token supplants the older one/s cast upon the same token. This may make vote buying and coercion more onerous than in postal voting procedures, where the paper-based election material may be used just once. The argument concerning protection against premature disclosure works the same way as with envelope protocols, a value of 1 is assigned.

7. CONCLUSION

This paper discussed the effects on the updated *Council of Europe Recommendation (2017)5* on e-voting protocol viability focussing on envelope and token protocols. A multi-dimensional model was advanced to systematically map the abilities of an e-voting protocol against the core requirements (dimensions) of CM/Rec(2017)5. A capabilities frontier was defined depending on how far technical safeguards protect each of the dimensions; beyond that only organisational safeguards apply. The paper then proceeded to present a typical envelope and a typical token protocol mapping it against the multi-dimensional model showing that there are considerable differences between the two protocol families in achieving the requirements of CM/Rec(2017)5.

The main weakness of enveloping is the complete absence of general verifiability and the necessity to keep the private key of the election committee and the ballot box apart, as both together enable to break voting secrecy on a large scale. The token protocol protects voting secrecy technically and enables a very high degree of individual and general verifiability, with individual verifiability exceeding the requirements of CM/Rec(2017)5.

As shown in the paper, the question of whether anonymization occurs before or after the insertion in the ballot box, is a true watershed between e-voting protocols. This question decides about the quality of individual verification, the possibility of a meaningful independent recount and the technical (not organisational) protection of voting secrecy. The authors hold that CM/Rec(2017)5 accentuates this watershed. In this regard the CM/Rec(2017)5 can be considered a seminal piece of work by the *Council of Europe* towards reliable e-voting.

LIST OF REFERENCES

[1] Actica Consulting. (2007) *Technical Evaluation of Rushmoor Borough Council e-voting Pilot 2007*. [online] Available from: http://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0019/16192/Actica_Rushmoor_27248-20137__E__N__S__W__.pdf [Accessed 31 May 2018].

[2] Actica Consulting. (2007) *Summary of Technical Assessments of May 2007 e-voting Pilots.* [online] Available from: http://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0018/16191/Actica_Summary_27244-20136__E__N__S__W__.pdf [Accessed 31 May 2018].

[3] Bagnato, D. (2019) The impact of the Council of Europe Recommendation CM/REC (2017)5 on eVoting protocols. In: Nemeslaki, A., Prosser, A., Scola, D., Szadeczky, T. (eds.). *Central and Eastern European eDem and eGov Days 2019*, Budapest, 2–3 May.

[4] Blakley, G.R. (1979) Safeguarding cryptographic keys. In: IEEE (eds.). *International Workshop on Managing Requirements Knowledge (MARK)*, New York, 4–7 June.

[5] Cohen, J. and Fischer, M. (1985) A robust and verifiable cryptographically secure election scheme. In: *26th Symposium on the Foundations of Computer Science*, October 21–23, IEEE.

[6] Common Criteria. (2014) *Common Criteria Recognition Arrangement, Common Criteria for Information Technology Security Evaluation*, Version 3.1R5, Parts 1 to 3. Available from: https://www.commoncriteriaportal.org/cc/ [Accessed 16 June 2020].

[7] Constitutional Court. (2011) V 85-96/11-15, 13 December.

[8] Estonian National Electoral Committee. (2010) *E-Voting System – General Overview*, Tallin, 2005–2010. [online] Available from: https://www.valimised.ee/sites/default/files/uploads/eng/General_Description_E-Voting_2010.pdf [Accessed 16 June 2020].

[9] Explanatory Memorandum to Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting, 14 June 2017 (CM(2017)50-add1 final) Available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168071bc84 [Accessed 17 April 2019].

[10] Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting, 14 June 2017(CM(2017)50-add2final). Available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680726c0b [Accessed 17 April 2019].

[11] Chaum, D. (1981) Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24 (2).

[12] Karhumäki, J. and Meskanen, T. (2008) *Audit Report on Pilot Electronic Voting in Municipal Elections.* University of Turku, Turku.

[13] Landgericht Regensburg. (2018) *Strafverfahren wegen Verdachts der Wahlmanipulation in Geiselhöring*. [press release] 15 October. Available from: https://www.justiz.bayern.de/gerichte-und-behoerden/landgericht/regensburg/presse/2018/7.php [Accessed 2 November 2018].

[14] Maaten, E. (2004) Towards remote e-voting: Estonian case. In: Prosser, A. and Krimmer, R. (eds.). *Electronic Voting in Europe – Technology, Law, Politics and Society*, GI-Edition, Lecture Notes in Informatics.

[15] Müller-Török, R. (2019) The Principles Established by the Recommendation CM/Rec (2017)5 on Standards for E-Voting Applied to Other Channels of Remote Voting. *Masaryk University Journal of Law and Technology*, 13 (1).

[16] National Institute of Standards and Technology. (2001) *Federal Information Processing Standards Publication 197*, ADVANCED ENCRYPTION STANDARD (AES). [online] Available from: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf [Accessed 16 June 2020].

[17] Pichler, G. (2019) Darf man seinen ausgefüllten Wahlzettel auf Instagram teilen? *Der Standard*, 25 May. [online] Available from: https://www.derstandard.at/story/2000103646954/darf-man-seinen-ausgefuellten-wahlzettel-auf-instagram-teilen [Accessed 16 June 2020].

[18] Prosser, A. (2014) Transparency in eVoting – Lessons learnt. *Transforming Government: People, Process and Policy*, 8 (2).

[19] Prosser, A. and Müller-Török, R. (2009) E-Voting: Lessons Learnt. In: Kaplan, B. and Aktan, D. (eds.). *International Conference on eGovernment and eGovernance*, Ankara.

[20] Prosser, A., Kofler, R., Krimmer, R. and Unger, M. K. (2004) Implementation of Quorum--Based Decisions in an Election Committee. In: Traunmüller, R. (ed.). *Proceedings of DEXA/EGOV 2004*, Lecture Notes in Computer Science LNCS 3183, Springer, Berlin.

[21] Prosser. A. and Müller-Török R. (2002) E-Democracy: Eine neue Qualität im demokratischen Entscheidungsprozess. *Wirtschaftsinformatik*, 44 (6).

[22] Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting, 14 June 2017 (CM/Rec(2017)5). Available from: https://rm.coe.int/0900001680726f6f [Accessed 17 April 2019].

[23] Recommendation Rec(2004)11 of the Committee of Ministers to member States on legal, operational and technical standards for e-voting, 30 September 2004. Available from: https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/Rec(2004)11_Eng_Evoting_and_Expl_Memo_en.pdf [Accessed 16 June 2020].

[24] Rivest, R. L., Shamir, A., Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21 (2).

[25] Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M. and Halderman, J. A. (2014) Security Analysis of the Estonian Internet Voting System. In: *CCS '14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ACM. [online] Available from: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf [Accessed 16 June 2020].

[26] State Electoral Office of Estonia. (2017) *General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia*, Document: IVXV-ÜK-1.0, Tallin. [online] Available from: https://www.valimised.ee/sites/default/files/uploads/eng/IVXV-UK-1.0-eng.pdf [Accessed 16 June 2020].

[27] Stein, R. and Wenda, G. (2014) Das Zentrale Wählerregister – Ein skalierbares Instrument zur Bürgerbeteiligung mit 1:1-Verifikation. In: Plodereder, E., Grunske, L., Ull, D. and Schneider, E. (eds.). *44. Jahrestagung der Gesellschaft für Informatik.* INFORMATIK 2014, 22–26 September, Bonn. [online] Available from: https://subs.emis.de/LNI/Proceedings/Proceedings232/1427.pdf [Accessed 16 June 2020].

[28] White, I. and Coleman, Ch. (2011) *Postal Voting & Electoral Fraud*, SN/PC/3667, House of Commons Library.

<<< ARTICLES

COMMENTARY >>>

DOI 10.5817/MUJLT2020-2-7

ELECTRONIC EVIDENCE IN INTELLECTUAL PROPERTY DISPUTES UNDER THE COUNCIL OF EUROPE'S GUIDELINES

by

MAREK SWIERCZYNSKI[*], REMIGIJUS JOKUBAUSKAS[**]

On 30 January 2019 the Council of Europe adopted guidelines on electronic evidence in civil and administrative law accompanied by the Explanatory Memorandum. The authors summarize and analyse this soft law instrument with respect to intellectual property (hereinafter "IP") disputes. They explain why its creation is important for the proper administration of justice and how it addresses and reflects technological developments, new business models and evolving case-law. Several conclusions have been identified regarding how use of the Guidelines will address current practical problems for courts in IP disputes. Both authors took active part in the preparatory works and believe it is in the interest of justice and effective IP protection that these guidelines are publicly available in the member states and widely disseminated among professionals dealing with electronic evidence.

KEY WORDS

Council of Europe, Electronic Evidence, Intellectual Property Enforcement, Metadata

[*] m.swierczynski@uksw.edu.pl, Professor of Law at the Department of Civil Law and Private International Law of the Faculty of Law and Administration of the Cardinal Stefan Wyszyński University in Warsaw, Poland. He is the author of numerous scientific publications in the field of private international law, civil law, health law and IT law.

[**] remigijus@jokubauskas.org, PhD in Law candidate at Mykolas Romeris university, Lithuania. His principal areas of interests are civil proceedings, corporate insolvency law. He was selected to the *Fulbright Foreign Student Program* for the 2018–2019 academic year to undertake research in Law at the University of Missouri, Columbia, USA.

1. INTRODUCTION

Effective enforcement of intellectual property rights requires proper handling of electronic evidence in courts. In this respect EU Members States should adapt their court practice to the latest *Guidelines of the Council of Europe on electronic evidence in civil and administrative proceedings* dated 30 January 2019[1] (hereinafter the "CoE Guidelines"). This is particularly important due to the new rules on IP protection in the digital single market,[2] but also the factual considerations, such as digitalisation of the court proceedings accelerated due to coronavirus pandemic in 2020. We would like to canvass the difficult issues related to electronic evidence in IP disputes and the CoE Guidelines are in the centre of our concerns. *The Council of Europe* (hereinafter "the CoE") has, among other duties, the task of continuing the on-going reflexion about the development of the new information technologies (IT) to improve the efficiency of justice. The regulatory efforts of the CoE could lead to higher quality standards of civil procedures.

The objectives and principles set out in the rules for protection of IP rights in national systems remain still valid, but there is an urgent need to adapt the procedural standards to the new technological reality.[3] It is necessary to eliminate obstacles to effective management of electronic evidence in the national justice systems.[4] The shortcomings are due to the lack of common standards and the diversity and complexity of the taking of evidence procedures. The correct handling of electronic evidence in courts triggers practical difficulties.

Certain aspects may be emphasized. For example, the European courts tend to request printouts of the electronic evidence from the parties and ignore the significance of the metadata. Some courts reject or ignore upfront

---

1 Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings adopted by the Committee of Ministers on 30 January 2019, at the 1335th meeting of the Ministers' Deputies, CM(2018)169--add1final.

2 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* (L 130/92). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0790 [Accessed 3 February 2020].

3 Shackelford, S. and Raymond, A. (2014) Building the Virtual Courthouse: Ethical Considerations for Design, Implementation, and Regulation in the World of ODR. *Wisconsin Law Review*, 3, p. 615.

