

# MASARYK UNIVERSITY JOURNAL OF LAW AND TECHNOLOGY

VOLUME 13 | NUMBER 1 | SUMMER 2019 | ISSN 1802-5943

PEER REVIEWED



## CONTENTS:

MÜLLER-TÖRÖK | DYMITRUK  
KIKERPILL | SIIBAK | TANODOMDEJ | GOLUBEVA  
DROGOZIUK | GALAJDOVÁ | LOUTOCKÝ

[www.muji.lt.law.muni.cz](http://www.muji.lt.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](http://www.mujlt.law.muni.cz)

### **Editor-in-Chief**

Jakub Harašta, Masaryk University, Brno

### **Deputy Editor-in-Chief**

Jan Zibner, Masaryk University, Brno

### **Founding Editor**

Radim Polčák, Masaryk University, Brno

### **Editorial Board**

Tomáš Abelovský, Swiss Re, Zurich

Zsolt Balogh, Corvinus University, Budapest

Michael Bogdan, University of Lund

Joseph A. Cannataci, University of Malta | University of Groningen

Josef Donát, ROWAN LEGAL, Prague

Julia Hörnle, Queen Mary University of London

Josef Kotásek, Masaryk University, Brno

Leonhard Reis, University of Vienna

Naděžda Rozehnalová, Masaryk University, Brno

Vladimír Smejkal, Brno University of Technology

Martin Škop, Masaryk University, Brno

Dan Jerker B. Svantesson, Bond University, Gold Coast

Markéta Trimble, UNLV William S. Boyd School of Law

Andreas Wiebe, Georg-August-Universität Göttingen

Aleš Završnik, University of Ljubljana

### **Editors**

Lenka Pastušková, Ondřej Woznica

### **Official Partner (Czech Republic)**

ROWAN LEGAL, advokátní kancelář s.r.o. ([www.rowanlegal.com/cz/](http://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](http://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](http://www.heinonline.org))

listed in Scopus ([www.scopus.com](http://www.scopus.com))

reg. no. MK ČR E 17653

# MASARYK UNIVERSITY JOURNAL OF LAW AND TECHNOLOGY

VOLUME 13 | NUMBER 1 | SUMMER 2019

## LIST OF ARTICLES

<b>Robert Müller-Török:</b> The Principles Established by the Recommendation CM/Rec(2017)5 on Standards for E-voting Applied to Other Channels of Remote Voting .....	3
<b>Maria Dymitruk:</b> The Right to a Fair Trial in Automated Civil Proceedings .....	27
<b>Kristjan Kikerpill, Andra Siibak:</b> Living in a Spamster's Paradise: Deceit and Threats in Phishing Emails .....	45
<b>Papawadee Tanodomdej:</b> The Tallinn Manuals and the Making of the International Law on Cyber Operations .....	67
<b>Nelli Golubeva, Kristina Drogoziuk:</b> Web-page Screenshots as an Evidence in Civil Procedure of Ukraine .....	87

## LIST OF BOOK REVIEWS

<b>Dominika Galajdová:</b> Rethinking the Jurisprudence of Cyberspace. Reed, C.; Murray, A. ....	115
<b>Pavel Loutocký:</b> 3D Printing and Beyond: Intellectual Property and Regulation. Mendis, D.; Lemley, M.; Rimmer, M. (eds.). ....	123



DOI 10.5817/MUJLT2019-1-1

# THE PRINCIPLES ESTABLISHED BY THE RECOMMENDATION CM/REC(2017)5 ON STANDARDS FOR E-VOTING APPLIED TO OTHER CHANNELS OF REMOTE VOTING

by

ROBERT MÜLLER-TÖRÖK\*

*E-voting is highly suspicious to many citizens and institutions. Past pilot implementations ended before Supreme Courts and mostly not in favour of e-voting. Beside these political and legal battles regarding e-voting, postal voting seems to be commonly accepted and not in question. Motivated by a landmark ruling of the Austrian Constitutional Court in 2016,<sup>1</sup> which led to the revocation of the run-off elections result due to irregularities with postal voting, this paper analyses whether current postal voting regulations and standards in Germany comply to the principles established by the latest Council of Europe (CoE) recommendation on standards for e-voting. Both voting channels are channels for remote voting, hence principles established for one channel must, in the view of the author, also be fully applicable for the other channel. This paper applies the standards set by the recommendation to e-voting to the more commonly used remote voting channel postal voting and concludes that most of these standards cannot be met.*

## KEY WORDS

*Elections, E-voting, Internet Voting, Postal Voting*

---

\* mueller-toeroek@hs-ludwigsburg.de, Professor, University of Public Administration and Finance Ludwigsburg, Reuteallee 36, D-71634 Ludwigsburg, Germany.

<sup>1</sup> *Verfassungsgerichtshof, W I 6/2016-125*, 1 July 2016. [online] Available from: [https://www.ris.bka.gv.at/Dokumente/Vfgh/JFT\\_20160701\\_16W\\_I00006\\_00/JFT\\_20160701\\_16W\\_I00006\\_00.pdf](https://www.ris.bka.gv.at/Dokumente/Vfgh/JFT_20160701_16W_I00006_00/JFT_20160701_16W_I00006_00.pdf) [Accessed 31 May 2018].

## 1. INTRODUCTION

The Council of Europe (CoE) in 2004 issued a recommendation Rec(2004)11 which was until 2017, in the absence of any regulations in most of the national constitutions on e-voting, the yardstick to decide whether any e-voting did meet democratic standards. Due to technical progress and a significant number of e-voting pilots in many member states of the Council of Europe, the recommendation was updated in 2017. The main consideration can be found in the preamble:

*“Aware of concerns about potential security, reliability or transparency problems of e-voting systems”.*<sup>2</sup>

These concerns exist, especially after several bad experiences with e-voting, namely:

- The Austrian Constitutional Court annulled an election where e-voting was used for the first (and last) time in Austria in 2009;<sup>3</sup>
- The Finnish Supreme Administrative Court annulled election results and ordered the elections to be repeated paper-based after a failed e-voting;<sup>4</sup>
- Several disappointing reports on e-voting pilots at municipal elections in the UK published by the Electoral Commission in 2007;<sup>5</sup>

<sup>2</sup> Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting. Council of Europe, p. 2.

<sup>3</sup> Verfassungsgerichtshof, V 85-96/11-15, 13 December 2011. [online] Available from: [https://www.vfgh.gv.at/downloads/VfGH\\_V\\_85-96-11\\_e-voting.pdf](https://www.vfgh.gv.at/downloads/VfGH_V_85-96-11_e-voting.pdf) [Accessed 31 May 2018].

<sup>4</sup> Decision KHO:2009:39 (687/1/09), Supreme Administrative Court of Finland, 9 April 2009. [online]. Available from: <https://www.finlex.fi/fi/oikeus/kho/vuosikirjat/2009/200900899> [Accessed 2 November 2018]; EFFI (Electronic Frontier Finland). *A Report on the Finnish E-voting Pilot*. [online] Available from: <https://www.verifiedvoting.org/wp-content/uploads/2014/09/Finland-2008-EFFI-Report.pdf> [Accessed 31 May 2018].

<sup>5</sup> Actica Consulting. *Technical Evaluation of Sheffield City Council e-voting Pilot 2007*. [online] Available from: [http://www.electoralcommission.org.uk/\\_data/assets/electoral\\_commission\\_pdf\\_file/0020/16193/Actica\\_Sheffield\\_27247-20138\\_\\_E\\_\\_N\\_\\_S\\_\\_W\\_\\_.pdf](http://www.electoralcommission.org.uk/_data/assets/electoral_commission_pdf_file/0020/16193/Actica_Sheffield_27247-20138__E__N__S__W__.pdf) [Accessed 31 May 2018]; Actica Consulting. *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](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]; Actica Consulting. *Technical Evaluation of Swindon Borough Council e-voting Pilot 2007*. [online] Available from: [http://www.electoralcommission.org.uk/\\_data/assets/electoral\\_commission\\_pdf\\_file/0005/16196/Actica\\_Swindon\\_27245-20141\\_\\_E\\_\\_N\\_\\_S\\_\\_W\\_\\_.pdf](http://www.electoralcommission.org.uk/_data/assets/electoral_commission_pdf_file/0005/16196/Actica_Swindon_27245-20141__E__N__S__W__.pdf) [Accessed 31 May 2018]; Actica Consulting. *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](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].

- Norway cancelled before usage.<sup>6</sup>

Setting aside the technical issues, which are not the focus of this paper, it is obvious that e-voting<sup>7</sup> and postal voting are two different voting channels for remote voting. If a renowned and distinguished institution like the Council of Europe defines requirements a remote voting channel A must meet, it seems obvious that voting channel B must meet them at least in principle, otherwise one channel is not as reliable as the other, so in legal terminology: preferred. If, for instance the recommendation on e-voting requires that

*“The voter shall receive confirmation by the system that the vote has been cast successfully and that the whole voting procedure has been completed,”*<sup>8</sup>

the question arises whether postal voting also complies with this requirement.

It does not make much sense to require a new remote voting channel, namely e-voting, to fulfil requirements an established remote voting channel, namely postal voting does not fulfil, not even at a much lower level.

The paper consists of a commented listing of some key requirements of the recommendation in Section 2, which includes an analysis as to whether these requirements are met by postal voting in Germany. Section 3 summarizes in brief, what immediate changes to postal voting must become effective, to meet this requirements. Section 4 opens the discussion, whether it seems acceptable to permit one remote voting channel to be preferred over another and what conclusions should be drawn.

The paper intends to start a discussion on legal, process and technical issues associated with postal voting.

Regarding the scientific literature on this topic, there are only a few sources, most of them quoted in the paper. In Germany, election fraud in general and issues of remote voting in particular are not discussed. Standard textbooks dealing with elections, like e.g. *Nohlen*, contain just

<sup>6</sup> BBC News. (2014) E-voting Experiments End in Norway Amid Security Fears. 27 June. [online] Available from: <https://www.bbc.com/news/technology-28055678> [Accessed 4 November 2018].

<sup>7</sup> E-voting in this paper means voting via the Internet.

<sup>8</sup> Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting. Council of Europe, p. 4.

a few sentences on postal voting and e-voting within a 588-page-volume<sup>9</sup> without raising any issues. *Ritter and Niehuss*, who provide the analyses for elections after 1945, also fail to raise the issue of fraud.<sup>10</sup> Finally, what may arguably be the German standard textbook on Election Research, *Falter/Schoen* fails to include a single line on election fraud or issues with remote voting. The index does not even contain the word “*Wahlbetrug*”, which means election fraud.<sup>11</sup> The standard legislative commentary on the German election law contains only one minor remark in the context of postal voting, which is referred to later in the text.

## 2. KEY REQUIREMENTS ON E-VOTING DERIVED FROM THE CM/REC(2017)5

The requirements, called standards in CoE-terminology, are grouped into thematic sections from I to VIII. Of course, they are focused on e-voting, but at least in principle they must be applicable to any other form of remote voting.

### 2.1 UNIVERSAL SUFFRAGE

The standards here are fully applicable to e-voting, but do not raise any issues except for Standard 3:

*“Unless channels of remote e-voting are universally accessible, they shall be only an additional and optional means of voting.”*

If we consider an election like the “*Sozialwahl*” in Germany, where people elect representatives in Social Security Councils, this election takes place in one channel only: postal voting.<sup>12</sup> The question arises as to what “universally accessible” means. The Explanatory Memorandum gives us the answer:

---

<sup>9</sup> Nohlen, D. (2014) *Wahlrecht und Parteiensystem – Zur Theorie und Empirie der Wahlsysteme*. 7., überarbeitete und aktualisierte Auflage. Lizenzausgabe für die Bundeszentrale für politische Bildung, Verlag Barbara Budrich, Opladen/Toronto, p. 46.