4 Cumming, G. et al. (2008) *Enforcement of intellectual property rights in Dutch, English and German civil courts*. Wolters Kluwer, p. 106.

evidence presented in electronic form. Other courts take very liberal approach and fail to test reliability of electronic evidence. There is also a question if the credibility of evidence would be better judged in a physical courtroom.

The case laws illustrates the difficulties with which the IP right holders encounter in practice.[5] The court typically requires the plaintiff to submit appropriate evidence stating that the defendant used protected goods to which the plaintiff has copyright. A general statement of the plaintiff on the use of the goods by the defendant seems not to be considered by the court as sufficient to prove the infringement of copyright. The plaintiff had to submit actual evidence to prove his claims.

There are good reasons to assume that electronic evidence become an increasingly common mean of proving the facts in IP disputes. In the past, it was predominantly concerned with conflicts arising from the use of the Internet, such as disputes over e-commerce transactions. Today, with accelerating digitalisation of courts it becomes a common practice. Therefore, we need to learn more about electronic evidence and establish effective ways how to prevent its destruction, manipulation or alteration. Such risks in IP disputes are particularly high due to intangible nature of protected goods.

As a result of the development of digital technologies, the role of the Internet increases as a major market for the distribution of and access to IP protected goods.[6] Nevertheless, many significant differences remain with regard the treatment of electronic evidence in IP cases under national laws. These differences do not merely reflect technical divergences between national legal systems. However, in recent years the digital market has become even more complex.[7] This is due to a mixture of concurrent factors such as the globalization of business and commerce, the increasing role of international providers of IP protected content (e.g. *Google*, *Netflix*, *Microsoft*), and the never-ending expansion of the Internet and other communication technologies.[8]

---

[5] Regional Court in Szczecin, VIII GC 509/14; Van Rhee, C: H. et al. (2018) *Transformation of Civil Justice, Ius Gentium: Comparative Perspectives on Law and Justice*. Springer, p. 70.

[6] Vaver, D. et al. (2010) *Intellectual Property in the New Millenium*. Cambridge, p. 20.

[7] Vică, C., Socaciu, E. (2019) Mind the Gap! How the Digital Turn Upsets Intellectual Property. *Science and Engineering Ethics*, 25, p. 248.

[8] Sciaudone, R. (2013) *Dealing with IP Matters in Cross-Border Cases. Journal of Intellectual Property Law & Practice*, 8 (4), p. 332.

The CoE Guidelines can be treated as an important supplement to international and regional rules on enforcing IP rights. In the EU the applicable rules can be found in the *Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights* (hereinafter "the Enforcement Directive") adopted on 29 April 2004[9], that contains a comprehensive regulation on issues related to evidence, including its gathering and securing (protection).[10] On international level this is the *TRIPS Agreement* that also contains provisions for the enforcement of intellectual property rights, including procedural measures for the protection of intellectual property rights in part III is entitled "Enforcement of rights intellectual property".

The aim of this paper is to answer the question how current national regulations on civil proceedings can be further adapted to the needs of the practice in the light of the CoE Guidelines. It should be noted that procedural frameworks differ between the member states, even when they regulate similar issues of electronic evidence.[11] The structure of this paper is as follows. We plan to answer this research question by presenting the solutions provided by the CoE Guidelines and recommending how it can be implemented to the national court practices. A major issue is the used normative framework (or more specifically lack thereof) as regards to the electronic evidence. The CoE Guidelines do not require the members states to amend the national law but we recommend to go step further and make such change.

2. WHAT CAN BE TREATED AS ELECTRONIC EVIDENCE IN IP DISPUTES?

The CoE Guidelines provide definitions of the key terms, including electronic evidence. Certainly, the definition of electronic evidence should be broad enough to cover all types of evidence, regardless of their origin. For the purposes of the CoE Guidelines, "electronic evidence" means any evidence of data contained in or generated by any device whose operation

[9] Michael, W. (2010) *European Copyright Law: A Commentary*. Oxford, New York: Oxford University Press; Stamatoudi, I. et al. (2014) *EU Copyright Law: A Commentary*. Edward Elgar Publishing, pp. 528–652; Pila, J. et al. (2019) *European Intellectual Property Law*. Second Edition. Oxford, New York: Oxford University Press, pp. 525–544.

[10] Cornish, W. R. et al. (2003) Procedures and Remedies for Enforcing IPRS: The European Commission's Proposed Directive. *European Intellectual Property Review*, 25 (10), p. 447.

[11] Micklitz, H. et al. (2012) *The European Court of Justice and the autonomy of the Member States*. Intersentia, pp. 281–323.

depends on software or data stored in a computer system or in a network or transmitted over a computer system or over a network.[12] We recommend adopting this definition in the national regulation on evidence.

There is no doubt that it is a broader concept than a document, a typical evidence submitted by the parties in IP disputes so far and explicitly defined in the national laws. This approach undergoes a change now as the new types of evidence are collected by the parties. Protected goods often include not only text but also visual images or sound for computer reading that are converted into bits in order to be transmitted over computer networks. An example is a website. From the technical point of view, it includes the source, result and database codes, and from the visual point of view: texts, graphic materials, animations, videos, sound sequences, etc.

What is even more important for the national regulator, under the CoE Guidelines electronic evidence relates to any method of data sharing. Whether online or stored on a computer, smartphone, separate hard drive, USB stick or stored using cloud computing services. There should be no distinction between data created in analogue or digital form and data created digitally. Therefore, scanned images or documents are also included in this definition.

In court practice, however, it happens that courts of lower instance fail to assess or even admit non-standard evidence presented by the claimant. In one of such cases *Polish Supreme Court* rightly pointed out that the *Polish Code of Civil Procedure* does not contain a closed catalogue of evidence and it is permissible to use any source of information on facts relevant to the decision on the case, as long as it is not contrary to the provisions of law.[13]

Undoubtedly, electronic evidence become more complex. Most of what we consider now as evidence in the courts is static. Such examples are documents or e-mails. However, more often courts deal with complex evidence, such as a multimedia, a record of an Internet session or the sophisticated system of linking. This new type of dynamic evidence requires much more experience and knowledge from both the parties' representatives and the courts. An example of technology used to secure

[12] This definition of electronic evidence is included in the "Definitions" section of the CoE Guidelines.

[13] The Supreme Court of Poland. (2008) I CSK 138/08, LEX No. 548795.

electronic evidence in intellectual property cases, that requires such knowledge, is blockchain[14] or evidence generated with use of artificial intelligence.

3. PECULIARITIES OF IP DISPUTES

The CoE Guidelines do not establish separate rules for electronic evidence in IP disputes. However, these disputes often involve electronic data and require specific legal and technical knowledge. The Enforcement Directive establishes specific rules for protection of IP holders in civil proceedings and recognizes that measures, procedures and remedies which ensure enforcement of intellectual property rights shall be effective, proportionate and dissuasive. *A. Kur and T. Dreier* underline that it lays down two specific provisions concerning evidence in IP disputes:

> *"access to evidence which is in the hands of the infringer (Article 6) and preservation of evidence (Article 7)".*[15]

It is however disputable whether the measures established in the Enforcement Directive are applicable to all IP disputes. For instance, whether it is applicable in case of peer-to-peer file sharing infringements and whether it is applicable to acts carried out on a commercial scale. Interestingly, in some legal traditions such "exploratory evidence" as established in Article 6 of the Enforcement directive is disputable. For instance, German civil law prohibits exploratory evidence (*Verbot des Ausforschungsbeweises*) since the underlying principle is that each party must plead and prove the facts (*Beibringungsgrundsatz*).[16] In Lithuania the plaintiff can ask the court to recover written evidence from participants in the proceedings or from other persons if they possess such evidence.[17] If the court's request to submit written evidence is not fulfilled and no substantial reasons for inability to submit evidence are presented or the court declare the reasons poor, the culprit persons may be imposed a fine within three hundred Euro.[18]

---

[14] Ito, K. et al. (2019) *A Critical Examination of the Application of Blockchain Technology to Intellectual Property Management*. Springer, p. 317.

[15] Kur, A. et al. (2013) *European Intellectual Property Law: Text, Cases and Materials*. Edward Elgar, p. 441.

[16] Cumming, G. et al. (2008) *Enforcement of intellectual property rights in Dutch, English and German civil courts*. Wolters Kluwer, p. 230.

[17] Article 199(1) of the Code of Civil Procedure of the Republic of Lithuania.

[18] Article 199(6) of the Code of Civil Procedure of the Republic of Lithuania.

One of the peculiarities of IP disputes is that the infringer is often in control of the relevant data and it may be difficult for the plaintiff to produce *prima facie* evidence of the infringement. The Enforcement Directive employs the term "control" in Article 6 which itself raises some practical dilemmas. For instance, how the word "control" should be interpreted? Does it cover evidence which is only in possession of the opposing party and (or) also evidence which are controlled by the third party? Even if the opposing party has the evidence, does it have to exercise any request which would require substantial costs? It seems that in such cases a clear answer is impossible. *The European Commission* suggests that in IP disputes the opposing party should carry out a diligent search for the evidence within its organization and it should be proportionate and not abusive.[19]

Furthermore, IP disputes are generally complex, involving difficult legal and factual questions and multiple parties. In practice it can be difficult for the plaintiff to specify evidence which are in possession of the opposing party or a third person and satisfy court's request to specify the exact nature, location, reference numbers or contents of the requested documents.[20] The "excessive level of detail" which the plaintiff has to specify what evidence the court should demand from other persons may hinder effectiveness of civil proceedings and "fair and equitable" nature of such requirements.[21] Therefore, though the plaintiff should specify certain evidence which the court should request as specific as possible, this duty shall be interpreted within the reasonable limits, in light of the specifics of the case at hand.[22] The national laws establish that court may order to present evidence upon a reasonable request from a party.[23] Also, in some member states the national regulation imposes an obligation

---

[19] Guidance on certain aspects of Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights COM (2017) 708 final. *Official Journal of the European Union* (COM(2017)708), pp. 12–13. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0708 [Accessed 7 February 2020].

[20] Ibid.

[21] Ibid.

[22] Ibid.

[23] Support study for the *ex post* evaluation and *ex ante* impact analysis of the IPR enforcement Directive (IPRED). *Publications Office of the EU*, pp. 179–184. [online] Available from: https://op.europa.eu/en/publication-detail/-/publication/1e3b2f41-d4ba-11e7-a5b9-01aa75ed71a1 [Accessed 23 January 2020].

to preserve electronic data when as soon as the litigation is commenced in order to avoid spoliation of relevant data.[24]

Particularly complex are disputes when infringements are committed online. For instance, infringements committed by using peer-to-peer file sharing protocols[25] which involve a number of infringers. In such disputes the use of electronic evidence is almost inevitable and the types of electronic evidence in IP disputes may be ubiquitous: IP addresses, information on websites and, information possessed in the respondent's and (or) third parties' servers ("cloud computing"), software programs. Moreover, electronic evidence may be possessed by the opposing party or a third person, likely in another jurisdiction.[26]

The CoE Guidelines recommend the member states to consider the peculiarities of electronic documents and amend the national laws on evidence accordingly. Also, the guidelines emphasize the importance of effective case management from the courts. The effective case management requires consideration whether certain proves of the validity of electronic evidence is required (for instance, shall be party submit the relevant metadata or a printout of the document is sufficient). The guidelines also recommend considering the practical issues of collection of electronic evidence which are in possession on the third party, such as the provider of trust services.