<sup>10</sup> Ritter, G. A. and Niehuss, M. (1991) *Wahlen in Deutschland 1946–1991*, C.H. Beck, München; Ritter, G. A. and Niehuss, M. (1995) *Wahlen in Deutschland 1991–1994*, C.H. Beck, München.

<sup>11</sup> Falter, J. W. and Schoen H. (2014) *Handbuch Wahlforschung*. 2., überarbeitete Auflage. Springer VS, Wiesbaden, p. 891.

<sup>12</sup> The “*Sozialwahl*” has an electorate of some 51 mio. People (see *Soziale Selbstverwaltung*. [online] Available from: <https://www.sozialwahl.de/sozialwahl/die-sozialwahl-auf-einen-blick/> [Accessed 31 May 2018]).



“However, offering the remote e-voting channel exclusively restricts accessibility, given the fact that the channel, namely internet, is not universally accessible for the time being. This provision aims at protecting the voter so that he or she is offered a means of voting which is effectively available to him or to her.”<sup>13</sup>

Unfortunately postal voting is not universally accessible as Müller-Török and Pautsch have pointed out.<sup>14</sup> There are severe differences between different states of the world in delivery times and delivery methods, which are not taken into account by today’s German postal voting regime. Registered mail with delivery to the identified addressee only is not available in e.g. Argentine, Brazil, Chile, China and India while the delivery time indications are between 10 and 18 working days.<sup>15</sup> This, due to the time-limits in the law, effectively hinders any postal voting. These issues, as Pautsch and Müller-Török discussed, lead to a situation where it depends on stochastic terms whether a postal ballot finds its voter and the way back within the timeframe stipulated by the election procedures and laws and whether it is counted or not. The overseas voters do not have another channel than postal voting – because it is unthinkable that e.g. a German citizen residing in Hawaii will fly to San Francisco to vote at the competent German Consulate – at his or her own expense. So at least with a view on the overseas ballot,<sup>16</sup> postal voting does not meet the requirement raised by the recommendation. In the literature on German elections there is in only one single publication concern raised with a view to privatization of domestic postal services, but the issue of overseas voters

<sup>13</sup> *Explanatory Memorandum to Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting*. Document Number CM(2017)50-add1final. Council of Europe, p. 6.

<sup>14</sup> Pautsch, A. and Müller-Török, R. (2015) Die grenzüberschreitende Zustellung von Briefwahlunterlagen vor den Schranken des Völkerrechts – Eine übersehene Problematik?. *Zeitschrift für Rechtspolitik*, 3, pp. 88-90, p. 89; Müller-Török, R. and Pautsch, A. (2015) Stochastische Verfälschungen von Wahlergebnissen bei grenzüberschreitender Briefwahl?. *Verwaltung und Management*, 4, pp. 192-197, p. 196; Prosser, A., Pautsch, A. and Müller-Török, R. Legal Aspects of Cross-Border Delivery of Voting Documents – A Neglected Issue?. In: *Proceedings of the 2015 2nd International Conference on Electronic Governance and Open Society: Challenges in Eurasia*, ACM New York NY 2015, pp. 123.

<sup>15</sup> For the delivery time estimates see *Länderinformationen und internationale Brieflaufzeiten*. [online] Available from: <https://www.deutschepost.de/de/b/briefe-ins-ausland/laenderinformationen.html>; a timely return of the postal ballot cannot be guaranteed such within the deadlines set by the electoral laws and authorities.

<sup>16</sup> In the days before the Bavarian Federal State Assembly Elections, which took place on October 14th, 2018, a doctor’s prescription needed five full days to be delivered within the City of Munich from a General Practitioner to the author. This may sound anecdotic, but raises serious questions in the context of postal voting.

is totally neglected.<sup>17</sup> And, with a view on the above mentioned “Sozialwahl” it does in no way meet this requirement.

## 2.2 EQUAL SUFFRAGE

Standard 7 states:

*“Unique identification of voters in a way that they can unmistakably be distinguished from other persons shall be ensured.”*

This standard seems, at first glance, to be fulfilled by postal voting in Germany, but with a view to the two explanatory notes, it becomes ambiguous:

*“The voters’ registers therefore need to provide means to avoid digital twins – i.e. persons holding the same identification data. In cases where central voters’ registers are used, unique identification may implicitly be given by the entry of the person in the database. With interconnected voters’ registers additional means may be necessary.”*

In Germany the voters’ registers are decentralized, but not interconnected. If we take Baden-Württemberg for example, the provisions in § 10 GemO state that the mayor of each municipality may keep the voter register in an electronic manner – but he is not legally obliged to. No mandatory formal checks for duplicates over community boundaries takes place. The very same appears for the elections to the European Parliament, where Balthasar and Müller-Török have shown that no reconciliation over Member States boundaries takes place,<sup>18</sup> despite legal requirements in European Union law.<sup>19</sup>

---

<sup>17</sup> Schreiber, W.; Hahlen, J. and Strelen, K.-L. (2017) *BWahlG Kommentar zum Bundeswahlgesetz unter Einbeziehung des Wahlprüfungsgesetzes, des Wahlstatistikgesetzes, der Bundeswahlordnung und sonstiger wahlrechtlicher Nebenvorschriften*. 10., vollständig neubearbeitete Auflage. Carl Heymanns Verlag, p. 614.

<sup>18</sup> In Germany, there was the famous case of *Giovanni di Lorenzo*, a renowned newspaper journalist, who voted twice in 2014 with his Italian and German passport on the Italian and German ballot. Charges against him were dropped after he agreed to pay a fine (see *Die Welt*. (2014) Verfahren gegen “Zeit” – Chef di Lorenzo eingestellt. 18 November. [online] Available from: <https://www.welt.de/politik/deutschland/article134483671/Verfahren-gegen-Zeit-Chef-di-Lorenzo-eingestellt.html> [Accessed 1 September 2018]).

<sup>19</sup> Balthasar, A. and Müller-Török, R. Ein Vorschlag zur Effektuierung des Artikels 13 der Richtlinie 93/109/EG. In: *Tagungsband des 14. Internationalen Rechtsinformatik Symposions – IRIS 2011*, 24.–26. Februar 2011, Salzburg.

Standard 8 states:

*“The e-voting system shall only grant a user access after authenticating her/him as a person with the right to vote,”*

and looks, at first glance, not applicable for postal voting. The respective explanatory note says:

*“In cases where anonymous voting tokens prove that a voter is eligible to vote, identification of the voter may not be required at this point as it has already taken place at an earlier stage, namely when the specific token is assigned to a specific voter.”*

The postal ballot is definitely an anonymous voting token in the meaning of the recommendation. Here a major question arises: Was the voter identified *before* he was handed over the postal ballot by the postman? Unfortunately, the application for postal voting in Germany consists of three steps, which do not require much identification as shown below:

1. The voter receives a postcard or letter by non-registered mail in his or her mailbox, which enables him or her to require a postal ballot. This can be done without the postcard/letter, even by plain fax or e-mail,<sup>20</sup> in this case jump step 2;
2. The voter ticks a box, signs the postcard or letter and sends it to his or her Election Authority. Note that an address different from the voter's address in the voter roll can be stated. The postal ballot is sent to this new address without further inquiries;
3. The Election Authority sends the postal ballot to the address stated on the request with non-registered mail.<sup>21</sup>

As *Stein and Müller-Török* have shown, a signature is a non-secure proof of identity in an election context, because it is expensive to verify and leads to a less-than-100 percent level of likelihood that the person who signed is

<sup>20</sup> The Federal Returning Officer suggests this at his website when explaining the process of postal voting (see *Briefwahl*. [online] Available from: <https://www.bundeswahlleiter.de/bundestagswahlen/2017/informationen-waehler/briefwahl.html#967be3c2-d7a4-46c4-8d77-1784f3fce9f2> [Accessed 1 September 2018]).

<sup>21</sup> The only occasions in the life of the author in Germany (1997–2018), where a postal ballot was sent by registered mail with a mandatory proof of identity were when receiving his ballots for the Austrian Parliamentary and Presidential Elections. For German elections the ballots were never sent registered mail nor had he to proof his identity to postmen.

the person in question.<sup>22</sup> A mailbox is, because of the lack of standardized and lockable mailboxes in Germany, not a safe place. It is easy to get an envelope out of a mailbox without a key, because no legal provision requires mailboxes to hinder third-party access. In Austria, on the other hand, § 34 PMG requires:

*“The mailbox must be such that postal shipments are protected against third-party access by an appropriate protection” (my translation).*

In Germany, there was a major case of election fraud regarding applications for postal voting at a local election. A farmer in Bavaria filled in hundreds of such request forms for her Romanian farmhands and managed to submit the postal ballots. Election authorities nullified the election and the criminal lawsuit is still pending.<sup>23</sup>

It is obvious that this protocol is not safe against misuse. Also the standard legislative commentary acknowledges these shortcomings, namely:

- A postal ballot can easily be requested by third parties in the name of the voter;
- The possibility of stating a different address the ballot shall be sent to;
- All documents included can easily be forged or copied;
- Issues with elderly or (mentally) disabled people in nursing homes.<sup>24</sup>

Standard 9 requires that only the appropriate number of votes per voter is cast, stored and counted. “One person, one vote” is mentioned in the explanatory note but, in the opinion of the author, violated in one

<sup>22</sup> Stein, R. and Müller-Török, R. (2010) Die Europäische Bürgerinitiative aus Sicht nationaler Wahlbehörden: Probleme der Verifikation von Unterstützungserklärungen in der Praxis. *Verwaltung und Management*, 5, pp. 255–262.

<sup>23</sup> Landgericht Regensburg. (2018) *Strafverfahren wegen Verdachts der Wahlmanipulation in Geiselhörung*. [press release] 15 October. Available from: <https://www.justiz.bayern.de/gerichte-und-behoerden/landgericht/regensburg/presse/2018/7.php> [Accessed 2 November 2018]. The assumption of innocence is not applicable; because the election was already nullified by the election authority (see *Die Welt*. (2014) Bayerischer Kreis muss wegen Fälschung neu wählen. 2 October. [online] Available from: <https://www.welt.de/politik/deutschland/article132875498/Bayerischer-Kreis-muss-wegen-Faelschung-neu-waehlen.html> [Accessed 2 November 2018]).

<sup>24</sup> Schreiber, W.; Hahlen, J. and Strelen, K.-L. (2017) *BWahlG Kommentar zum Bundeswahlgesetz unter Einbeziehung des Wahlprüfungsgesetzes, des Wahlstatistikgesetzes, der Bundeswahlordnung und sonstiger wahlrechtlicher Nebenvorschriften*. 10., vollständig neubearbeitete Auflage. Carl Heymanns Verlag, p. 613.

special situation: If the voter dies before election day, he or she can of course not vote at the polling station but his or her postal vote cast before his or her dying day and well before election day is counted if mailed. This may sound irrelevant at the first glance, but if you consider narrow results in a constituency and some 20 days between receiving postal ballots and Election Day this may well become relevant.<sup>25</sup> At least it seems obvious, that voters cannot be treated equally dependent of the voting channel chosen.