4. METADATA IN IP DISPUTES

Metadata is indispensable from electronic evidence.[27] The CoE Guidelines establish that metadata is significant for the courts when dealing with

[24] Practice direction 31b relating to disclosure of electronic documents in civil proceedings prepared for UK courts. [online] Available from: https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part31/pd_part31b) [Accessed 7 February 2020]. *"As soon as litigation is contemplated, the parties' legal representatives must notify their clients of the need to preserve disclosable documents. The documents to be preserved include Electronic Documents which would otherwise be deleted in accordance with a document retention policy or otherwise deleted in the ordinary course of business."*

[25] In a P2P network, the "peers" are computer systems which are connected to each other via the Internet. Files can be shared directly between systems on the network without the need of a central server. In other words, each computer on a P2P network becomes a file server as well as a client. While P2P networking makes file sharing easy and convenient, is also has led to a lot of software piracy and illegal music downloads. See The Computer Dictionary. [online] Available from: https://techterms.com/definition/p2p [Accessed 23 February 2020].

[26] Support study for the *ex post* evaluation and *ex ante* impact analysis of the IPR enforcement Directive (IPRED). *Publications Office of the EU*, p. 54. [online] Available from: https://op.europa.eu/en/publication-detail/-/publication/1e3b2f41-d4ba-11e7-a5b9-01aa75ed71a1 [Accessed 23 January 2020].

[27] Mason, S. et al. (2017) *Electronic evidence*. Institute of Advanced Legal Studies, p. 27.

electronic evidence.[28] Generally speaking, metadata is electronic information about other electronic information (data about data).[29] Metadata is usually created automatically by the software and without user's knowledge.[30] *The Explanatory memorandum*[31] recognizes that metadata contains some evidentiary value of electronic data (the date and time of creation or modification of a file or document, or the author and the date and time of sending the data) and it is usually not directly accessible.[32] We recommend that member states adopt such definition of the metadata in national regulation.

A practical dilemma is not only what information metadata may reveal, but also how it can be retrieved. Metadata is often hidden in the electronic file and is viewed only when the file is viewed in its native form. In some cases, special software may be necessary to retrieve metadata and courts may need technological expertise.

One of the common blunders in civil proceedings is submission of the content of a webpage (so-called "screenshots") to the court. It may be particularly tempting to present printouts of the screenshots as evidence in IP disputes when the infringement is committed online. Though it might me a rather easy task from the technological point of view, the credibility of such information is doubtful since "screenshots" do not guarantee that information is correct and precise. Courts usually rely on electronic data presented in a human-readable format, e.g. printed on paper. Printing out "screenshots" means a loss of valuable metadata. The printout is merely a copy of the screen display and it can be modified in a very simple manner without special software or hardware requirements. Therefore, it could hardly be recognized as reliable electronic evidence or the basis for the expert's verification of authenticity and equal treatment of the parties to the dispute.[33] *S. Mason* is correct in his argument that even if we correctly

---

[28] Article 8 of the CoE Guidelines. Courts should be aware of the probative value of metadata and of the potential consequences of not using it.

[29] CoE Guidelines defines metadata as electronic information about other electronic data, which may reveal the identification, origin or history of the evidence, as well as relevant dates and times; Mason, S. et al. (2017) *Electronic evidence*. Institute of Advanced Legal Studies, p. 27.

[30] Ibid.

[31] Council of Europe. (2019) *The Explanatory Memorandum to the Guidelines*. [online] Available from: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680902e0e [Accessed 3 April 2020].

[32] Article 12 of the Explanatory memorandum.

[33] Article 17 of the Explanatory memorandum.

identify the carrier of original evidence carrier and rely on physical objects only, such as printouts, they may have no value at all or limited value unless a party to the dispute confirms their significance and the features that make them relevant.[34] Unsurprisingly, some national courts find that screenshots are not trustworthy.[35] Under the CoE Guidelines, the printouts are to be recognised as a secondary proof (copy) in the sense that originally they exist in electronic form.[36]

Nevertheless, evidence in civil proceedings should be defined in a broad sense, encompassing virtually any information. Due to the widespread use and easy collection of "screenshots" the parties can submit them as evidence in civil proceedings. Depending on the national laws, "screenshots" may be accepted, if it is sufficiently visible and precise and comply with certain procedural safeguards.[37] Also, it should not raise difficulties, if the other party does not dispute such evidence and it complies with the general rules for admissibility and legitimacy of evidence in civil proceedings. *The Explanatory Memorandum* establishes that in case a printout of electronic evidence is filed, the court may order, at the request of a party or on its own initiative, provision of the original of the electronic evidence by the relevant person.[38] The court should also consider the principles of proportionality and economy of litigation and should not demand excessive metadata.

To conclude, we recommend that the member states should adopt these principles regarding the significance of metadata for evidentiary purposes in the national regulations. In particular this refers to Article 8 of the CoE Guidelines that reads:

> *"Courts should be aware of the probative value of metadata and of the potential consequences of not using it".*

---

[34] Mason, S. et al. (2017) *Electronic evidence*. Institute of Advanced Legal Studies, p. 27.

[35] Court of Appeal of Lithuania. (2018) e2A-226-516/2018.

[36] See Articles 8 and 9 of the Explanatory Memorandum.

[37] Guidance on certain aspects of Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights COM (2017) 708 final. *Official Journal of the European Union* (COM(2017)708), p 22. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0708 [Accessed 7 February 2020].

[38] Article 23 of the Explanatory Memorandum.

5. TAKING OF EVIDENCE IN IP DISPUTES AND ITS RELIABILITY

Taking of electronic evidence is a challenging task which may significantly impact the course of the civil proceedings. The Enforcement Directive lays down no practical rules how electronic evidence in IP disputes should be collected, meaning that the national rules for taking of evidence in civil proceedings are applicable. The recent report reveals that the courts of the EU Member States collect electronic evidence in IP disputes in three forms:

1. establishment of the infringement and appointment of an expert;
2. description;
3. seizure.[39]

Thus, courts rely either on the submission of electronic evidence by the parties or appoint an expert to collect such data.

The major difficulties in taking of evidence in IP disputes are:

1. taking evidence in cross-border cases;
2. excessive costs among the member states for production of evidence;
3. inconsistency of information among the member states;
4. different national legislation for production and preservation of evidence.[40]

Obtaining and securing electronic evidence, as well as using evidence in the cross-border context, has proved to particularly challenge the effectiveness of the Enforcement Directive.[41] In the digital environment, cross-border use of intellectual property is becoming increasingly common. The dissemination of IP protected goods on the Internet is inherently cross--border in nature. Only mechanisms adopted at the international level, such

---

[39] Support study for the *ex post* evaluation and *ex ante* impact analysis of the IPR enforcement Directive (IPRED). *Publications Office of the EU*, p. 54. [online] Available from: https://op.europa.eu/en/publication-detail/-/publication/1e3b2f41-d4ba-11e7-a5b9-01aa75ed71a1 [Accessed 23 January 2020].

[40] Op. cit., p. 284.

[41] Guidance on certain aspects of Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights COM (2017) 708 final. *Official Journal of the European Union* (COM(2017)708), p. 10. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0708 [Accessed 7 February 2020].

as *Council of Europe*, can ensure the proper functioning of the market of digital goods.[42]

The solutions to these issues are not simple. The existing rules of the *Regulation on taking of evidence*[43] establishes a model for the co-operation among the courts of the EU Member States in taking of evidence in cross-border civil cases. Nevertheless, it seems that practical issues in taking evidence in cross-border cases are hardly avoidable. Also, the recognition of electronic evidence collected in one member state may be disputable in another. The CoE Guidelines recognize that courts should co-operate in the cross-border taking of evidence.[44] Therefore, taking of evidence in IP disputes may be particularly complicated due to the complexity of the disputes, but also involvement of "a cross-border element" which almost inevitably require a close co-operation between the national courts.

We recommend that member states should adopt in particular the following principles in the national regulations in accordance with the CoE Guidelines:[45]

1. Electronic evidence should be collected in an appropriate and secure manner, and submitted to the courts using reliable services, such as trust services.[46]
2. Having regard to the higher risk of the potential destruction or loss of electronic evidence compared to non-electronic evidence, member states should establish procedures for the secure seizure and collection of electronic evidence.

---

[42] Blakeney, M. (2004) International intellectual property jurisprudence after TRIPS. In: Vaver, D., Bently, L. (eds.). *Intellectual Property in the New Millenium*. Cambridge, p. 5.

[43] Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters. *Official Journal of the European Union* (L 174). Available from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32001R1206 [Accessed 3 February 2020].

[44] Article 13 of the CoE Guidelines

[45] Articles 10–16 of the CoE Guidelines.

[46] Trust services play a critical role in the identification, authentication and security of online transactions. The definition of "trust service" can be found in Article 3 (16) of the Regulation (EU) No 910/2014 of the European Parliament and Council of 23 July 2014. *Official Journal of the European Union* (L 257). Available from: https://eur-lex.europa.eu/eli/reg/2014/910/oj [Accessed 3 March 2020]. In the CoE guidelines, reference is also made to specific trust services related to "simple", "advanced" or "qualified" electronic signatures and certificates, which implies possible application of other definitions adopted in the eIDAS Regulation. Secure mechanisms include, in particular: i) certificates to electronic signatures; ii) confirmations by the payment system operator; iii) public trust services providing technological mechanisms that ensure proper authentication of the data source.

3. Courts should be aware of the specific issues that arise when dealing with the seizure and collection of electronic evidence abroad, including in cross-border cases.[47]
4. Courts should co-operate in the cross-border taking of evidence. The court receiving the request should inform the requesting court of all the conditions, including restrictions, under which evidence can be taken by the requested court.
5. Electronic evidence should be collected, structured and managed in a manner that facilitates its transmission to other courts, in particular to an appellate court.
6. Transmission of electronic evidence by electronic means should be encouraged and facilitated in order to improve efficiency in court proceedings.[48]
7. Systems and devices used for transmitting electronic evidence should be capable of maintaining its integrity.

Electronic evidence has unique properties that distinguish it from traditional paper evidence. The method of storage and the type of information relevant to evidence are subject to changes due to the use of different electronic devices. The collection and presentation of evidence in its original electronic form in court requires necessary expertise. Still, electronic evidence retains the general characteristics of the evidence. Therefore, the general rules on evidence should continue to be applied. The general principles of the law of evidence should not be ignored, but applied to electronic evidence, taking into consideration the uniqueness and technical aspects of electronic evidence bearing in mind the discretionary power of the judge.

Another complicated issue regarding taking of evidence in IP cases is protection of personal data.[49] This issue is complex and deserves a separate analysis. In this paper we would like only to state that IP rights are not absolute and protection of the fundamental right to property, which

[47] Good example in case of IP dispute is use of data sharing (clouds) technology. It has become a common security technique. The global nature of the internet and the growing use of cloud services make it increasingly difficult to assume that access to data is strictly domestic in nature.

[48] As further explained in Article 33 of the Explanatory Memorandum. Encouragement and facilitation of the transmission of electronic evidence by electronic means can be achieved through implementation of common technical standards, files formats and digitisation of domestic judicial and administrative systems. Having regard to the higher risk of destruction of electronic evidence, local procedures should be adopted which permit secure transmission of electronic evidence.

includes the rights linked to intellectual property, must be balanced against the protection of other fundamental rights.[50] Thus, a fair balance between protection of IP and protection of the fundamental rights of individuals who are affected by the measures which protect IP holders should be found.[51]

6. CONCLUSIONS

IP right owners are entitled to effective legal protection.[52] In the case of exploitation of IP protected goods in the digital environment, it becomes more difficult. Online transmission of books, music, films and computer programs enable the use of goods at any time and without geographical limitations. It is becoming increasingly problematic for IP rights holders to assert their rights. There is a high risk that rights holders give up their claims at all. Those who bring an action with little evidence to support their claims are not able to win the case because it is impossible to prove the real extent of the damage without all the evidence available. That is why courts must exercise caution when dealing with electronic evidence in such cases.

Due process is determined not only by legal but also by technological aspects. Therefore, a more technological approach and practical to the regulation of electronic evidence is necessary. For example, regulations should safeguard the reliability of electronic evidence. A solution to these shortcomings could be seen in uniform application of the CoE Guidelines. These standards specify both the legal and the technological requirements for the electronic evidence and serve as a complementary regulatory tool.

Our recommendations for the member states are following. Due to the relevance and nature of electronic evidence the national legislation should define electronic evidence and thus separate it from the other types of evidence. Such definition should encompass the major traits of electronic evidence as established in the CoE Guidelines. Also, because

---

[49] Support study for the *ex post* evaluation and *ex ante* impact analysis of the IPR enforcement Directive (IPRED). *Publications Office of the EU*, p. 54. [online] Available from: https://op.europa.eu/en/publication-detail/-/publication/1e3b2f41-d4ba-11e7-a5b9-01aa75ed71a1 [Accessed 23 January 2020].

[50] Judgment of 2010 November 24. *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, ECLI:EU:C:2011:771, paragraph 44.

[51] Op. cit., para. 45.

[52] Ohly, A. (2009) *Three Principles of European IP Enforcement Law: Effectiveness, Proportionality, Dissuasiveness*. Larcier, pp. 257–274.

of the increasing importance of metadata and technical problems associated with it, we suggest that the national regulation should adopt definition of metadata. Moreover, the courts should be aware that the content of a webpage may not be sufficient to prove certain facts since they lack metadata. It is particularly important in IP disputes in which the parties often present various screenshots. The court should be aware how metadata collected and stored.

The treatment of electronic evidence shall be different from other types of evidence. The effective case management and enforcement of IP rights are particularly important since the information related to electronic evidence may be abroad in possession of the third party.

Also, the national law should specify taking of electronic evidence since their collection and submission to the court. In many cases the IP disputes involve various countries and the cooperation between national institutions may be inevitable. The practical issue is storage of electronic evidence in courts. In countries in which electronic case management systems are not used all evidence shall be printed out meaning that crucial elements such as metadata may be lost. The adoption in national law of a common and comprehensive regulation of proceedings concerning the handling of electronic evidence in IP disputes on the basis of the CoE Guidelines would facilitate the application of the procedural rules and specify the differences between these proceedings and the general principles.

LIST OF REFERENCES

[1] Blakeney, M. (2004) International intellectual property jurisprudence after TRIPS. In: Vaver, D., Bently, L. (eds.). *Intellectual Property in the New Millenium*. Cambridge.

[2] Van Rhee, C. H. et al. (2018) *Transformation of Civil Justice, Ius Gentium: Comparative Perspectives on Law and Justice*. Springer.

[3] Code of Civil Procedure of the Republic of Lithuania.

[4] Cornish, W. R. et al. (2003) Procedures and Remedies for Enforcing IPRS: The European Commission's Proposed Directive. *European Intellectual Property Review*, 25 (10).

[5] Council of Europe. (2019) *The Explanatory Memorandum to the Guidelines*. [online] Available from: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680902e0e [Accessed 3 April 2020].

[6] Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters. *Official*

Journal of the European Union (L 174). Available from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32001R1206 [Accessed 3 February 2020].

[7] Court of Appeal of Lithuania. (2018) e2A-226-516/2018.

[8] Cumming, G. et al. (2008) *Enforcement of intellectual property rights in Dutch, English and German civil courts*. Wolters Kluwer.

[9] 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* (L 130/92). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0790 [Accessed 3 February 2020].

[10] Guidance on certain aspects of Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights COM (2017) 708 final. *Official Journal of the European Union* (COM(2017)708). Available from: https://eur-lex. europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0708 [Accessed 7 February 2020].

[11] Ito, K. et al. (2019) *A Critical Examination of the Application of Blockchain Technology to Intellectual Property Management*. Springer.

[12] Judgment of 2010 November 24. *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, ECLI:EU:C:2011:771.

[13] Kur, A. et al. (2013) *European Intellectual Property Law: Text, Cases and Materials*. Edward Elgar.

[14] Mason, S. et al. (2017) *Electronic evidence*. Institute of Advanced Legal Studies.

[15] Micklitz, H. et al. (2012) *The European Court of Justice and the autonomy of the Member States*. Intersentia.

[16] Michael, W. (2010) *European Copyright Law: A Commentary*. Oxford, New York: Oxford University Press.

[17] Ohly, A. (2009) *Three Principles of European IP Enforcement Law: Effectiveness, Proportionality, Dissuasiveness*. Larcier.

[18] Pila, J. et al. (2019) *European Intellectual Property Law*. Second Edition. Oxford, New York: Oxford University Press.

[19] Practice direction 31b relating to disclosure of electronic documents in civil proceedings prepared for UK courts. [online] Available from: https://www.justice.gov.uk/courts/ procedure-rules/civil/rules/part31/pd_part31b) [Accessed 7 February 2020].

[20] Regional Court in Szczecin, VIII GC 509/14.

[21] Regulation (EU) No 910/2014 of the European Parliament and Council of 23 July 2014. *Official Journal of the European Union* (L 257). Available from: https://eur-lex.europa.eu/eli/reg/2014/910/oj [Accessed 3 March 2020].

[22] Sciaudone, R. (2013) Dealing with IP Matters in Cross-Border Cases. *Journal of Intellectual Property Law & Practice*, 8 (4).

[23] Shackelford, S. and Raymond, A. (2014) Building the Virtual Courthouse: Ethical Considerations for Design, Implementation, and Regulation in the World of ODR. *Wisconsin Law Review*, 3.

[24] Stamatoudi, I. et al. (2014) *EU Copyright Law: A Commentary*. Edward Elgar Publishing.

[25] Support study for the ex-post evaluation and ex-ante impact analysis of the IPR enforcement Directive (IPRED). *Publications Office of the EU*. [online] Available from: https://op.europa.eu/en/publication-detail/-/publication/1e3b2f41-d4ba-11e7-a5b9-01aa75ed71a1 [Accessed 23 January 2020].

[26] The Computer Dictionary. [online] Available from: https://techterms.com/definition/p2p [Accessed 23 February 2020].

[27] The Supreme Court of Poland. (2008) I CSK 138/08, LEX No. 548795.

[28] Vaver, D. et al. (2010) *Intellectual Property in the New Millenium*. Cambridge.

[29] Vică, C., Socaciu, E. (2019) Mind the Gap! How the Digital Turn Upsets Intellectual Property. *Science and Engineering Ethics*, 25.

<<< COMMENTARY

BOOK REVIEWS >>>

DOI 10.5817/MUJLT2020-2-8

THE ENERGY CHARTER TREATY: A COMMENTARY. HOBÉR, K.

by

MARTIN ŠVEC*

Hobér, K. (2020) The Energy Charter Treaty: A Commentary. Oxford: Oxford University Press, 688 p.

This book examines the *Energy Charter Treaty*, one of the most important sources of international energy law. The Energy Charter Treaty (referred to also as "ECT" or "Treaty") provides a multilateral framework for energy cooperation that is unique under international law. It was signed in December 1994 and entered into force four years later, in April 1998. Being inspired by the *European Energy Charter*, a declaration of political intent to promote East-West energy cooperation,[1] the ECT is based on the principles of open and competitive energy markets. The ECT covers five broad areas in the energy sector: trade; transit; protection and promotion of foreign energy investments; environmental protection and energy efficiency. Moreover, the Treaty aims to create conditions favourable to private investment. The Treaty includes mechanisms for the resolution of state-to-state and investor-to-state disputes. To date, the ECT has been signed or acceded to by 53 states (European and Asian) as well as the European Union and *Euratom*. Due to its complexity and geographical coverage, the ECT is a document unique in its kind.

The Energy Charter Treaty: A Commentary, published under the *Oxford University Press*, represents an in-depth, article-by-article commentary on all aspects of the Treaty. The book provides a thorough analysis of all ECT's provisions, relevant case law, arbitral awards, and academic scholarship. Its

* svec.martin@yahoo.com, Department of Energy Law, Institute of Law and Technology, Faculty of Law, Masaryk University, The Czech Republic.

1 Konoplyanik, A., Walde, T. (2006) Energy Charter Treaty and Its Role in International Energy. *Journal of Energy & Natural Resources Law*, 24 (4).

author, *Kaj Hobér*, is an Associate Member of *3 Verulam Buildings*, a barristers' chambers, and Professor of International Investment and Trade Law at *Uppsala University*. As an arbitrator, *Prof. Hobér* has been appointed to panels in more than 200 international arbitrations, commercial as well as treaty based, across a variety of tribunals.[2]

The Energy Charter Treaty has gained increasing attention in recent years. First, the use of the ECT investor-state dispute settlement mechanisms (referred to also as "ISDS") has been increasing rapidly.[3] It is worth acknowledging that the Energy Charter Treaty is currently the most often-invoked investment agreement worldwide.[4] Second, a backlash against ISDS encompassing criticism of both the system of investment treaty arbitration and criticism of its specific aspects (e.g. transparency, inconsistency of awards),[5] is likely to affect an ongoing modernisation of the ECT.[6] Third, the *Court of Justice of the European Union* (referred to also as "CJEU") in its judgment of 6 March 2018 in Case C-284/16, *Achmea v. Slovakia* held that the investor-state arbitration clauses in international investment agreements concluded between EU member states were not compatible with EU law. Although the Court did not address the ECT, most of the EU member states are of the opinion that the ECT's investor-state arbitration clause is also incompatible with EU law.[7] However, to date, in all publicly known arbitral awards rendered since 6 March 2018, tribunals found that they had jurisdiction and rejected the argument that the Energy

---

[2] 3 Verulam Buildings. (2020) *3VB*. [online] Available from: https://www.3vb.com/our-people/associate-members/prof.-dr.-kaj-hober [Accessed 1 September 2020].

[3] As of 15 July 2020, the total number of publicly known *ISDS* claims has more than doubled over the last six years and reached 131. See Energy Charter Treaty. (2020) [online] Available from: https://www.energychartertreaty.org/cases/list-of-cases/ [Accessed 1 September 2020].