### 2.3 FREE SUFFRAGE

Standard 15 to 17 are the most crucial requirements when they are applied to existing postal voting. 15 states:

*“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 without being altered. Any undue influence that has modified the vote shall be detectable,”*

while 16 requires:

*“The voter shall receive confirmation by the system that the vote has been cast successfully and that the whole voting procedure has been completed.”*

And 17 finally asks:

*“The e-voting system shall provide sound evidence that each authentic vote is accurately included in the respective election results. The evidence should be verifiable by means that are independent from the e-voting system.”*

As the explanatory notes show, a chain of trust must be established. Individual verifiability by the voter, as demanded by explanatory note 55, cannot exist in a postal voting regime where ballots are sent to the Election Authority by non-registered mail and in envelopes, which must not carry the address of the voter. So it is also impossible to tell whether a ballot from an individual voter arrived and was cast and counted, let alone the detection of unlawful alterations. The current postal voting in Germany is like a letter in a bottle, thrown into the sea: Once the voter put his or her envelope into the post box, no one can tell whether it arrived and whether it

---

<sup>25</sup> Heiner Geißler, former chairman and long-term Member of Parliament of the German Christian Democratic Party died in his 88th year on 12 September 2017, 12 days before Election Day. He is likely to have voted by postal voting with his vote being counted.

was counted or not. As the repealed Austrian Presidential Elections of 2016 have shown, irregularities do occur even in the Electoral Commissions when opening the envelopes with the postal ballots and counting.<sup>26</sup> The requirement that any undue influence shall be detectable, does not fully apply to postal voting. As *Schreiber et al.* pointed out, election authorities in Germany do not even check whether incoming postal ballots match postal ballots sent to voters<sup>27</sup> and all documents can easily be copied and/or modified.<sup>28</sup>

## 2.4 SECRET SUFFRAGE

Standard 19 is an obvious necessity; nevertheless, it can easily be violated when postal voting from overseas voters occurs. It states that

*“the secrecy of the vote is respected at all stages of the voting procedures.”*

As *Pautsch and Müller-Török* have shown, jurisdiction of e.g. the US Supreme Court is not compatible with this (European) standard. In *United States vs. Ramsey*, the court ruled regarding the opening and searching of post sent to Ramsey from abroad:

*“[...] That searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border should, by now, require no extended demonstration.”<sup>29</sup>*

And with even more clarity in the same case:

*“Border searches, then, from before the adoption of the Fourth Amendment, have been considered to be “reasonable” by the single fact that the person or item in question had entered into our country from outside. There has never been any additional requirement that the reasonableness of a border search depended on the existence of probable cause. This longstanding*

<sup>26</sup> *Verfassungsgerichtshof*, V 85-96/11-15, 13 December 2011. [online] Available from: [https://www.vfgh.gv.at/downloads/VfGH\\_V\\_85-96-11\\_e-voting.pdf](https://www.vfgh.gv.at/downloads/VfGH_V_85-96-11_e-voting.pdf) [Accessed 31 May 2018].

<sup>27</sup> *Schreiber, W.; Hahlen, J. and Strelen, K.-L. (2017) BWahlG Kommentar zum Bundeswahlgesetz unter Einbeziehung des Wahlprüfungsgesetzes, des Wahlstatistikgesetzes, der Bundeswahlordnung und sonstiger wahlrechtlicher Nebenvorschriften. 10., vollständig neubearbeitete Auflage. Carl Heymanns Verlag, p. 613.*

<sup>28</sup> *Ibid.*

<sup>29</sup> *United States vs. Ramsey* (1977) 431 U.S. 606.

*recognition that searches at our borders without probable cause and without a warrant are nonetheless “reasonable” has a history as old as the Fourth Amendment itself.*<sup>30</sup>

This standard can be obeyed to in an e-voting environment, where encryption by e.g. TLS/SSL hinders U.S. Postal Inspection Service, Customs and Border Protection and other agencies to open and search the e-voting ballot,<sup>31</sup> but no one can hinder the before mentioned agencies to open and search postal voting ballots for contraband, such breaking the secrecy of the vote. Collecting all postal votes from the US at a German consulate and sending it to Germany with diplomatic mail seems not to be a viable option.

Setting aside the lawful interception of postal voting documents, of course Secret Suffrage can be breached illegally, e.g. by opening the envelopes and closing them again. In the former GDR the State Security Service (“*Staatssicherheit*” or short “*Stasi*”) opened nearly each letter to and from abroad, read it and closed it in a manner which nearly perfectly camouflaged the fact that it had been opened.<sup>32</sup> A postal ballot does not have sufficient precautions against such measures. Even if it were not possible to close it again, the vote would be lost – that the voter cannot learn that his or her vote was lost seems to be an obvious violation of standard 15, namely:

*“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 without being altered. Any undue influence that has modified the vote shall be detectable.”*

---

<sup>30</sup> Ibid.

<sup>31</sup> In this paper the author lets aside the issues associated with more restrictive internet usage regimes like e.g. The Great Firewall of China (see *Bloomberg*. (2018) The Great Firewall of China. 6 November. [online] Available from: <https://www.bloomberg.com/quicktake/great-firewall-of-china> [Accessed 4 November 2018]).

<sup>32</sup> For an introduction and legal documents of the GDR regarding this practice see the websites of the Federal Agency for Civic Education regarding the regular checks of postal shipments by the State Security Service (*Allwissenheit als Ziel – Die Postkontrolle der DDR-Geheimpolizei*. [online] Available from: <http://www.bpb.de/geschichte/deutsche-geschichte/stasi/223937/postkontrolle> [as per 1 September 2018]) and of the Federal Commissioner for the Records of the State Security Service of the former German Democratic Republic (*Das Recht auf Postgeheimnis*. [online] Available from: [https://www.demokratie-statt-diktatur.de/DSD/DE/Postgeheimnis/Aus-dem-Archiv/\\_node.html](https://www.demokratie-statt-diktatur.de/DSD/DE/Postgeheimnis/Aus-dem-Archiv/_node.html) [as per 1 September 2018]).

This postal voting also creates another conflict with standard 19: When posting the postal ballot into a post box, at least the following parties are able to intercept the vote:

- The person collecting the post from the box, in specific boroughs you may assume tendencies, so e.g. a conservative or nationalist postal worker could throw away postal ballots in a borough, which traditionally votes for communist, socialist or ecological parties. Since the envelope does not bear a sender's address in Germany and since the posting is not documented, there is no way to even detect this offence;
- Any other postal worker from the collection to the delivery, a number likely to be in the two-digit-range;
- Sorting machines could probably open or destroy postal ballots by mistake or, probably the worst case, leave them undelivered because of an assumed or real lack of sufficient franking;
- Staff at the election authority could make a broad variety of mistakes as the landmark case regarding Austrian Presidential Elections has shown, e.g.
  - Non-members of the election authority opened envelopes and took out the ballots,<sup>33</sup>
  - Non-members of the election authority decided whether ballots were invalid.<sup>34</sup> They could at least theoretically, have invalidated them on their own, as the Constitutional Court argued;<sup>35</sup>
- The person who receives the postal ballots from the postal services on behalf of the election authority could destroy them or hide them away. Since there is neither a closed and reliable chain of trust, nor even some paper-based protocol requirements, the likelihood of detection is quite low.

---

<sup>33</sup> *Verfassungsgerichtshof, W I 6/2016-125*, 1 July 2016. [online] Available from: [https://www.ris.bka.gv.at/Dokumente/Vfgh/JFT\\_20160701\\_16W\\_I00006\\_00/JFT\\_20160701\\_16W\\_I00006\\_00.pdf](https://www.ris.bka.gv.at/Dokumente/Vfgh/JFT_20160701_16W_I00006_00/JFT_20160701_16W_I00006_00.pdf) [Accessed 31 May 2018]; RZ 201, 202 and 217 and several others.

<sup>34</sup> Ibid, RZ 233 and 234.

<sup>35</sup> Ibid, RZ 237 and 238; the whole ruling has 175 pages and the two illegal practices occurred many time in many constituencies, hence only a few were quoted here.



## 2.5 REGULATORY AND ORGANIZATIONAL REQUIREMENTS

At the first glance, postal voting fulfils the standards of this section. A closer analysis however shows, a conflict occurs with standard 29:

*“The relevant legislation shall regulate the responsibilities for the functioning of e-voting systems and ensure that the electoral management body has control over them.”*

As explanatory note 88 shows:

*“member States not to be dependent on just a few vendors since this could result in a vendor-lock-in.”*

A vendor-lock-in, as described by literature<sup>36</sup> is when a customer, in this context an election authority, is fully dependent on a vendor. This vendor is, with respect to postal voting, the Deutsche Post AG (together with many smaller postal services providers) which cannot be monitored nor controlled by election authorities and also, at a later stage, courts. The explanatory note 88 becomes even more concrete and states:

*“When considering outsourcing, it is essential that those who are responsible for the elections understand what is being outsourced, why it is being outsourced and what methods and processes the vendor intends to undertake.”*

Explanatory note 87 adds:

*“It is recommended that the relevant legislation provides for the supervisory role of the electoral management body over e-voting. The role and the responsibilities of the other parties involved should be clarified at the appropriate regulatory or contractual level.”*

As shown above in the section regarding secret suffrage, foreign postal services are impossible to be controlled by the Election Authorities. If we take e.g. the delivery times, *Pautsch and Müller-Török* have shown that they

---

<sup>36</sup> Liebowitz, S. J.; Margolis, Stephen E. (1995) Path dependence, lock-in and history. *Journal of Law, Economics, and Organization*. 11, p. 205–226.

are beyond any national control<sup>37</sup> and it is obvious that no regulation nor contract other than the Convention union postale universelle<sup>38</sup> exists.

## 2.6 TRANSPARENCY AND OBSERVATION

Transparency is an issue from the time the postal voter drops his or her ballot into the mailbox. From here on absolutely no transparency exists, because:

- The envelope bears no sender in German postal voting, hence a totally anonymous vote is being transferred (or not) totally untracked to the respective Election Authority and no one can ever tell whether it arrived, was counted etc.;
- Unlike e.g. registered mail or parcels, which can be tracked via the Internet, the postal ballot cannot be tracked.

Explanatory note no. 91 is violated, which states:

*“In particular system’s transparency, or the possibility to check that it is functioning properly, must be guaranteed. Member States regulate who has access to what and when and under what circumstances.”*

The national – and much more the foreign – postal authorities are neither transparent nor can anyone guarantee their proper functioning. Recent newspaper reports show that the Deutsche Post AG decided to introduce other days other than Sundays where no mail is delivered. If such causes a loss of a handful of ballots, the outcome of elections can be changed as e.g. in 2013 a narrow constituency for German Parliament, Märkischer Kreis II was won by a margin of 53 votes – or 27 ballots would have made a change.<sup>39</sup>

## 2.7 ACCOUNTABILITY

These standards are obviously focused on e-voting, but if applied to postal voting, it becomes obvious that their underlying principles are violated by postal voting practice. If we take standard 37, it states:

---

<sup>37</sup> Pautsch, A. and Müller-Török, R. (2015) Die grenzüberschreitende Zustellung von Briefwahlunterlagen vor den Schranken des Völkerrechts – Eine übersehene Problematik?. *Zeitschrift für Rechtspolitik*, 3, pp. 88–90, p. 90.

<sup>38</sup> Convention union postale universelle. [online] Available from: <http://www.upu.int/fr/lupu/actes/actes-en-trois-volumes.html> [Accessed 4 November 2018].

<sup>39</sup> Der Bundeswahlleiter. (2014) *Wahl zum Deutschen Bundestag am 22. 9. 2013, Heft 5, Teil 1, Textliche Auswertung Wahlergebnisse*, p. 69, anhangtabelle 1.