[4] Verburg, C. (2019) Modernising the Energy Charter Treaty: An Opportunity to Enhance Legal Certainty in Investor-State Dispute Settlement. *The Journal of World Investment & Trade*, 20 (2–3), pp. 425–454. [online] Available from: https://doi.org/10.1163/22119000-12340144 [Accessed 1 September 2020].

[5] Hobér, K. (2015) Investment Treaty Arbitration and Its Future – If Any. *Yearbook on Arbitration & Mediation*, 7 (8). [online] Available from: https://elibrary.law.psu.edu/cgi/viewcontent.cgi?article=1030&context=arbitrationlawreview [Accessed 1 September 2020].

[6] The EU aims to reform the ECT's investor-to-state dispute settlement mechanism in line with the EU's work in the ongoing multilateral reform process in the *United Nations Commission on International Trade Law (UNCITRAL)*. See European Commission. (2020) *Commission presents EU proposal for modernising Energy Charter Treaty*. Publications Office of the European Union. [online] Available from: https://trade.ec.europa.eu/doclib/press/index.cfm?id=2148 [Accessed 1 September 2020].

[7] Declaration of the Member States of 15 January 2019 on the legal consequences of the Achmea judgment and on investment protection. (2019) [online] Available from: https://ec.europa.eu/info/publications/190117-bilateral-investment-treaties_en [Accessed 1 September 2020].

Charter Treaty is not applicable between EU member states.[8] It is worth mentioning that the compatibility of the ECT's investor-state arbitration clause with EU law is currently contested before a national court – *Svea Court of Appeal* in Sweden.[9] However, the court rejected the request to obtain a preliminary ruling from the CJEU.[10] Fourth, the EU aims to ensure that the ECT contributes to the objectives of the *Paris Agreement* and better reflects climate change and clean energy transition goals, and facilitates a transition to a low-carbon energy system.[11] Against the background of recent developments in EU law and international law, a thorough legal analysis of the ECT's provisions and recent case law is more than timely. *The Energy Charter Treaty: A Commentary* will be undoubtedly a helpful resource for practitioners, academics, and policymakers.

As noted above, the Energy Charter Treaty is a sector-specific treaty. It comprises of provisions regulating the trade and transit of energy products and materials, providing for investment protection of energy investments, and promoting energy efficiency and environmental protection. In other words, the ECT comprises of legal standards having origins in different fields of international law, particularly international economic law, international investment law and international environmental law. As *Prof. Hobér* aptly points out, the ECT was not drafted in legal vacuum and legal fields whose instruments were incorporated into the ECT cannot be ignored.[12] As far as investment protection is concerned, there were in place several thousands of international investment agreements providing for

[8] Švec, M. (2019) The Energy Charter Treaty as a Key Instrument of International Energy Law: The 20th Anniversary of the Energy Charter Treaty's Entry into Force. *Časopis pro právní vědu a praxi*, 27 (4), pp. 519–538. [online] Available from: https://journals.muni.cz/cpvp/article/view/12525 [Accessed 1 September 2020].

[9] See Decision by the Svea Court of Appeal, 25 April 2019, Case No. T 4658-18. [online] Available from: https://www.arbitration.sccinstitute.com/Swedish-Arbitration-Portal/Court-of-Appeal/Court-of-Appeal/Court-of-Appeal/d_3646301-decision-by-the-svea-court-of-appeal-25-april-2019-case-no.-t-4658-18 [Accessed 1 September 2020].

[10] Liebkind, A., Agrell, K. (2020) *The Swedish Court of Appeal again rejects Spain's request of a preliminary ruling from the Court of Justice of the European Union (CJEU)*. Global Arbitration News. [online] Available from: https://jusmundi.com/en/document/decision/en-novenergia-ii-energy-environment-sca-grand-duchy-of-luxembourg-sicar-v-the-kingdom-of-spain-decision-of-the-svea-court-of-appeal-wednesday-27th-may-2020 [Accessed 1 September 2020].

[11] European Commission. (2020) *Commission presents EU proposal for modernising Energy Charter Treaty*. Publications Office of the European Union. [online] Available from: https://trade.ec.europa.eu/doclib/press/index.cfm?id=2148 [Accessed 1 September 2020]; Švec, M. (2019) The Energy Charter Treaty as a Key Instrument of International Energy Law: The 20th Anniversary of the Energy Charter Treaty's Entry into Force. *Časopis pro právní vědu a praxi*, 27 (4), pp. 519–538. [online] Available from: https://journals.muni.cz/cpvp/article/view/12525 [Accessed 1 September 2020].

[12] See p. 1 of the book.

the protection of foreign investment in a manner very similar to the corresponding provisions which eventually found their way into the ECT. Regarding international economic law, the ECT explicitly incorporated legal standards of the *GATT* and the *WTO*. Hence, acknowledging significant volumes of legal commentary in relation to both international economic and international investment law, *Prof. Hobér* sought to elaborate only on general aspects of these two legal fields, which are particularly relevant for the ECT's provisions in question. By the same token, the book addresses only arbitration issues specifically concerning the provisions of the ECT. With respect to some general matters, the reader is referred to other scholarly publications. As stated in the book's *Introduction*, striking this balance has been a challenge.[13]

The book is composed of five introductory chapters presenting the Energy Charter Treaty as a source of international law and exploring its background as well as the negotiating history. Subsequent nine chapters offer an article-by-article commentary to the ECT. More specifically, Chapter 2 provides a brief introduction of the ECT, Chapter 3 explores the background and the negotiating history of the ECT, Chapter 4 presents general rules of interpretation enshrined in the *Vienna Convention on the Law of Treaties* and Chapter 5 is focused on rules of attribution. Chapters 6–14 provide a legal analysis of all provisions of the Energy Charter Treaty. In order to make the book's structure easy-to-follow, these Chapters are divided into following Parts: *The Preamble*; *Definitions and Purpose*; *Commerce*; *Investment Promotion and Protection*; *Miscellaneous Provisions*; *Dispute Settlement*; *Transitional Provisions*; *Structure and Institutions*; and *Final Provisions*. At the very end of the book the reader finds following documents: *Final Act of the European Energy Charter Conference*; *European Energy Charter*; *The Energy Charter Treaty*; *Decisions Relating to the Final Act of the European Energy Charter*; *Protocol on Energy Efficiency and Related Matters*; *Final Act of the International Conference*; and *Decision of the Energy Charter Conference*.

Chapter 4 is focused on the interpretation of the Energy Charter Treaty pursuant to the *Vienna Convention on the Law of Treaties* (referred to also as "VCLT"). However, although it is widely accepted that the VCLT reflects customary international law, the reviewer is of the opinion that the book

[13] See pp. 1–2 of the book.

should explicitly notify that France, Iceland and Norway, contracting parties to the ECT, have neither signed nor ratified the VCLT.

With respect to Chapter 5, the reviewer strongly disagrees with the author's conclusion that only states can be responsible for any breaches of the ECT. In fact, an important distinctive feature of the ECT is that not only states but also regional economic integration organisations (REIOs) may become contracting parties to the Treaty. Accordingly, the author should have implied that even international organisation can be responsible for breaches of the ECT. Hence, Chapter 5 should have dealt with both the *ILC Articles on Responsibility of States for Internationally Wrongful Acts* and the *ILC Articles on Responsibility of International Organisations for Internationally Wrongful Acts*. Such analysis would be particularly helpful in the context of an investment arbitration against the EU under the Energy Charter Treaty recently initiated by *Nord Stream 2 AG*.[14]

With respect to Chapters 6–14, the commentary on each article follows the same structure. The author first establishes the object, purpose and meaning of each provision, relevant parts of the *travaux préparatoires* are referred to when necessary. What makes the book extraordinarily useful are detailed references to relevant case law and jurisprudence, i.e. to arbitral awards rendered on the basis of the ECT as per 1 January 2019 and which were in the public domain as per such date.[15]

The Energy Charter Treaty: A Commentary, authored by *Prof. Hobér*, represents the second commentary on the Energy Charter Treaty published in recent years. In contrast to *The Commentary on the Energy Charter Treaty*, edited by *Rafael Leal-Arcas*, published by *Elgar Commentaries* in 2018, *Prof. Hobér's* book is more than just another article-by-article commentary. His book also covers the context of the negotiations of the ECT and discusses its interpretation. The reviewer particularly appreciates detailed, logical and comprehensive analysis of ECT's provisions accompanied by references to relevant case law and jurisprudence.

All that being said, *Prof. Hobér's* commentary will undoubtedly become an important and helpful book for anyone dealing with international energy law. Nonetheless, the reviewer regrets that the author did not discuss the present challenges the ECT has been facing, particularly the ECT's role

[14] *Nord Stream 2 AG v. The European Union*, PCA Case No 2020-07, pending. [online] Available from: https://www.italaw.com/cases/8187 [Accessed 1 September 2020].

[15] See p. 1 of the book.

in the effort to hold the increase in global average temperature below 2° C above pre-industrial levels. The underlying policy rationale of the ECT is to be neutral as to the sources of the energy. In other words, fossil-fuel investments are treated no differently to renewable energy investments.[16] Hence, international obligations arising from the ECT, such as the obligation to accord fair and equitable treatment to energy investments and to compensate for direct or indirect expropriation may discourage governments to decarbonize their energy sector. The energy sector is the largest contributor to global GHG emissions and regulatory chill can be major obstacle for the successful implementation of the *Paris Agreement*.[17] Potential use of the ECT's investor-state dispute settlement mechanism by the fossil fuel industry may effectively stall action on climate change.[18] Therefore, the EU aims to ensure the ECT better reflects climate change and clean energy transition goals and facilitates a transition to a low-carbon energy system.[19]

In addition, since the book is more than just an article-by-article commentary and the author explores the background and the negotiating history of the ECT, the reviewer would appreciate some remarks on the ongoing efforts to modernise the ECT. More specifically, in 2017 a subgroup on ECT modernisation was established in order to conduct discussions on the potential modernisation of the Treaty.[20] In November 2018, the *Energy Charter Conference* approved the list of topics for the discussion on the modernization of the ECT, including pre-investment; definition of charter; definition of economic activity in the energy sector; definition of investment; definition of investor; right to regulate; definition of fair and equitable treatment; MFN clause; clarification of most constant protection and security; definition of indirect expropriation; compensation

[16] Bernasconi-Osterwalder, N., Brauch, M. D. (2019) *Redesigning the Energy Charter Treaty to Advance the Low-Carbon Transition*. Transnational Dispute Management. [online] Available from: https://www.transnational-dispute-management.com/article.asp?key=2632 [Accessed 1 September 2020].

[17] Tienhaara, K. (2018) Regulatory Chill in a Warming World: The Threat to Climate Policy Posed by Investor-State Dispute Settlement. *Transnational Environmental Law*, 7 (2), pp. 229–250. [online] Available from: https://doi.org/10.1017/S2047102517000309 [Accessed 1 September 2020].

[18] Ibid.

[19] European Commission. (2020) *Commission presents EU proposal for modernising Energy Charter Treaty*. Publications Office of the European Union. [online] Available from: https://trade.ec.europa.eu/doclib/press/index.cfm?id=2148 [Accessed 1 September 2020].