*“Before an e-voting system is introduced and at appropriate intervals thereafter, and in particular after any significant changes are made to the system, an independent and competent body shall evaluate the compliance of the e-voting system and of any information and communication technology (ICT) component with the technical requirements. This may take the form of formal certification or other appropriate control.”*

Who certified postal services? In the recent years, not only the formerly state-operated Deutsche Bundespost was transferred into a stock-exchange-listed entity Deutsche Post AG but also new, mostly local, postal service providers were founded. Some of them went bankrupt at short notice, e.g. RegioPost Pfalz GmbH that stopped postal services in February 2018 and told some 500 staff on 19 January 2018 that they are laid off with effect from 20 January 2018.<sup>40</sup> If this were in the six weeks before a Parliamentary Election Day, irregularities would surely have occurred in postal voting. It seems notable in this context that nowadays mail, including postal ballots, is not handled by sworn officers like in the days of the Deutsche Bundespost but by low-paid staff in sub entities of the Deutsche Post AG with significantly lower wages.<sup>41</sup> This seems to be an international trend.<sup>42</sup> Schreiber *et al.* heavily criticized the privatization of postal services in the context of postal voting.<sup>43</sup>

Another standard is 39, the requirement for auditability, namely:

*“The audit system shall [...] actively report on potential issues and threats.”*

It is obvious that this requirement is not fulfilled by any paper-based postal system. No post box actively reports when it is damaged or shipments are

<sup>40</sup> Karin Hurre. (2018) Müssen entlassene Mitarbeiter nun wieder die Zeche für ein Missmanagement zahlen? *Nachrichten Regional*, 23 January. [online] Available from: <https://www.nachrichten-regional.de/index.php/%C3%BCberregional/6733-regio-post-pfalz-und-regio-post-beteiligungsgesellschaft-ein-undurchsichtiges-konstrukt.html> [Accessed 4 November 2018].

<sup>41</sup> *Spiegel Online*. (2018) Zusteller der Deutschen Post sollen in neuen Betrieb ausgelagert werden. 12 March. [online] Available from: <https://www.spiegel.de/wirtschaft/unternehmen/deutsche-post-zusteller-sollen-in-neuen-betrieb-ausgelagert-werden-a-1197588.html>

<sup>42</sup> See e.g. *The Telegraph*. (2017) Threat of Royal Mail Strike Lessens as Progress Made in Union Talks. 6 December. [online] Available from: <https://www.telegraph.co.uk/business/2017/12/06/threat-royal-mail-strike-lessens-progress-made-union-talks/>

<sup>43</sup> Schreiber, W.; Hahlen, J. and Strelen, K.-L. (2017) *BWahlG Kommentar zum Bundeswahlgesetz unter Einbeziehung des Wahlprüfungsgesetzes, des Wahlstatistikgesetzes, der Bundeswahlordnung und sonstiger wahlrechtlicher Nebenvorschriften*. 10., vollständig neubearbeitete Auflage. Carl Heymanns Verlag, p. 613.

stolen out of it. No one can tell whether envelopes with postal votes are fished out of a post box, at least at the present technological standards in Germany. If we compare this to explanatory note 114, it is obvious that no Intrusion Detection System exists for postal services and that, hopefully, for registered mail, no audit trails exist as required by explanatory note 115. Explanatory note 118, which requires:

*“observers should be able to see the total number of ballots cast in real time, so that independent cross checks can be performed,”*

cannot be fulfilled by a postal service based on post boxes, manual transport with trucks and no electronic tracking system at all. Concerning the other explanatory notes, we must state that none of these audit requirements can be met by postal voting. No postal system can detect voter fraud, as *Isobel White* has shown for the UK.<sup>44</sup>

## 2.8 RELIABILITY AND SECURITY OF THE SYSTEM

With respect to reliability and security, already the first standard no. 40 cannot be fulfilled by postal voting:

*“The electoral management body shall be responsible for the respect for and compliance with all requirements even in the case of failures and attacks.”*

This would mean that election authorities are in charge of all involved postal services used – even of the postal services in Thailand or Argentina, if a voter cast his or her ballot there. Access to central infrastructure (of postal services worldwide) cannot be granted to persons *“authorised by the electoral management body”* as standard 41 requests. Also, among others, standard 47 is impossible to fulfil, namely:

*“Where incidents that could threaten the integrity of the system occur, those responsible for operating the equipment shall immediately inform the electoral management body.”*

would require the e.g. Argentine postal service to report to (German) election authorities when a bag of shipments is stolen, which could contain ballots for German elections. Moreover, finally standard 49 is impossible

---

<sup>44</sup> White, I. and Coleman, Ch. (2011) *Postal Voting & Electoral Fraud*, SN/PC/3667, House of Commons Library; White, I. (2015) *Electoral Offences since 2010*, House of Commons Library Briefing Paper Number 625.

to be fulfilled by postal voting: Identifying votes that are affected by irregularities.

### 3. IMMEDIATE CHANGES NECESSARY FOR GERMAN POSTAL VOTING

With a view to the section above the following changes seem unavoidable necessities in order to comply with essential principles of voting:

1. Introduction of either a centralized German voter registry or automatic reconciliation of the decentralized registers to ensure effectively that no identity twin nor double-registered voter occurs. This registry must also be able to deal with people dying after having applied for postal ballots etc.;
2. Sending postal ballots to the voter by registered mail only with a mandatory and high profile proof of identity,<sup>45</sup> thereby hindering bogus applications and theft of ballots;<sup>46</sup>
3. A mechanism shall be established where a voter may verify whether his or her vote actually arrived with the Election Authorities and entered the ballot box. This mechanism must guarantee anonymity;
4. Regarding overseas voters, the timelines and the whole legal framework must be reengineered according to the recommendations of *Pautsch and Müller-Török*. The risk that any other authoritarian state manipulates the cornerstone of German democracy is far too high with some 2 million German voters living abroad. If we take e.g. the preliminary results of the latest election in Germany, the one for the State Assembly of the Federal State of Hesse on October 28, 2018, the race for the second place between Social Democrats and Green Party was decided by a margin of 94 votes.<sup>47</sup> If only 47 ballots were different, it would have been a tie.

---

<sup>45</sup> The author was handed a letter sent by registered mail today (October 16th, 2018) when opening the door w/o any proof of identity. The “signature” required consisted of “signing his name” with his pointing finger on a mobile device, some kind of touchpad. It is obvious that such a “signature” will not be highly valued in a Constitutional Court.

<sup>46</sup> Such offences are common in e.g. the UK as shown by *White and Coleman* (p. 20) and *White* (see fn. 44). Unfortunately comparable statistics are not available for Germany.

These measures cannot hinder third parties, e.g. spouses to steal postal ballots or violently force the voter to cast his or her vote.<sup>48</sup> Because a mechanism like a replacing vote, which can be implemented in an e-voting system, cannot be implemented in postal voting, this risk still exists.

#### 4. RESUME

To summarize, the current German (and other) regime of postal voting has one big issue, which seems to be totally underestimated regarding its effect on election results:

Once the election authority sends the postal ballot to an address (hopefully the address of the voter), it totally loses any control until the ballot returns. In the meantime, which means within a period of several weeks, the following persons/entities could have corrupted the ballot, by stealing, forging, casting their own vote on behalf of the voter etc.:

1. Postal services and their employees of Germany and all other countries affected;
2. State agencies like the above-mentioned US Customs and US Postal Inspectors but, in our days, also rogue states which want to manipulate German elections by manipulating the ballots of imprisoned German citizens;
3. Individuals, including neighbours, relatives and spouses who intercept ballots or use force to make the voter cast his or her vote in violation of voting principles.

The major problem, according to the literature, the political discussion and discussions with fellow scientists and election practitioners is that postal voting once was the rare exception, when being abroad, ill etc. Nowadays it has become a way of “convenience voting”, which frees

<sup>47</sup> Hessisches Statistisches Landesamt. (2018) *Statistische Berichte, Kennziffer B VII 2-3 – 5j/18, Die Landtagswahl in Hessen am 28. Oktober 2018, Vorläufige Ergebnisse*. [online] Available from: [https://statistik.hessen.de/sites/statistik.hessen.de/files/BVII2-3\\_5j18.pdf](https://statistik.hessen.de/sites/statistik.hessen.de/files/BVII2-3_5j18.pdf) [Accessed 2 November 2018], p. 12; it is notable that the final result is not available on 9 November 2018 due to irregularities, mistakes and necessary recounts. The final result is expected for 16 November 2018 (see *Die Welt*. (2018) *Es gab eine Reihe von Übermittlungs- und Eingabefehlern*. 9 November. [online] Available from: <https://www.welt.de/politik/deutschland/article183584926/Landtagswahl-Hessen-2018-So-erklaert-der-Wahlleiter-die-Auszaehlungspanne.html> [Accessed 9 November 2018]).

<sup>48</sup> White, I. and Coleman, Ch. (2011) *Postal Voting & Electoral Fraud*, SN/PC/3667, House of Commons Library, pp. 18, 27 and 33.

the voter from the perceived burden of appearing in person at the polling station. From 1994 to 2017 the share of postal voters at the parliamentary elections in Germany has more than doubled and stands at 28.6 percent with Hamburg and Bavaria leading the way with 37.0 and 37.3 percent respectively.<sup>49</sup> If you take e.g. the Federal State of Hamburg, it is a city with 984,926 votes cast out of approx. 1.8 Mio. inhabitants occupying some 755 square kilometres, hence it seems unreproducible that 364,213 postal voters were sick, disabled, abroad or in a comparable situation which hindered them to appear in person at the polling station.<sup>50</sup>

The major thing to do now is to start a serious scientific discussion about these issues. As shown above, the issues exist but unfortunately not the scientific publications dealing with them. So the first duty of the Social Sciences would be to provide a sound basis for a political discussion. This contribution is intended to be a stimulus starting a discussion.

## LIST OF REFERENCES

- [1] Actica Consulting. *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](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].
- [2] Actica Consulting. *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](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].
- [3] Actica Consulting. *Technical Evaluation of Sheffield City Council e-voting Pilot 2007*. [online] Available from: [http://www.electoralcommission.org.uk/\\_\\_data/assets/electoral\\_commission\\_pdf\\_file/0020/16193/Actica\\_Sheffield\\_27247-20138\\_E\\_N\\_S\\_W\\_.pdf](http://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0020/16193/Actica_Sheffield_27247-20138_E_N_S_W_.pdf) [Accessed 31 May 2018].
- [4] Actica Consulting. *Technical Evaluation of Swindon Borough Council e-voting Pilot 2007*. [online] Available from: [http://www.electoralcommission.org.uk/\\_\\_data/assets/electoral\\_](http://www.electoralcommission.org.uk/__data/assets/electoral_)

---

<sup>49</sup> Der Bundeswahlleiter. (2017) *Anteil der Briefwählerinnen und Briefwähler bei den Bundestagswahlen 1994 bis 2017 nach Ländern (auf Grundlage des amtlichen Endergebnisses)*, Wiesbaden. [online] Available from: [https://www.bundeswahlleiter.de/dam/jcr/b4aeabb8-7fac-473e-8581-cd718cb7a007/BTW\\_ab94\\_briefwahl.pdf](https://www.bundeswahlleiter.de/dam/jcr/b4aeabb8-7fac-473e-8581-cd718cb7a007/BTW_ab94_briefwahl.pdf) [Accessed 1 September 2018].

<sup>50</sup> Ibid.