[20] International Energy Charter. (2020) *Modernisation Group*. [online] Available from: https://www.energycharter.org/who-we-are/subsidiary-bodies/modernisation-group/ [Accessed 1 September 2020].

for losses; umbrella clause; denial of benefits; transfers related to investments; frivolous claims; transparency; security for costs; valuation of damages; third party funding; sustainable development and corporate social responsibility; definition of transit; access to infrastructure; definition and principles of tariff setting; regional economic integration organisation; and obsolete provisions.[21]

LIST OF REFERENCES

[1] 3 Verulam Buildings. (2020) *3VB*. [online] Available from: https://www.3vb.com/our-people/associate-members/prof.-dr.-kaj-hober [Accessed 1 September 2020].

[2] Bernasconi-Osterwalder, N., Brauch, M. D. (2019) *Redesigning the Energy Charter Treaty to Advance the Low-Carbon Transition.* Transnational Dispute Management. [online] Available from: https://www.transnational-dispute-management.com/article.asp?key=2632 [Accessed 1 September 2020].

[3] Decision by the Svea Court of Appeal, 25 April 2019, Case No. T 4658-18. [online] Available from: https://www.arbitration.sccinstitute.com/Swedish-Arbitration-Portal/Court-of-Appeal/Court-of-Appeal/Court-of-Appeal/d_3646301-decision-by-the-svea-court-of-appeal-25-april-2019-case-no.-t-4658-18 [Accessed 1 September 2020].

[4] Declaration of the Member States of 15 January 2019 on the legal consequences of the Achmea judgment and on investment protection. (2019) [online] Available from: https://ec.europa.eu/info/publications/190117-bilateral-investment-treaties_en [Accessed 1 September 2020].

[5] Energy Charter Treaty. (2020) [online] Available from: https://www.energycharter treaty.org/cases/list-of-cases/ [Accessed 1 September 2020].

[6] European Commission. (2020) *Commission presents EU proposal for modernising Energy Charter Treaty*. Publications Office of the European Union. [online] Available from: https://trade.ec.europa.eu/doclib/press/index.cfm?id=2148 [Accessed 1 September 2020].

[7] Hobér, K. (2015) Investment Treaty Arbitration and Its Future – If Any. *Yearbook on Arbitration & Mediation*, 7 (8). [online] Available from: https://elibrary.law.psu.edu/cgi/viewcontent.cgi?article=1030&context=arbitrationlawreview [Accessed 1 September 2020].

[8] International Energy Charter. (2020) *Approved topics for the modernisation of the Energy Charter Treaty*. [online] Available from: https://www.energychartertreaty.org/modernisation-of-the-treaty/ [Accessed 1 September 2020].

[21] International Energy Charter. (2020) *Approved topics for the modernisation of the Energy Charter Treaty*. [online] Available from: https://www.energychartertreaty.org/modernisation-of-the-treaty/ [Accessed 1 September 2020].

[9] International Energy Charter. (2020) *Modernisation Group*. [online] Available from: https://www.energycharter.org/who-we-are/subsidiary-bodies/modernisation-group/ [Accessed 1 September 2020].

[10] Konoplyanik, A., Walde, T. (2006) Energy Charter Treaty and Its Role in International Energy. *Journal of Energy & Natural Resources Law*, 24 (4).

[11] Liebkind, A., Agrell, K. (2020) *The Swedish Court of Appeal again rejects Spain's request of a preliminary ruling from the Court of Justice of the European Union (CJEU)*. Global Arbitration News. [online] Available from: https://jusmundi.com/en/document/decision/en-novenergia-ii-energy-environment-sca-grand-duchy-of-luxembourg-sicar-v-the-kingdom-of-spain-decision-of-the-svea-court-of-appeal-wednesday-27th-may-2020 [Accessed 1 September 2020].

[12] *Nord Stream 2 AG v. The European Union*, PCA Case No 2020-07, pending. [online] Available from: https://www.italaw.com/cases/8187 [Accessed 1 September 2020].

[13] Švec, M. (2019) The Energy Charter Treaty as a Key Instrument of International Energy Law: The 20th Anniversary of the Energy Charter Treaty's Entry into Force. *Časopis pro právní vědu a praxi*, 27 (4). [online] Available from: https://journals.muni.cz/cpvp/article/view/12525 [Accessed 1 September 2020].

[14] Tienhaara, K. (2018) Regulatory Chill in a Warming World: The Threat to Climate Policy Posed by Investor-State Dispute Settlement. *Transnational Environmental Law*, 7 (2). [online] Available from: https://doi.org/10.1017/S2047102517000309 [Accessed 1 September 2020].

[15] Verburg, C. (2019) Modernising the Energy Charter Treaty: An Opportunity to Enhance Legal Certainty in Investor-State Dispute Settlement. *The Journal of World Investment & Trade*, 20 (2–3). [online] Available from: https://doi.org/10.1163/22119000-12340144 [Accessed 1 September 2020].

DOI 10.5817/MUJLT2020-2-9

ONLINE COURTS AND THE FUTURE OF JUSTICE. SUSSKIND, R. E.

by

ANNA BLECHOVÁ[*], PAVEL LOUTOCKÝ[**]

Susskind, R. E. (2019) Online Courts and the Future of Justice. Oxford: Oxford University Press, 368 p.

1. INTRODUCTION

> *"More people in the world now have access to the internet than access to justice. According to OECD, only 46 per cent of human beings live under the protection of the law."*[1, 2]

This statement could be seen as the main reason, why the treatise such as *Online Courts and the Future of Justice* is more than actual. *Richard E. Susskind* dedicated almost four decades to the work and research on the utilization of technology within the courts, which is also proven by his plentiful publication activity.[3]

In the introduction of the book, the author is pointing out that the topic of online courts is stirring some emotions especially in legal circles because of its conservative environment. Since it is thorny issue, it is crucial to keep

[*] 458594@mail.muni.cz, master student of the Faculty of Law, Masaryk University, The Czech Republic.

[**] loutocky@law.muni.cz, legal specialist and post doc at the Institute of Law and Technology, Faculty of Law, Masaryk University, lawyer and research specialist at Faculty of Informatics, Masaryk University, The Czech Republic.

[1] According to *Statista.com*, 59 % of the global population has access to the Internet. Clement, J. (2020) *Worldwide digital population as of July 2020.* [online] Available from: https://www.statista.com/statistics/617136/digital-population-worldwide/ [Accessed 1 August 2020].

[2] Susskind, R. (2019) *Online Courts and the Future of Justice*. Oxford: Oxford University Press, p. 27.

[3] For example, Susskind, R. (1996) *The Future of Law*. Oxford: Oxford University Press; Susskind, R. (2000) *Transforming the Law*. Oxford: Oxford University Press; Susskind, R. (2017) *Tomorrow's Lawyers.* Second Edition. Oxford: Oxford University Press.

an open mind about approach to the topic.[4] *Susskind's* book is in fact not about replacing human judges by the computer ones but about exploring the potential of the online courts – online decision-making process,[5] extension of the courts and digital transformation of the court system to better serve the public. The improvement of the access to the courts should be seen as the main philosophy of the online courts. According to *Susskind's* idea of online courts, he recommends firstly to focus on the minor conflicts (especially low-value civil disputes). Subsequently the knowledge would be transferred to more challenging tasks (criminal law disputes or "hard cases"[6]).

The book is divided into four parts. The first part is called *Court and Justice*, and it explains what is the purpose and value of court systems, the access to justice, if it is time to make a change and how to use technology to reach these goals. The second part of the book is called *Is Court Service or a Place?* and it is developing the central vision of the book – the idea of the architecture of online courts. The third part is focusing on obstacles when building online courts and it is called *The Case Against*. The most innovative part is the last one which is called *The Future*. In this review, we are respecting the order of the book and our comments and observations follow the same structure.

2. COURT AND JUSTICE

The importance of the courts is significant and the author of the book is emphasising it by the explanation of the jurisprudential function and constitutional significance.[7] The motivation for innovating the court system is however not only because of the fact that in some jurisdictions it is under staggering backlogs, but also because the justice should be available to everyone.[8] *Susskind* is stating that the ways how to change rooted system

[4] Susskind, R. (2019) *Online Courts and the Future of Justice*. Oxford: Oxford University Press, p. 3.

[5] According to *Susskind's* opinion, understanding online judging involves determination of cases by human judges but not in physical courtrooms. He is also mostly trying to exclude a videoconferencing, or any other synchronous communication and he is favouring written submissions. Moreover, online judging shall be (by his opinion) conducted via online platform where all the evidences and arguments will be submitted and subsequently the decision will be delivered. Op. cit., pp. 116–117.

[6] To see more on that: Dworkin, R. (1975) Hard Cases. *Harvard Law Review*, 88 (6), p. 1060 *et seq*.

[7] Susskind, R. (2019) *Online Courts and the Future of Justice*. Oxford: Oxford University Press, pp. 19–25.

[8] Op. cit., pp. 27–29.

are two – automatization of known operations and transformation of processes.[9] The first mentioned method is about changing the repetitive, routine tasks in the way that humans will be able to focus on more challenging aspects and they will not be overloaded by routine. The transformation of processes is then targeting revolutionary scenarios like creating an online court. *Susskind's* idea of online court(s) consists of the virtual instrument which would be based on textual description of the dispute only.[10] The decisions then would be (still) made by the human judge, however in cooperation with predictive systems. Even though this technology will be able to save time, money and human resources, it is also important to mention its drawbacks.

The author of the book is aware of some of them, but he is not paying enough attention, in our opinion, for example to biases[11] in more complex way, technological aspect of the issue, partly open texture of the law or the level of quality of written submissions.[12] We would thus stress out (not only in connection with online courts) that especially the connection and cooperation between the lawyers and computer scientists will be crucial in the future (and it is crucial already in the moment).

If, according to *Susskind's* model, online courts will be developed, it will mean that algorithm will help with the preparing the case, predicting the possible outcome, evaluating inserted data. Human beings, judges included, are biased. The architecture of prediction algorithms is by default unbiased since it is just code without feelings, memories, cultural background or knowledge of history (if the algorithm is biased it is not the fault of the system but of its creator).[13] Similar applies also to the processed datasets. The de-biasing of the dataset is theoretically possible and, in our opinion, if the system will be free of such defects, it will

---

[9] Op. cit., p. 34.

[10] Op. cit., p. 60.

[11] Završnik, A. (2019) Algorithmic justice: Algorithms and big data in criminal justice setting. *European Journal of Criminology*, 20 (1). [online] Available from: https://journals.sagepub.com /doi/pdf/10.1177/1477370819876762 [Accessed 1 August 2020].

[12] To see more on these issues e.g.: Scherer, M. (2019) Artificial Intelligence and Legal Decision-Making: The Wide Open? *Journal of International Arbitration*, 36 (5), p. 554 *et seq.*; Surden, H. (2018) Machine Learning and Law. *Washington Law Review*, 89 (1), p. 105; or historically D'Amato, A. (1977) Can/Should Computers Replace Judges? *Georgia Law Review*, 11, p. 1300 *et seq*.

[13] Završnik, A. (2019) Algorithmic justice: Algorithms and big data in criminal justice setting. *European Journal of Criminology*, 20 (1), p. 11. [online] Available from: https://journals.sage pub.com/doi/pdf/10.1177/1477370819876762 [Accessed 1 August 2020].

be potentially able (and will be prepared) to offer more transparent and objective outputs.