- commission\_pdf\_file/0005/16196/Actica\_Swindon\_27245-20141\_\_E\_\_N\_\_S\_\_W\_\_.pdf  
[Accessed 31 May 2018].
- [5] *Allwissenheit als Ziel – Die Postkontrolle der DDR-Geheimpolizei*. [online] Available from: <http://www.bpb.de/geschichte/deutsche-geschichte/stasi/223937/postkontrolle>
- [6] Balthasar, A. and Müller-Török, R. Ein Vorschlag zur Effektuierung des Artikels 13 der Richtlinie 93/109/EG. In: *Tagungsband des 14. Internationalen Rechtsinformatik Symposions – IRIS 2011*, 24.–26. Februar 2011, Salzburg.
- [7] *BBC News*. (2014) E-voting Experiments End in Norway Amid Security Fears. 27 June. [online] Available from: <https://www.bbc.com/news/technology-28055678>  
[Accessed 4 November 2018].
- [8] *Bloomberg*. (2018) The Great Firewall of China. 6 November. [online]. Available from: <https://www.bloomberg.com/quicktake/great-firewall-of-china> [Accessed 4 November 2018].
- [9] *Briefwahl*. [online] Available from: <https://www.bundeswahlleiter.de/bundestagswahlen/2017/informationen-waehler/briefwahl.html#967be3c2-d7a4-46c4-8d77-1784f3fce9f2>  
[Accessed 1 September 2018].
- [10] *Convention union postale universelle*. [online] Available from: <http://www.upu.int/fr/lupu/actes/actes-en-trois-volumes.html> [Accessed 4 November 2018].
- [11] *Das Recht auf Postgeheimnis*. [online] Available from: [https://www.demokratie-statt-diktatur.de/DSD/DE/Postgeheimnis/Aus-dem-Archiv/\\_node.html](https://www.demokratie-statt-diktatur.de/DSD/DE/Postgeheimnis/Aus-dem-Archiv/_node.html)
- [12] *Decision KHO:2009:39 (687/1/09)*, Supreme Administrative Court of Finland, 9 April 2009. [online] Available from: <https://www.finlex.fi/fi/oikeus/kho/vuosikirjat/2009/200900899>  
[Accessed 2 November 2018].
- [13] Der Bundeswahlleiter. (2014) *Wahl zum Deutschen Bundestag am 22. 9. 2013, Heft 5, Teil 1, Textliche Auswertung Wahlergebnisse*, p. 69, anhangtabelle 1.
- [14] Der Bundeswahlleiter. (2017) *Anteil der Briefwählerinnen und Briefwähler bei den Bundestagswahlen 1994 bis 2017 nach Ländern (auf Grundlage des amtlichen Endergebnisses)*, Wiesbaden. [online] Available from: [https://www.bundeswahlleiter.de/dam/jcr/b4aeabb8-7fac-473e-8581-cd718cb7a007/BTW\\_ab94\\_briefwahl.pdf](https://www.bundeswahlleiter.de/dam/jcr/b4aeabb8-7fac-473e-8581-cd718cb7a007/BTW_ab94_briefwahl.pdf)  
[Accessed 1 September 2018].
- [15] *Die Welt*. (2014) Bayerischer Kreis muss wegen Fälschung neu wählen. 2 October. [online] Available from: <https://www.welt.de/politik/deutschland/article132875498/Bayerischer-Kreis-muss-wegen-Faelschung-neu-waehlen.html> [Accessed 2 November 2018].



- [16] *Die Welt*. (2014) Verfahren gegen “Zeit” – Chef di Lorenzo eingestellt. 18 November. [online] Available from: <https://www.welt.de/politik/deutschland/article134483671/Verfahren-gegen-Zeit-Chef-di-Lorenzo-eingestellt.html> [Accessed 1 September 2018].
- [17] *Die Welt*. (2018) Es gab eine Reihe von Übermittlungs- und Eingabefehlern. 9 November. [online] Available from: <https://www.welt.de/politik/deutschland/article183584926/Landtagswahl-Hessen-2018-So-erklaert-der-Wahlleiter-die-Auszaehlungspanne.html> [Accessed 9 November 2018].
- [18] EFFI (Electronic Frontier Finland). *A Report on the Finnish E-voting Pilot*. [online] Available from: <https://www.verifiedvoting.org/wp-content/uploads/2014/09/Finland-2008-EFFI-Report.pdf> [Accessed 31 May 2018].
- [19] *Explanatory Memorandum to Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting*. Document Number CM(2017)50-add1final. Council of Europe.
- [20] Falter, J. W. and Schoen H. (2014) *Handbuch Wahlforschung*. 2., überarbeitete Auflage. Springer VS, Wiesbaden.
- [21] Hessisches Statistisches Landesamt. (2018) *Statistische Berichte, Kennziffer B VII 2-3 – 5j/18, Die Landtagswahl in Hessen am 28. Oktober 2018, Vorläufige Ergebnisse*. [online] Available from: [https://statistik.hessen.de/sites/statistik.hessen.de/files/BVII2-3\\_5j18.pdf](https://statistik.hessen.de/sites/statistik.hessen.de/files/BVII2-3_5j18.pdf) [Accessed 2 November 2018].
- [22] Karin Hurrle. (2018) Müssen entlassene Mitarbeiter nun wieder die Zeche für ein Missmanagement zahlen? *Nachrichten Regional*, 23 January. [online] Available from: <https://www.nachrichten-regional.de/index.php/%C3%BCberregional/6733-regio-post-pfalz-und-regio-post-beteiligungsgesellschaft-ein-unddurchsichtiges-konstrukt.html> [Accessed 4 November 2018].
- [23] *Länderinformationen und internationale Brieflaufzeiten*. [online] Available from: <https://www.deutschepost.de/de/b/briefe-ins-ausland/laenderinformationen.html>
- [24] Landgericht Regensburg. (2018) *Strafverfahren wegen Verdachts der Wahlmanipulation in Geiselhörung*. [press release] 15 October. Available from: <https://www.justiz.bayern.de/gerichte-und-behoerden/landgericht/regensburg/presse/2018/7.php> [Accessed 2 November 2018].
- [25] Liebowitz, S. J.; Margolis, Stephen E. (1995) Path dependence, lock-in and history. *Journal of Law, Economics, and Organization*. 11.

- [26] Müller-Török, R. and Pautsch, A. (2015) Stochastische Verfälschungen von Wahlergebnissen bei grenzüberschreitender Briefwahl?. *Verwaltung und Management*, 4.
- [27] Nohlen, D. (2014) *Wahlrecht und Parteiensystem – Zur Theorie und Empirie der Wahlsysteme*, 7., überarbeitete und aktualisierte Auflage. Lizenzausgabe für die Bundeszentrale für politische Bildung, Verlag Barbara Budrich, Opladen/Toronto.
- [28] Pautsch, A. and Müller-Török, R. (2015) Die grenzüberschreitende Zustellung von Briefwahlunterlagen vor den Schranken des Völkerrechts – Eine übersehene Problematik?. *Zeitschrift für Rechtspolitik*, 3.
- [29] Prosser, A., Pautsch, A. and Müller-Török, R. Legal Aspects of Cross-Border Delivery of Voting Documents – A Neglected Issue?. In: *Proceedings of the 2015 2nd International Conference on Electronic Governance and Open Society: Challenges in Eurasia*, ACM New York NY 2015.
- [30] *Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting*. Council of Europe.
- [31] Ritter, G. A. and Niehuss, M. (1991) *Wahlen in Deutschland 1946–1991*, C.H. Beck, München.
- [32] Ritter, G. A. and Niehuss, M. (1995) *Wahlen in Deutschland 1991–1994*, C.H. Beck, München.
- [33] Schreiber, W.; Hahlen, J. and Strelen, K.-L. (2017) *BWahlG Kommentar zum Bundeswahlgesetz unter Einbeziehung des Wahlprüfungsgesetzes, des Wahlstatistikgesetzes, der Bundeswahlordnung und sonstiger wahlrechtlicher Nebenvorschriften*. 10., vollständig neubearbeitete Auflage. Carl Heymanns Verlag.
- [34] *Soziale Selbstverwaltung*. [online] Available from: <https://www.sozialwahl.de/sozialwahl/die-sozialwahl-auf-einen-blick/> [Accessed 31 May 2018].
- [35] *Spiegel Online*. (2018) Zusteller der Deutschen Post sollen in neuen Betrieb ausgelagert werden. 12 March. [online] Available from: <https://www.spiegel.de/wirtschaft/unternehmen/deutsche-post-zusteller-sollen-in-neuen-betrieb-ausgelagert-werden-a-1197588.html>
- [36] Stein, R. and Müller-Török, R. (2010) Die Europäische Bürgerinitiative aus Sicht nationaler Wahlbehörden: Probleme der Verifikation von Unterstützungserklärungen in der Praxis. *Verwaltung und Management*, 5.

- [37] *The Telegraph*. (2017) Threat of Royal Mail Strike Lessens as Progress Made in Union Talks. 6 December. [online] Available from: <https://www.telegraph.co.uk/business/2017/12/06/threat-royal-mail-strike-lessens-progress-made-union-talks/>
- [38] *United States vs. Ramsey* (1977) 431 U.S. 606.
- [39] *Verfassungsgerichtshof, V 85-96/11-15*, 13 December 2011. [online] Available from: [https://www.vfgh.gv.at/downloads/VfGH\\_V\\_85-96-11\\_e-voting.pdf](https://www.vfgh.gv.at/downloads/VfGH_V_85-96-11_e-voting.pdf) [Accessed 31 May 2018].
- [40] *Verfassungsgerichtshof, W I 6/2016-125*, 1 July 2016. [online] Available from: [https://www.ris.bka.gv.at/Dokumente/Vfgh/JFT\\_20160701\\_16W\\_I00006\\_00/JFT\\_20160701\\_16W\\_I00006\\_00.pdf](https://www.ris.bka.gv.at/Dokumente/Vfgh/JFT_20160701_16W_I00006_00/JFT_20160701_16W_I00006_00.pdf) [Accessed 31 May 2018].
- [41] White, I. (2015) *Electoral Offences since 2010*, House of Commons Library Briefing Paper Number 625.
- [42] White, I. and Coleman, Ch. (2011) *Postal Voting & Electoral Fraud*, SN/PC/3667, House of Commons Library.



DOI 10.5817/MUJLT2019-1-2

## THE RIGHT TO A FAIR TRIAL IN AUTOMATED CIVIL PROCEEDINGS

by

MARIA DYMITRUK<sup>\*</sup>

*Challenges associated with the use of artificial intelligence (AI) in law are one of the most hotly debated issues today. This paper draws attention to the question of how to safeguard the right to a fair trial in the light of rapidly changing technologies significantly affecting the judiciary and enabling automation of the civil procedure. The paper does not intend to comprehensively address all aspects related to the right to a fair trial in the context of the automation of civil proceedings but rather seeks to analyse some legal concerns from the perspective of the Article 6 of the European Convention on Human Rights and the case-law of the European Court of Human Rights. Section 1 discusses the issues of using artificial intelligence in the justice and automation of the judicial proceedings. Section 2 is devoted to the judge supporting system based on artificial intelligence and psychological requirements of its practical use. Section 3 presents the right to a fair trial in civil cases established by the Article 6 of the European Convention on Human Rights, while subsequent sections characterize its elements with respect to the possibility to automate civil proceedings: a right to have case heard within a reasonable time in section 4 and a right to a reasoned judgment in section 5.*

### KEY WORDS

*Artificial Intelligence, Automation, Civil Proceedings, Right to a Fair Trial*

### 1. INTRODUCTION

The law and the judiciary are elements of social life.<sup>1</sup> Their main purpose is to regulate interpersonal relations. Legal norms are meant to indicate what

---

<sup>\*</sup> maria.dymitruk@uwr.edu.pl; PhD student; Research Centre on Legal and Economic Issues of Electronic Communication; Faculty of Law, Administration and Economics; University of Wrocław, Poland.

people shall or must do; what is forbidden or allowed to. The law could not fulfill its function if there were not for institutions providing its compliance (an application and an execution). The judiciary – one of three main branches of state's government – was assigned to perform this function. The justice system, as almost all modern spheres of social life, is currently experiencing changes caused by technological development. A lot of attention has been recently paid to the possibility to use the artificial intelligence (AI) tools in order to improve the judiciary. This concept is expressed both in scientific initiatives,<sup>2</sup> as well as in the endeavors of the public authorities of some countries.<sup>3</sup> Although a scientific research on the AI applications in law has been carried out since the 1970s,<sup>4</sup> many of the AI techniques require further study and in-depth analysis of their societal implications. Issues arising from the use of AI as a part of the legal decision-making process are manifold and complex. At the same time, the debate about its possible consequences both for individuals and societies is at an early stage.<sup>5</sup> Nevertheless, it should not prevent efforts towards understanding the role of the judiciary and the human rights concerns in the context of the development of the artificial intelligence technologies.