According to *Caliskan, Bryson and Narayanan* also the language itself is naturally biased.[14] This means that since one of the inputs (the language) is by its nature biased it is almost impossible to have an unbiased product at the end. Moreover, there is a dilemma concerns whether de-biasing is desirable. One aspect is the architecture of the de-biasing procedure ("cleaning algorithm"), the second aspect to decide what is exactly a bias (or which part of algorithm / dataset is biased). This entails a series of inherent "political" decisions which will answer the questions as to what should be "cleaned", what is sexist, which word is unacceptable.[15] These questions and problems are unfortunately resonating in the book just under the lines and *Susskind* is not focusing on them. Nevertheless, in our opinion these are very important because of the previously mentioned fact that the law (and generally the language even more) has open texture and character.

Susskind is mentioning the prejudice of the legal practitioners who are against the transformation of the system.[16] These people are, in our eyes, not open-minded enough to the concept of online courts. Nevertheless, more interesting point is the bias of the machine involved, which is not sufficiently mentioned in the book.

As further mentioned in the book, the online courts are built on the written submissions – this could however collide with the idea of access to justice. The author understands access to justice as much more than providing faster, cheaper and less combative mechanism for resolving disputes. *Susskind* claims that the system of online courts could help to avoid disputes and could have a greater insight into the benefits that the law can confer. Citizens in the future will be able to own and manage their legal disputes at online courts (write submissions, manage the dispute without the intervention of somebody else). The access to justice will thus

[14] Caliskan, A., Bryson, J. J., Narayanan, A. (2017) Semantics derived automatically from language corpora contain human-like biases. *Science*, 356 (6334), p. 185. [online] Available from: https://science.sciencemag.org/content/sci/356/6334/183.full.pdf [Accessed 1 August 2020].

[15] Završnik, A. (2019) Algorithmic justice: Algorithms and big data in criminal justice setting. *European Journal of Criminology*, 20 (1), p. 11. [online] Available from: https://journals.sagepub.com/doi/pdf/10.1177/1477370819876762 [Accessed 1 August 2020].

[16] Susskind, R. (2019) *Online Courts and the Future of Justice*. Oxford: Oxford University Press, p. 44.

increase,[17] also because such submissions and using online courts is only a possibility not obligation.[18] Nevertheless, we think that this idea could be met only if the laypeople would be able to write and manage their submissions effectively. But that could be a difficult task. The main issues are the use of accurate language and "evaluating" or "presenting" the evidence. Laypeople are not trained to identify which information could be relevant and which is not. The solution to that problem could be some assistance offered by the online court (guide, documentation or personal assistance).

3. IS COURT A SERVICE OR A PLACE?

One of the important questions of the book is *If the Court is a Service or a Place?* The answer to this question is a crucial element for digitalisation and *Susskind* sees it as a service.

The architecture of the innovative court system by *Susskind* is, without a doubt, unique. He is describing a four-layer model which includes three tiers.[19] Firstly, there is a layer of "dispute resolution". In this layer, it is possible to find traditional courts, virtual hearings. The second layer is "dispute containment", which contains mainly alternative ways to settle the dispute and tools connected with classical understanding of online dispute resolution (ODR). The other two layers are "dispute avoidance" and "legal health promotion", and they have no plausible equivalent in current legal systems.[20]

The tiers are divided by *Susskind* into the *Tier 1*, the *Tier 2* and the *Tier 3*. The aim of the *Tier 1* is to organise and classify the problems of the people. Some of the goals of this tier are to help laypeople to fully understand their problem, rights and duties and also to guide them through possible remedies available to them.[21] This aim could be fulfilled via the system of decision trees. It is important to mention that we already have a tool that could help the courts with such a task – *Susskind* is using a concrete

[17] Op. cit., p. 70.

[18] This has been already proven in out-of-court online dispute resolution. To see more on that: Loutocký, P. (2016) Online Dispute Resolution to Resolve Consumer Disputes from the perspective of European Union Law: Is the Potential of ODR Fully Used? *Masaryk University Journal of Law and Technology*, 10 (1), pp. 113–127.

[19] Susskind, R. (2019) *Online Courts and the Future of Justice*. Oxford: Oxford University Press, pp. 113–119.

[20] Op. cit., pp. 113–116.

[21] Op. cit., pp. 117–118.

example of Resolver.[22, 23] *Tier 1* is more about giving a legal advice, which is not compatible with the typical agenda of courts. There is an objective reason to assume that the private sector would be involved in *Tier 1* as well.[24]

Tier 2 is containing a dispute resolution but necessarily not only with the involvement of a judge. The central figure of this tier is a "case officer". This person will be trying to settle the dispute (to help achieving the agreement). Case officer would act as a mediator and their main goal would be to prevent the litigation and settle and manage the dispute. *Susskind* is emphasising that they should not act as "lite" judges,[25] however, it is questionable if it is possible to fulfil this condition. The case officers will probably need a legal education at least on some level. The principle of *Tier 2* has been already used in the court system of England and Wales for online civil money claims and also by *Canadian Civil Resolution Tribunal*.[26]

Suggested tools and principles in *Tier 1* and *Tier 2* are exceeding the scope of the current court system and also their time and human sources in the moment. Prevention should be however better than *ex post* reaction, and well-set system of *Tier 1* and *Tier 2* will be able to reduce the involvement of judges in many cases, thus transformation of the court capacities is important.[27] Conversely, the easy access and affordability of justice through *Tier 1* and *Tier 2* could trigger an enormous interest in litigations. Moreover, if the tiers would not be appropriately set, the system will collapse.[28] This is however not primarily a disadvantage and we see the great potential in ODR tools, where it is proven, that rising number of disputes does not lead to limiting the resolution but helps the users not to be afraid of dealing with their problems.[29] Also already working scenarios (e.g. *Civil Resolution Tribunal* in Canada) prove that *Tier 1*

---

[22] Op. cit., p. 126.

[23] For example, Resolver. [online] Available from: https://www.resolver.co.uk [Accessed 1 August 2020].

[24] Susskind, R. (2019) *Online Courts and the Future of Justice*. Oxford: Oxford University Press, pp. 127–128.

[25] Op. cit., p. 137.

[26] For example Civil Resolution Tribunal. [online] Available from: https://civilresolutionbc.ca/ [Accessed 1 August 2020].

[27] Susskind, R. (2019) *Online Courts and the Future of Justice*. Oxford: Oxford University Press, p. 141.

[28] The author of the book is opposing this argument in chapter 22. Op. cit. pp. 224–226.

[29] Rule, C. (2012) Quantifying the Economic Benefits of Effective Redress: Large E-Commerce Data Sets and the Cost-Benefit Case for Investing In Dispute Resolution. *University of Arkansas at Little Rock Law Review*, 24 (4), p. 772 *et seq*.

and *Tier 2* can eliminate (even by involving the negotiation phase between the parties) many simple cases and the court (and especially the judges themselves) is only dealing with fraction of the initiated cases.[30]

Last tier is described as the online litigation, which involves a human judge. Nevertheless, the dispute should be still completely led online and based on written submissions.[31]

There are concerns that judging online is not possible. This argument is supported by the cases like *The Queen v. Dudley and Stephens*.[32] "Hard cases" containing moral dilemmas or difficult ethical questions require special attention. Online courts are according to *Susskind* primarily focused on quick settlement of "easy" cases. This approach will let human judges to focus just on hard cases. The question is if the system will be able to distinguish in *Tier 1* between the "hard" and "easy" cases.[33]

In the last chapter of this part, *Susskind* introduces the successful projects similar to online courts. He is mentioning examples like systems in China, Australia, Canada or England and Wales.[34] On the other hand, the author is surprisingly ignoring situation within the European Union, for example approaches in Denmark or Estonia.[35]

---

[30] Almost 85 % of the cases were resolved in *Tier 1* and *Tier 2* by *Civil Resolution Tribunal*. Rozenberg, J. *The Civil Resolution Tribunal. The Online Court: will IT work?* The Legal Education Foundation. [online] Available from: https://long-reads.thelegaleducation foundation.org/ [Accessed 1 August 2020].

[31] For the first generation of online courts, there would be no involvement of "AI" judges or predictive systems in the *Tier 3*. However, the *Tier 3* has potential space for it in the next generations of online courts.

[32] *Dudley and Stephenson* is an English criminal law case, which is challenging the justification of cannibalism. The main idea of the case is if it is murder of fellow crew member justifiable under specific circumstances or not. *Regina v. Dudley and Stephens*, 14 Q.B.D. 273 (1884). [online] Available from: https://cyber.harvard.edu/eon/ei/elabs/majesty/stephens.html [Accessed 1 August 2020].

[33] Susskind, R. (2019) *Online Courts and the Future of Justice*. Oxford: Oxford University Press, pp. 146–147.

[34] Op. cit., pp. 165–176.

[35] See CEPEJ European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment. [online] Available from: https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment [Accessed 1 August 2020]; or Justice of the future: predictive justice and artificial intelligence. [online] Available from: https://www.coe.int/en/web/cepej/justice-of-the-future-predictive-justice-and-artificial-intelligence [Accessed 1 August 2020]; Vasdani, T. (2019) *From Estonian AI judges to robot mediators in Canada, U.K.* LexisNexis. [online] Available from: https://www.lexisnexis.ca/en-ca/ihc/2019-06/from-estonian-ai-judges-to-robot-mediators-in-canada-uk.page [Accessed 1 August 2020]; Numa, A. (2020) *Artificial intelligence as the new reality of e-justice*. [online] Available from: https://e-estonia.com/artificial-intelligence-as-the-new-reality-of-e-justice/ [Accessed 1 August 2020]; Danmarks Domstole. [online] Available from: https://www.minretssag.dk/frontpage [Accessed 1 August 2020].

The main criticism to this part of the book is the lack of the technological aspect. The author is introducing his vision of the online court system, but he is not focusing on the technologies he suggests to involve.

4. THE CASE AGAINST

Since online courts are quite a sensitive topic, *Susskind* is pre-empting the possible opposing arguments by dedicating a whole part III of the book to this topic. This part of the book is in our view very important as it is trying to break traditional stereotypes connected with use of the online technologies in the justice. The author of the book is discussing issues as economy-class justice, transparency, human face of justice, fair trial, digital exclusion, public sector technology and jurisprudential miscellany. However, especially this part of the book is just scratching the surface. Susskind is not dealing with each problem in depth.

Another topic is the human face of justice. Question is if we need a contact with human being judge from flesh and bones, or it would be possible to accept a decision through the computer. This is more a psychology question than legal one, but still, it should be at least partly considered. The human element in justice in online courts is in the book compared to the online psychotherapy sessions. *Susskind* is arguing through psychotherapist *Yalom* that when text psychotherapy could be such a success, online courts would be the same.[36, 37] Understandably, patients of psychotherapy are preferring texting over videoconferencing or calling. The texting is giving them a time to think about their message and they can hide behind their phones or computer. The comparison to psychotherapy is however in our opinion unfortunate. Psychotherapy is not litigation. The main purpose of the court system is finding the justice and it is crucial that the judge will be able to find it. According to acquisition of information, the human judge or psychotherapist could reach some information via body language or immediate responses. In the online court system, this would not be possible anymore.