This paper analyses the possibility to automate the civil proceedings by creating an artificial intelligence system, which is able to carry out

---

<sup>1</sup> Quoting McGinnis and Pearce: "Law is an information technology – a code that regulates social life" (see McGinnis, J. O. and Pearce, R. G. (2014) The great disruption: how machine intelligence will transform the role of lawyers in the delivery of legal services. *Fordham Law Review*, 82 (6), p. 3041).

<sup>2</sup> E.g. Floris Bex, Henry Prakken, Tom van Engers and Bart Verheij (eds.). (2017) special issue of Artificial Intelligence and Law Journal "AI4J". *Artificial Intelligence and Law*, 25 (1); Giovanni Sartor and Luther Karl Cranting (eds.). (1998) *Judicial Applications of Artificial Intelligence*. Dordrecht: Springer Netherlands; Barros, R. et al. (2018) Case Law Analysis with Machine Learning in Brazilian Court. In: Malek Mouhoub, Samira Sadaoui, Otmane Ait Mohamed and Moonis Ali (eds.). *IEA/AIE 2018*, Cham: Springer.

<sup>3</sup> As an example, the Brazilian project-in-progress *VICTOR* aims to support the Brazilian Supreme Court by analysing the lawsuit cases that reach the Court, using document analysis and natural language processing tools. *VICTOR* is a project at the Brazilian Supreme Court, developed in a partnership with the University of Brasília. For more information see *Victor*. [online] Available from: <http://gpam.unb.br/victor/> [Accessed 30 January 2019].

<sup>4</sup> E.g. Buchanan, B. and Headrick, T. (1970) Some Speculation About Artificial Intelligence and Legal Reasoning. *Stanford Law Review*, 23 (1), pp.40–62; McCarty, L. T. (1977) Reflections on "Taxman": An Experiment in Artificial Intelligence and Legal Reasoning. *Harvard Law Review*, 90, pp. 837–893.

<sup>5</sup> Committee of experts on internet intermediaries (MSI-NET). (2018) *Algorithms and Human Rights – Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications*. Council of Europe. Available from: <https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5> [Accessed 30 January 2019].

the judicial decision-making process. In this respect, artificial intelligence may be successfully used in two forms: as an independent adjudicating entity or as a judge's supporting tool. In the first model, the AI system shall settle legal cases unassisted (the system adjudicates instead of a human judge). The second model focuses on the use of AI as a judge-supporting system. Such a supporting tool should provide a judge with a final proposal of the decision after finding relevant provisions, analysis of the case-law and review of the doctrine.

The presented models of the automated civil proceedings are possible to be implemented from the technical point of view (at least in some civil cases). Nevertheless, both of them require prior detailed analysis of their compatibility with legal frameworks determining the shape and the functions of the civil procedure. What is important, both models have different level of a human judge involvement in the decision-making process. According to the model of AI as an independent adjudicating entity, the judge is not directly involved in the reasoning process of the system, which takes a binding legal decision unassisted. On the other hand, the judge's supporting model assumes that the system's proposal will be afterwards verified by human judge, who after assessing the decision with all his competences and knowledge, will consider the decision as:

- (a) completely correct (and as a result, will issue identical decision);
- (b) only partially correct (what will result with the necessity to change the content of the decision and possibly – issue a decision which is different from the system-suggested one);
- (c) entirely incorrect (resulting in rejection of the system's proposal and the necessity to conduct separate legal reasoning and take a legal decision by a human judge).

Obviously, due to the complexity of the judicial decision-making process, the possibility to use AI as a judge-supporting system (when compared to the first model of unassisted decision-making) is much more realistic. Moreover, it can be implemented sooner. However, the research on the automation of the judicial proceedings shall not focus only on judicial decision support systems. In my opinion, in the future they will constitute only the first stage in the process of full automation of the judicial proceedings and possible creation of the AI-judge. Modern achievements

in the field of AI & law lead to the conclusion that use of artificial intelligence in the judiciary is a foreseeable future, and not only futurological issue.<sup>6</sup>

## 2. QUASI-AUTOMATED DECISION-MAKING

As indicated above, the automation of the civil proceedings may have two forms:

- (a) of handing over the whole adjudicating process in hands of the AI system taking legal decisions, which are binding to parties to the proceedings; and
- (b) using AI to create the judge's support system, which shall provide the judge with the proposal of the case settlement.

With regard to the second model, one may ask completely justified question: *what influence on the existence of the right to a fair trial may have the fact, whether the judge is using any tools in his work or not?* Despite appearances, also the use of AI in the judicial decision support systems is of great importance for obedience of the right to a fair trial. It might have seemed that this model is neutral to this right, as a decision-making process still remains in human's hands. However, it turns out that using AI only as a supporting tool for human judges may have an equivalent effect as the full automation of the civil proceedings. It is connected with psychological results of human behavior and the "persuasiveness" of the AI supporting systems.

The publication of the Council of Europe entitled "*Algorithms and Human Rights – Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications*" prepared by the *Committee of Experts on Internet Intermediaries (MSI-NET)* in March 2018 correctly distinguishes fully automated decision-making (in which the decision is made by the AI system without participation of a human judge) and semi-automated decision-making (the system presents the suggested proposal, but it is the human who formally takes final decision).<sup>7</sup> The authors of the publication have also accurately noticed

<sup>6</sup> E.g. Estonia runs a project to introduce AI into the justice system. For more information see Niler, E. (2019) *Can AI be a Fair Judge in Court? Estonia Thinks So*. [online] Available from: <https://www.wired.com/story/can-ai-be-fair-judge-court-estonia-thinks-so/> [Accessed 29 April 2019].

<sup>7</sup> Committee of experts on internet intermediaries (MSI-NET), op. cit., p. 8.



that the algorithms are increasingly used in the context of the civil and the criminal justice systems where artificial intelligence is being developed to eventually support or replace decision-making by human judges.<sup>8</sup> An emphasis was also put on the fact that in cases where the human judge is supported by the algorithm-based system:

*“the human being may often be led to ‘rubber stamp’ an algorithmically prepared decision [...]. Thus, while it may seem logical to draw a distinction between fully automated decision-making and semi-automated decision-making, in practice the boundaries between the two are blurred”.*<sup>9</sup>

*“Given the pressure of high caseloads and insufficient resources from which most judiciaries suffer, there is a danger that support systems based on artificial intelligence are inappropriately used by judges to “delegate” decisions to technological systems that were not developed for that purpose and are perceived as being more ‘objective’ even when this is not the case. Great care should therefore be taken to assess what such systems can deliver and under what conditions that may be used in order not to jeopardise the right to a fair trial”.*<sup>10</sup>

The doubts indicated in the publication are confirmed by the experimental psychological research. It turns out that despite people’s knowledge and competences, they are often willing to follow the advice of the AI system without verifying its correctness. There are very interesting studies conducted outside the legal sphere by *Salem et al.*<sup>11</sup> and *Robinette et al.*<sup>12</sup> Both studies were conducted in order to verify the human’s trust level towards the artificial intelligence systems when the machines were intentionally designed to act in an obviously inappropriate manner. *Salem et al.* focused on human-robot interaction by using home companion robot. They investigated how the perception of erroneous robot behavior may influence human interaction choices and the willingness to cooperate

---

<sup>8</sup> Op. cit., p. 11.

<sup>9</sup> Op. cit., p. 8.

<sup>10</sup> Op. cit., p. 12.

<sup>11</sup> Salem, M. et al. (2015) Would You Trust a (Faulty) Robot? Effects of Error, Task Type and Personality on Human-Robot Cooperation and Trust. In: *10th Annual ACM/IEEE International Conference on Human-Robot Interaction*, Portland, Oregon, USA. 2–5 March, pp. 141–148.

<sup>12</sup> Robinette, P. et al. (2016) Overtrust of Robots in Emergency Evacuation Scenarios. In: *11<sup>th</sup> Annual ACM/IEEE International Conference on Human Robot Interaction*, Christchurch, New Zealand, 7–10 March.

with the robot by following a number of its unusual requests. On the other hand, *Robinette et al.* performed an experiment concerning an emergency scenario, where in the first place a participant interacts with a robot in a non-emergency task to experience its behavior and afterwards chooses whether to follow the robot's instructions in an emergency or not. Both experiments proved that humans have tendency to over-trust the automated decision-making systems. This trust is so significant that people follow the robot's advice even though they have previously witnessed their faulty activity. As a result, the participants of the research complied with a faulty robot's unusual requests (such as "*Please pour the orange juice from the bottle into the plant on the windowsill*"<sup>13</sup>) or followed the lead of a potentially dysfunctional emergency guide robot in case of fire alarm.<sup>14</sup>

Both of the abovementioned studies concerned cooperation between the AI system and non-expert user in everyday situations, which did not require any specialist knowledge of any field to be involved. The civil proceedings and the cooperation between the system supporting the judge and the judge himself is obviously of completely different character. The judge is an expert in the field of law. His vast competences make it possible to verify the correctness of the legal decision suggested by the AI system, which is about to be taken in particular civil proceedings. The extensive possibilities to control the AI system allow a theoretical hypothesis that a judge, as an expert in the field of law, will be more "resistant" to the persuasiveness of the AI systems. However, it turns out that the psychological effect of the over-trust towards the AI systems presented by *Salem et al.* and *Robinette et al.* concerns lawyers and legal reasoning as well.

*Dijkstra* carried out a psychological experiment examining how lawyers respond to an advice automatically generated by legal knowledge-based systems while resolving a legal case.<sup>15</sup> It turned out that lawyers have difficulties with the assessment of the accuracy of the automatically generated advice, as they focus on argumentation presented by the system and ignore alternative solutions. They carelessly accept the system's advice

---

<sup>13</sup> Salem, M. et al., op. cit., p. 143.

<sup>14</sup> Robinette, P. et al., op. cit., pp. 104–107.

<sup>15</sup> Dijkstra, J. (2001) Legal Knowledge-based Systems: The Blind leading the Sheep? *International Review of Law, Computers & Technology*, 15 (2), pp. 119–128.

(including incorrect one, put into experiment on purpose), and in case of being advised by two entities (the system and the human) participants considered the system's advice "*to be more objective and rational than the human advices*" (even when the human's advice was identical as the system's). As a result, the participants performing legal reasoning without the support of the system achieved better results than the participants using the decision support system.<sup>16</sup>

The research proves that people tend to use computer systems to reduce the decision-making process rather than to increase the quality of their own decisions.<sup>17</sup> It is therefore probable that the use of the decision support systems would not improve civil proceedings. An excessive reliance on the decision automatically generated by the AI system may result with the fact that decisions about the legal issues of the citizens would actually be made by the computer program – despite the impression that all principles of human adjudicating process are obeyed. The above conclusions prove that the "persuasiveness" of judge's supporting systems can result not only in "semi-automated decision-making", but also in "quasi-automated decision-making" whereby the human part in judging would be seeming and the role of the judge would be limited to indiscriminate following the system's suggestions.

### 3. THE RIGHT TO A FAIR TRIAL

The right to a fair trial is an essential mechanism guarantying obedience of the fundamental human rights and freedoms. It represents one of the most essential safeguards for the respect of democracy and the rule of law within the European legal system.<sup>18</sup> Not surprisingly, it occupies a central place in the *European Convention on Human Rights (ECHR)*.<sup>19</sup> Article 6 of the ECHR guarantees the procedural rights of parties to judicial proceedings, which are meant to create conditions to make an accurate and fair judgement.

<sup>16</sup> Dijkstra, J., op. cit., p. 122.

<sup>17</sup> Todd, P. and Benbasat, I. (1994) The Influence of Decision Aids on Choice Strategies: An Experimental Analysis of the Role of Cognitive Effort. *Organizational Behavior and Human Decision Processes*, 60 (1), pp. 36–74.

<sup>18</sup> Rozakis, C. (2004) The right to a fair trial in civil cases. *Judicial Studies Institute Journal*, 4 (2), p. 96.

<sup>19</sup> *Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols Nos. 11 and 14, supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16*, 4 November 1950. Available from: [https://www.echr.coe.int/Documents/Convention\\_ENG.pdf](https://www.echr.coe.int/Documents/Convention_ENG.pdf) [Accessed 30 January 2019].

Out of the three paragraphs of Article 6, the first applies both to civil and criminal proceedings (it provides the same guarantees, irrespective of civil or criminal nature of the proceedings), whereas the second and third paragraphs apply to criminal proceedings.<sup>20</sup> In accordance with Article 6(1) of the ECHR:

*"In the determination of his civil rights and obligations [...], everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law [...]"*.<sup>21</sup>

This article requires from public authorities not only a mere abstention from acts which may be detrimental to an individual, but most of all taking the initiatives to ensure good administration of justice within the state.<sup>22</sup>

The European Court of Human Rights reads Article 6 of the ECHR extensively and attempts to give practical effect to the purpose of the provision. Consequently, the Court has derived from Article 6 a number of specific rights through teleological, non-literal and contextual interpretation.<sup>23</sup> In the result, the Strasbourg case-law has led to the creation of new guarantees which are not specifically mentioned in the article but emanate from the spirit of protection guaranteed by Article 6.<sup>24</sup>

<sup>20</sup> According to some researchers, paragraphs 2 and 3 are applicable only in criminal proceedings (See Brems, E. (2005) *Conflicting Human Rights: An Exploration in the Context of the Right to a Fair Trial in the European Convention for the Protection of Human Rights and Fundamental Freedoms*. *Human Rights Quarterly*, 27 (1), p. 295), while other experts indicate that they mainly refer to criminal proceedings, but *"the Strasbourg organs have widely construed the obligations appearing on paragraphs 2 and 3, which has led to their application by analogy in civil cases, whenever feasible."* (See Rozakis, C., op. cit., p. 96).

<sup>21</sup> Similar guarantees have been established in: (a) article 47 of *The Charter of Fundamental Rights of the European Union*, 7 December 2000 (OJ C 326, 26.10.2012, pp. 391–407). Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT> [Accessed 30 January 2019]; (b) article 14 of *The United Nations (UN) International Covenant on Civil and Political Rights*, adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966, entry into force 23 March 1976, in accordance with Article 49. Available from: <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx> [Accessed 30 January 2019]; (c) article 10 of *The UN Universal Declaration of Human Rights proclaimed by the United Nations General Assembly (General Assembly resolution 217 A)*. 10 December 1948. Available from: [http://www.un.org/en/udhrbook/pdf/udhr\\_booklet\\_en\\_web.pdf](http://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf) [Accessed 30 January 2019].

<sup>22</sup> Rozakis, C., op. cit., p. 96.

<sup>23</sup> Vitkauskas, D. and Dikov, G. (2017) *Protecting the right to a fair trial under the European Convention on Human Rights: A handbook for legal practitioners*. 2nd ed. Council of Europe, p. 12. Available from: <https://rm.coe.int/protecting-the-right-to-a-fair-trial-under-the-european-convention-on-168075a4dd> [Accessed 30 January 2019].

<sup>24</sup> Rozakis, C., op. cit., p. 97.

In the case-law of the *European Court of Human Rights* in Strasbourg, it is emphasized that the right to a fair trial must be “practical and effective”, not “theoretical or illusory”.<sup>25</sup>

*“The essence of the right of access to a court is impaired when the rules cease to serve the aims of legal certainty and the proper administration of justice and form a sort of barrier preventing the litigant from having his or her case determined on the merits by the competent court”.*<sup>26</sup>

Analysing Article 6 of the ECHR, the Court often puts emphasis on two elements: “legal certainty” and “proper administration of justice”. Both of them must be interpreted

*“in the light of the Preamble to the Convention, which declares the rule of law to be part of the common heritage of the Contracting States”*<sup>27</sup>

and

*“the principle of legal certainty constitutes one of the basic elements of the rule of law”*<sup>28</sup>.

The role that the right to a fair trial has in democratic societies shall not be forgotten when analysing the admissibility to use artificial intelligence in the judiciary. It is particularly important in the context of the crisis of the rule of law concept in many European countries.

As the fundamental requirement of the rule of law, the notion of legal certainty shall refer not only to the substantive law but also to the procedural requirements of the civil proceedings. It is a complex, multi-faceted term. The “procedural legal certainty” is designed to ensure a fair trial to the parties to the proceedings. Its purpose is mainly to provide the parties with legal possibility to establish their legal situation in the judicial proceedings. It does not prejudice the final result of the proceedings. Its main purpose is rather to make the non-breaching party feels protected when someone violates its rights.

<sup>25</sup> *Bellet v. France* (1995) No. 23805/94, § 38; *Zubac v. Croatia* (2018) No. 40160/12, §§ 76–79; *Airey v. Ireland* (1979) No. 6289/73, § 24; *Perez v. France* (2004) No. 47287/99, § 80.

<sup>26</sup> *Zubac v. Croatia* (2018) No. 40160/12, § 98.

<sup>27</sup> *Brumărescu v. Romania* (1999) No. 28342/95, § 61; *Nejdet Şahin and Perihan Şahin v. Turkey* (2011) No. 13279/05, § 57.

<sup>28</sup> *Beian v. Romania* (no. 1) (2007) No. 30658/05, § 39; *Lupeni Greek Catholic Parish and Others v. Romania* (2016) No. 76943/11, § 116.

As it is correctly emphasised by the *European Court of Human Rights*, Article 6 of the ECHR should be interpreted in the light of present-day conditions, while taking into account the prevalent economic and social circumstances. The concept of “*the Convention as a living instrument*”<sup>29</sup> shall also refer to the technological changes which may have influence on the justice, including the possibility of automation of the civil proceedings with AI tools. The Court has not yet discussed the right to court in the light of potential use of AI in the judiciary, however, it may seem that due to its increasing application, this issue may one day become the subject of the Court's case-law. Regardless, it may seem that it is worth to start looking into this problem. Deciding, whether the right to a fair trial will be correctly realized in automated civil proceedings, is a prerequisite for further considerations on the usefulness of the artificial intelligence technology in the judiciary. Indeed, the parties to automated civil procedure still should be entitled to procedural protection guaranteed by Article 6 of the ECHR. Consequently, all standards established by the Court pursuant to Article 6 of the ECHR shall be respected. It is impossible in the limited space of this paper to deal exhaustively with all procedural guarantees provided by Article 6 of the ECHR which have been raised by the case-law of the Court and concern civil proceedings. For that reason, this paper concentrates on two elements: the right to have case heard within a reasonable time and the right to a reasoned judgment.

#### 4. THE RIGHT TO HAVE CASE HEARD WITHIN A REASONABLE TIME

The duty to provide a final judgment within a reasonable time derives both from the wording of Article 6 of the ECHR and from the principle of effectiveness. As the Court has pointed out:

*“in requiring cases to be heard within a ‘reasonable time’, the Convention underlines the importance of administering justice without delays which might jeopardise its effectiveness and credibility”.*<sup>30</sup>

The discussed right includes a structural obligation for the state parties to the ECHR to organize their legal system in such a manner that justice can

<sup>29</sup> *Tyrer v. United Kingdom* (1978) No. 5856/72, § 31.

<sup>30</sup> *H. v. France* (1989) No. 10073/82, § 58; *Vernillo v. France* (1991) No. 11889/85, § 38; *Katte Klitsche de la Grande v. Italy* (1994) No. 12539/86, § 61.

be done within a reasonable time.<sup>31</sup> It ensures that all parties to court proceedings, whether criminal or civil, are protected from excessive delays. An access to the courts will remain largely theoretical and illusory if delays in legal proceedings result in keeping an individual in a protracted state of doubt that may be considered akin to a denial of justice.<sup>32</sup> Since delayed justice is denied justice, one should not ignore the efficiency potential the creators of the AI systems can offer to the judiciary.

Regarding the length of the court proceedings (the most obvious element of the right to a fair trial with respect to the automation of civil procedure) AI has undeniable advantage: it is able to process information on a scale which is out of reach of any human judge. Thanks to the machine learning and other AI techniques the work of a judge may be significantly improved. Actions taken within continental law, such as determination of the legal basis of the decision, analysis of the case-law or doctrine could be carried out more accurately and incomparably faster than by any human judge. Many hours search of the precedence or the opinion of the legal doctrine could be shortened to a few seconds. The arduous analysis of the court files (often consisting of many tomes) may also be an option for AI tools. It would speed up procedure and enable more accurate and complete analysis of the case. The computer system, which is resistant to monotony, exhaustion and other biological and psychological limitations of human body, would be able to carry out this job as good as humans in traditional civil procedure (or even better). AI may be successfully used in order to improve evidence proceedings, during the analysis of the arguments provided by the participants of the trial and during many other stages of the proceedings.

It is worth highlighting that from a statistical point of view, the number of findings of violations of the right to be tried within a reasonable time has decreased considerably in recent years. In 2012 and 2013 a failure to uphold this right was the 2<sup>nd</sup> out of 24 causes of violation of the ECHR, and in 2014, 2015 and 2016 these failures fell to the 5<sup>th</sup> position.<sup>33</sup> Nevertheless,

<sup>31</sup> Brems, E., op. cit., p. 297.

<sup>32</sup> Edel, F. (2007) *The length of civil and criminal proceedings in the case-law of the European Court of Human Rights*. Human rights files, No. 16. 2nd ed. Council of Europe Publishing, p. 6. Available from: [https://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-16\(2007\).pdf](https://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-16(2007).pdf) [Accessed 30 January 2019].

<sup>33</sup> Calvez, F. and Regis, N. (2018) *Length of court proceedings in the member states of the Council of Europe based on the case law of the European Court of Human Rights*. [online] 3rd ed. Council of Europe Publishing, p. 5. Available from: <https://rm.coe.int/cepej-2018-26-en-rapport-calvez-regis-en-length-of-court-proceedings-e/16808ffc7b> [Accessed 30 January 2019].

the backlogs in dealing with cases constitute a serious issue for courts of many European countries. For example, in Poland recent statistical data published by the *Polish Ministry of Justice* indicate that the backlog in dealing with civil cases in Polish common courts is currently at the level of 2.828.932 unresolved cases.<sup>34</sup> Although the current rate of settling the cases is high (i.e. the difference between the number of cases delivered to the common courts in a given period of time and the number of cases resolved), it is a consequence of delays caused in previous years. What is important, this situation is typical not only for Poland. *The European Commission for the Efficiency of Justice* emphasizes that backlogs of cases in courts are caused by the increase in litigation with no concomitant increase in resources, which is one of the main factors in excessive length of proceedings in many European countries.<sup>35</sup> The problem of processing the growing stock of cases in the event of excessive court workloads and the fact that priority must go to old or pending cases, endanger the right to a fair trial to the extent that any remedy shall be considered. Although the reasons of the backlogs may be different, it may seem that the possibility to automate some of the proceedings may constitute a good solution to speed up at least some kind of cases, and as a result would contribute to realize the right to a fair trial in a more appropriate manner.