On the other hand, the potential dispute settlement online has been already discovered by some private providers of ODR (it seems more

[36] Yalom, I. (2017) *Becoming Myself: A Psychiatrist's Memoir*. Basic Books, p. 306.

[37] Susskind, R. (2019) *Online Courts and the Future of Justice*. Oxford: Oxford University Press, pp. 210–214.

important to offer the solution than to meet face to face)[38]; these aspects are however not mentioned in the book.[39]

The last topic we would like to mention is the digital exclusion. According to *Susskind*, objection to online courts is that many people do not have access to the Internet, or they do not have a necessary level of computer literacy.[40] Nevertheless, he is emptying this argument by the fact that even non-users of the Internet are indirect beneficiaries of the internet.[41] He suggests that less confident users should be assisted by online guidance, which will solve the problem with the lack of computer literacy. To support his conclusion, *Susskind* mentions several statistics.[42] Even though *Susskind's* argumentation seems convincing we are critical about it. Firstly, *Susskind* relies on statistics and data relevant only to the United Kingdom. Secondly, he overlooks the digital skills gap in Europe.[43] Lastly, *Susskind* is not making any difference between consuming the social media and using an online court.

5. THE FUTURE

The last part of the book is dedicated to the emerging technologies, AI, computer judges and the global challenge. As the author mentions this final part is about his predictions.[44] This approach caused the fact that some of his ideas are not supported by any relevant source. The author of the book is firstly exploring the emerging technologies as telepresence, augmented reality or advanced ODR. He believes that these technologies could be used in the current courtrooms.[45]

Another chapter is dedicated to the artificial intelligence (AI) and its impact to future of online courts. Even though *Susskind* is highlighting that

---

[38] Rule, C. (2012) Quantifying the Economic Benefits of Effective Redress: Large E-Commerce Data Sets and the Cost-Benefit Case for Investing in Dispute Resolution. *University of Arkansas at Little Rock Law Review*, 24 (4), pp. 767–777, p. 772 *et seq*.

[39] To see more on that: Loutocký, P. (2019) Online Dispute Resolution as an Inspiration for Contemporary Justice. *Jusletter IT. Die Zeitschrift für IT und Recht*, pp. 1–8, p. 2 *et seq*.

[40] Susskind, R. (2019) *Online Courts and the Future of Justice*. Oxford: Oxford University Press, p. 215.

[41] Op. cit., p. 216.

[42] Op. cit., pp. 216–218.

[43] According to data from 2017 *"*[…] *169 million Europeans between 16 and 74 years – 44 % – do not have basic digital skills.*" DG Connect, "The Digital skills Gap in Europe", Digital Single Market. [online] Available from: https://ec.europa.eu/digital-single-market/en/news/digital-skills-gap-europe [Accessed 1 August 2020].

[44] Susskind, R. (2019) *Online Courts and the Future of Justice*. Oxford: Oxford University Press, p. 253.

[45] *Cisco's* telepresence, op. cit., pp. 255–258.

he has been focusing his research to AI and law, he is not consistent and specific about the "AI" systems he is proposing to use for example in the *Tier 3*. He is briefly describing the different concepts of AI, its history and breakthroughs, but he is not explaining how the AI works.[46] We consider this lack of explanation of technological aspect and clear definition of AI as shortcoming of the book.

Subsequently, the author points out the "AI fallacy"; the view that only way to get machines to outperform the best human lawyers is to copy the way that human lawyers work. He claims that this is not a good approach to AI in this context.[47] We think that such author's idea is exciting, but since the programmers of AI will be humans, it is challenging to imagine how AI could overcome this problem. Humans will program the machine in the way how humans understand the law and legal procedures. If we are then talking about different view (using neuron networks or quantum computing), this should be introduced in the book (and not ignored).

Penultimate chapter of the book is about the computer judge. *Susskind* is examining the question *Can machines replace human judges?*, but he is not giving a clear answer to it.[48] Nevertheless, he is more focusing on prediction machines. Even though, *Susskind* is dealing with moral boundaries of AI replacing judges he is not mentioning the moral boundaries of predictive systems. He also barely writes about bias problems of these systems[49] and he is ignoring their deficiencies, for example racial profiling[50], privacy threads[51] or misunderstanding of causal relationships[52].

6. CONCLUSION

The *Online Court and the Future of Justice* is a great and complex introduction and a guide to the topic. *Susskind* is mentioning many of his bright ideas

[46] Op. cit., pp. 263–272.

[47] Op. cit., pp. 272–273.

[48] Op. cit., pp. 278–281.

[49] Op. cit., p. 289.

[50] Crawford, K., Schultz, J. (2013) Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College Law Review*, 55 (93). [online] Available from: https://ssrn.com/abstract=2325784 [Accessed 1 August 2020].

[51] Stroud, M. (2014) *The minority report: Chicago's new police computer predicts crimes, but is it racist?* The Verge. [online] Available from: https://www.theverge.com/2014/2/19/5419854/the-minority-report-this-computer-predicts-crime-but-is-it-racist [Accessed 1 August 2020].

[52] Sgaier, S., Huang, V., Charles, G. (2020) The Case for Causal AI. *Stanford Social Innovation review*, 18 (3). [online] Available from: https://ssir.org/articles/entry/the_case_for_causal_ai# [Accessed 1 August 2020].

and experiences and the language of the book is accessible for general public. The book is easy to read and easy to understand which is hard to achieve in such a complex topic.

Despite that, some of the issues just scratch the surface and the author is not developing his ideas in a depth. This is however understandable for the sake of consistency and length of the book. The significant shortcoming of the book is the lack of the technological aspect of suggested online court tools and systems. The author of the book is not explaining how the system will work. Moreover, we believe that since the online courts would be closely associated with technology, as predictive systems or AI in the future, it is crucial to dedicate some part of the book to understand the systems and suggested technologies. In the best scenario this part of the book should have been a cooperation with computer scientists.

On the other hand, we are convinced that the suggested automatization and autonomous systems are a step in the right direction. Despite the criticism, the book is the only complex work on online courts. In conclusion, if there is any desire to understand the future of justice, we have to recommend this book as one of the important foundations.

LIST OF REFERENCES

[1] Caliskan, A., Bryson, J. J., Narayanan, A. (2017) Semantics derived automatically from language corpora contain human-like biases. *Science*, 356 (6334). [online] Available from: https://science.sciencemag.org/content/sci/356/6334/183.full.pdf [Accessed 1 August 2020].

[2] CEPEJ European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment. [online] Available from: https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment [Accessed 1 August 2020].

[3] Civil Resolution Tribunal. [online] Available from: https://civilresolutionbc.ca/ [Accessed 1 August 2020].

[4] Clement, J. (2020) *Worldwide digital population as of July 2020*. [online] Available from: https://www.statista.com/statistics/617136/digital-population-worldwide/ [Accessed 1 August 2020].

[5] Crawford, K., Schultz, J. (2013) Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College Law Review*, 55 (93). [online] Available from: https://ssrn.com/abstract=2325784 [Accessed 1 August 2020].

[6] D'Amato, A. (1977) Can/Should Computers Replace Judges? *Georgia Law Review*, 11.

[7] Danmarks Domstole. [online] Available from: https://www.minretssag.dk/frontpage [Accessed 1 August 2020].

[8] DG Connect, "The Digital skills Gap in Europe", Digital Single Market. [online] Available from: https://ec.europa.eu/digital-single-market/en/news/digital-skills-gap-europe [Accessed 1 August 2020].

[9] Dworkin, R. (1975) Hard Cases. *Harvard Law Review*, 88 (6).

[10] Justice of the future: predictive justice and artificial intelligence. [online] Available from: https://www.coe.int/en/web/cepej/justice-of-the-future-predictive-justice-and-artificial-intelligence [Accessed 1 August 2020].

[11] Loutocký, P. (2019) Online Dispute Resolution as an Inspiration for Contemporary Justice. *Jusletter IT. Die Zeitschrift für IT und Recht*.

[12] Loutocký, P. (2016) Online Dispute Resolution to Resolve Consumer Disputes from the perspective of European Union Law: Is the Potential of ODR Fully Used? *Masaryk University Journal of Law and Technology*, 10 (1).

[13] Numa, A. (2020) *Artificial intelligence as the new reality of e-justice*. [online] Available from: https://e-estonia.com/artificial-intelligence-as-the-new-reality-of-e-justice/ [Accessed 1 August 2020].

[14] *Regina v. Dudley and Stephens*, 14 Q.B.D. 273 (1884). [online] Available from: https://cyber.harvard.edu/eon/ei/elabs/majesty/stephens.html [Accessed 1 August 2020].

[15] Resolver. [online] Available from: https://www.resolver.co.uk [Accessed 1 August 2020].

[16] Rozenberg, J. *The Civil Resolution Tribunal. The Online Court: will IT work?* The Legal Education Foundation. [online] Available from: https://long-reads.thelegaleducation foundation.org/ [Accessed 1 August 2020].

[17] Rule, C. (2012) Quantifying the Economic Benefits of Effective Redress: Large E-Commerce Data Sets and the Cost-Benefit Case for Investing in Dispute Resolution. *University of Arkansas at Little Rock Law Review*, 24 (4).

[18] Scherer, M. (2019) Artificial Intelligence and Legal Decision-Making: The Wide Open? *Journal of International Arbitration*, 36 (5).

[19] Sgaier, S., Huang, V., Charles, G. (2020) The Case for Causal AI. *Stanford Social Innovation review*, 18 (3). [online] Available from: https://ssir.org/articles/entry/the_case_for_causal_ai# [Accessed 1 August 2020].

[20] Stroud, M. (2014) *The minority report: Chicago's new police computer predicts crimes, but is it racist?*. The Verge. [online] Available from: https://www.theverge.com/2014/2/19/54198

54/the-minority-report-this-computer-predicts-crime-but-is-it-racist [Accessed 1 August 2020].

[21] Surden, H. (2018) Machine Learning and Law. *Washington Law Review*, 89 (1).

[22] Susskind, R. (1996) *The Future of Law*. Oxford: Oxford University Press.

[23] Susskind, R. (2000) *Transforming the Law*. Oxford: Oxford University Press.

[24] Susskind, R. (2017) *Tomorrow's Lawyers.* Second Edition. Oxford: Oxford University Press.

[25] Susskind, R. (2019) *Online Courts and the Future of Justice*. Oxford: Oxford University Press.

[26] Vasdani, T. (2019) *From Estonian AI judges to robot mediators in Canada, U.K.* LexisNexis. [online] Available from: https://www.lexisnexis.ca/en-ca/ihc/2019-06/from-estonian-ai-judges-to-robot-mediators-in-canada-uk.page [Accessed 1 August 2020].

[27] Yalom, I. (2017) *Becoming Myself: A Psychiatrist's Memoir*. Basic Books.

[28] Završnik, A. (2019) Algorithmic justice: Algorithms and big data in criminal justice setting. *European Journal of Criminology*, 20 (1). [online] Available from: https://journals.sagepub.com/doi/pdf/10.1177/1477370819876762 [Accessed 1 August 2020].

MUJLT Official Partner (Czech Republic)

ROWAN LEGAL, advokátní kancelář s.r.o.
www.rowanlegal.com/cz/

Cyberspace 2019 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