## 5. THE RIGHT TO A REASONED JUDGMENT

The right to a fair trial also includes the possibility to learn the reasons of the court's decision.<sup>36</sup> *The European Court of Human Rights* indicates that

*"according to its established case-law reflecting a principle linked to the proper administration of justice, judgments of courts and tribunals should adequately state the reasons on which they are based".*<sup>37</sup>

The fairness of the court's actions is reflected the most in the justifications of the judicial decisions prepared by the judges, in which they describe the factual and legal circumstances of the case, legal

<sup>34</sup> The most recent data of the Ministry of Justice were updated in the third quarter of 2018 (i.e. they remain actual as of 30 September 2018). See *Ewidencja spraw w sądach powszechnych według działów prawa I instancyjności w III kw. 2018 r.*, p. 1. Available from: <https://isws.ms.gov.pl/pl/baza-statystyczna/opracowania-jednoroczne/rok-2018/download,3756,0.html> [Accessed 30 January 2019].

<sup>35</sup> Calvez, F. and Regis, N., op. cit., p. 42.

<sup>36</sup> *Hadjianastassiou v. Greece* (1992) No. 12945/87.

<sup>37</sup> *Hirvisaari v. Finland* (2001) No. 49684/99, § 30.



reasoning and manner of interpretation, as well as they refer to the arguments presented by the parties during the trial. The right to a reasoned decision, therefore, protects an individual from arbitrariness. For this reason, the Court points out that a court decision should contain reasons that are sufficient to reply to the essential aspects of the party's factual and legal – substantive or procedural – argument.<sup>38</sup>

The justification of the judicial decision shall ensure the transparency of the judiciary, and as a result, shall increase public trust towards the state authorities. On the other hand, the justification serves the realization of the legal interest of the party to the proceedings. Its existence is a condition to argue with the court decision and – if necessary – to lodge an appeal against the decision. Lack of justification of the judicial decision would cause that the right to appeal against the final decision would be purely illusory.<sup>39</sup> Moreover, a justification demonstrates to the parties that they have been actually heard.<sup>40</sup> Thus, the right to a reasoned decision constitutes a guarantee that during the civil proceedings, rights of the party have been respected, and also confirms the public scrutiny of the administration of justice.<sup>41</sup>

Any AI system constructed for the purpose of judicial decision-making, if it does not possess the power of explaining its action, will be potentially dangerous to the right to a fair trial. Some of the contemporary AI systems, in particular those based on the machine learning, are not transparent. Their internal workings are opaque or too complex to furnish explanations on why a certain decision has been taken.<sup>42</sup> Usually, the most accurate AI models are not very explainable (for example deep neural nets, boosted trees, random forests, and support vector machines), and the most interpretable models are less accurate (for example linear or logistic regression).<sup>43</sup>

The solution to the lack of transparency of the chosen AI systems and their inability to explain their actions is the concept of the “explainable AI”

<sup>38</sup> *Ruiz Torija v. Spain* (1994) No. 18390/91, §§ 29–30.

<sup>39</sup> Łazarska, A. (2012) *Rzetelny proces cywilny*. Warszawa: Wolters Kluwer Polska, p. 363.

<sup>40</sup> *Fomin v. Moldova* (2011) No. 36755/06, § 31.

<sup>41</sup> *Suominen v. Finland* (2003) No. 37801/97, § 37.

<sup>42</sup> Sileno, G., Boer, A. and van Engers, T. (2018) *The role of Normware in Trustworthy and Explainable AI*. [online] Available from: <https://arxiv.org/abs/1812.02471> [Accessed 30 January 2019].

<sup>43</sup> Adadi, A. and Berrada, M. (2018) Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI). *IEEE Access*, 6, p. 52145.

(XAI). The XAI is a research field, which aims to create understandable AI models with high-efficiency level and make AI systems results more understandable to humans. In the context of the automation of civil proceedings, the opaque nature of AI can be potentially dangerous to the right to a reasoned decision. One of the requirements for the proper functioning of the AI system automating any court proceedings must be its ability to explicate its actions. The impossibility of understanding and validating the decision process of the system can both lead its users to doubt the reliability of the decision that is provided, and violate the right to a reasoned decision. Therefore, the XAI is of great significance for the proper realization of the right to a fair trial and, in the result, for the success of the potential use of AI in civil proceedings.

Taking the above into account, it should be stated that as long as the AI systems are not able to present the manner the specific legal decision was made, their use in order to automate any judicial proceedings (including support of the human judge) shall be deemed unacceptable. The explanation delivered by the system enables the human to have control over the system and makes it possible to verify the reliability of the system's processes and the accuracy of the system's decision. Knowing the reasons of the system's decision is necessary both in the model of full automation of the civil proceedings, as well as in the model of using the AI system as a judge's support tool:

- (a) in the first model, it determines the admissibility to automate the proceedings in general (it should be considered as completely unacceptable and directly violating the right to a reasoned judgement if the AI system does not provide the justification of the decision made against a citizen);
- (b) in the second model, it enables the judge to verify the decision (without the possibility to check the correctness of the system, the use of AI as a judge's support tool would result in "quasi-automated decision-making" – see section 2).

As a result, the great potential of effectiveness of the AI models (presented in section 4) is limited by their incapacity to explain their decisions. Only existence of the fully explainable AI systems may enable the automation of the civil proceedings without endangering the right

to a fair trial. For this reason, any XAI developing initiatives shall deserve a full support.<sup>44</sup>

## 6. CONCLUSION

Thanks to artificial intelligence, the work of a judge and functioning of the entire civil justice system may be significantly improved. On the other hand, the use of AI in order to resolve civil cases cannot incidentally imperil the right to a fair trial. The key is to understand what can or cannot be achieved thanks to algorithms, and not to let their use in the judiciary be dictated merely by considerations of efficiency or effectiveness alone. Significant attention shall be paid not only to the acceleration of the civil proceedings but also to increase the quality of the civil justice, full realization of the right to a fair court trial and increase of the citizens' satisfaction of the judiciary.

## LIST OF REFERENCES

- [1] Adadi, A. and Berrada, M. (2018) Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI). *IEEE Access*, 6.
- [2] *Airey v. Ireland* (1979) No. 6289/73.
- [3] Barros, R. et al. (2018) Case Law Analysis with Machine Learning in Brazilian Court. In: Malek Mouhoub, Samira Sadaoui, Otmane Ait Mohamed and Moonis Ali (eds.). *IEA/AIE 2018*, Springer, Cham.
- [4] *Beian v. Romania* (no. 1) (2007) No. 30658/05.
- [5] *Bellet v. France* (1995) No. 23805/94.
- [6] Brems, E. (2005) Conflicting Human Rights: An Exploration in the Context of the Right to a Fair Trial in the European Convention for the Protection of Human Rights and Fundamental Freedoms. *Human Rights Quarterly*, 27 (1).
- [7] *Brumărescu v. Romania* (1999) No. 28342/95.
- [8] Buchanan, B. and Headrick, T. (1970) Some Speculation About Artificial Intelligence and Legal Reasoning. *Stanford Law Review*, 23 (1).
- [9] Calvez, F. and Regis, N. (2018) *Length of court proceedings in the member states of the Council of Europe based on the case law of the European Court of Human Rights*. [online] 3rd ed.

---

<sup>44</sup> Such as group of academics operating under the acronym *FAT* or civilian and military researchers funded by the *Defense Advanced Research Projects Agency*, *DARPA* (see *FAT/ML*. [online] Available from: <http://www.fatml.org> [Accessed 30 January 2019]; *DARPA*. [online] Available from: <https://www.darpa.mil/program/explainable-artificial-intelligence> [Accessed 30 January 2019]).

- Council of Europe Publishing. Available from: <https://rm.coe.int/cepej-2018-26-en-rapport-calvez-regis-en-length-of-court-proceedings-e/16808ffc7b> [Accessed 30 January 2019].
- [10] Committee of experts on internet intermediaries (MSI-NET). (2018) *Algorithms and Human Rights – Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications*. Council of Europe. Available from: <https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5> [Accessed 30 January 2019].
- [11] *Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols Nos. 11 and 14, supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16*, 4 November 1950. Available from: [https://www.echr.coe.int/Documents/Convention\\_ENG.pdf](https://www.echr.coe.int/Documents/Convention_ENG.pdf) [Accessed 30 January 2019].
- [12] Dijkstra, J. (2001) Legal Knowledge-based Systems: The Blind leading the Sheep? *International Review of Law, Computers & Technology*, 15 (2).
- [13] Edel, F. (2007) *The length of civil and criminal proceedings in the case-law of the European Court of Human Rights*. Human rights files, No. 16. 2nd ed. Council of Europe Publishing. Available from: [https://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-16\(2007\).pdf](https://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-16(2007).pdf) [Accessed 30 January 2019].
- [14] Ewidencja spraw w sądach powszechnych według działów prawa i instancyjności w III kw. 2018 r. Available from: <https://isws.ms.gov.pl/pl/baza-statystyczna/opracowania-jednoroczne/rok-2018/download,3756,0.html> [Accessed 30 January 2019].
- [15] Floris Bex, Henry Prakken, Tom van Engers and Bart Verheij (eds.). (2017) special issue of Artificial Intelligence and Law Journal “AI4J”. *Artificial Intelligence and Law*, 25 (1).
- [16] *Fomin v. Moldova* (2011) No. 36755/06.
- [17] Giovanni Sartor and Luther Karl Cranting (eds.). (1998) *Judicial Applications of Artificial Intelligence*. Dordrecht: Springer Netherlands.
- [18] *H. v. France* (1989) No. 10073/82.
- [19] *Hadjianastassiou v. Greece* (1992) No. 12945/87.
- [20] *Hirvisaari v. Finland* (2001) No. 49684/99.
- [21] *Charter of Fundamental Rights of the European Union*, 7 December 2000 (OJ C 326, 26. 10. 2012, pp. 391–407). Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT> [Accessed 30 January 2019].
- [22] *Katte Klitsche de la Grande v. Italy* (1994) No. 12539/86.
- [23] Łazarska, A. (2012) *Rzeczony proces cywilny*. Warszawa: Wolters Kluwer Polska.

- [24] *Lupeni Greek Catholic Parish and Others v. Romania* (2016) No. 76943/11.
- [25] McCarty, L. T. (1977) Reflections on “Taxman”: An Experiment in Artificial Intelligence and Legal Reasoning. *Harvard Law Review*, 90.
- [26] McGinnis, J. O. and Pearce, R. G. (2014) The great disruption: how machine intelligence will transform the role of lawyers in the delivery of legal services. *Fordham Law Review*, 82 (6).
- [27] *Nejdet Şahin and Perihan Şahin v. Turkey* (2011) No. 13279/05.
- [28] Niler, E. (2019) *Can AI be a Fair Judge in Court? Estonia Thinks So*. [online] Available from: <https://www.wired.com/story/can-ai-be-fair-judge-court-estonia-thinks-so/> [Accessed 29 April 2019].
- [29] *Perez v. France* (2004) No. 47287/99.
- [30] Robinette, P. et al. (2016), Overtrust of Robots in Emergency Evacuation Scenarios. In: *11th Annual ACM/IEEE International Conference on Human Robot Interaction*, Christchurch, New Zealand, 7–10 March.
- [31] Rozakis, C. (2004) The right to a fair trial in civil cases. *Judicial Studies Institute Journal*, 4 (2).
- [32] *Ruiz Torija v. Spain* (1994) No. 18390/91.
- [33] Salem, M. et al. (2015) Would You Trust a (Faulty) Robot? Effects of Error, Task Type and Personality on Human-Robot Cooperation and Trust. In: *10th Annual ACM/IEEE International Conference on Human-Robot Interaction*, Portland, Oregon, USA. 2–5 March.
- [34] Sileno, G., Boer, A. and van Engers, T. (2018) *The role of Normware in Trustworthy and Explainable AI*. [online] Available from: <https://arxiv.org/abs/1812.02471> [Accessed 30 January 2019].
- [35] *Suominen v. Finland* (2003) No. 37801/97.
- [36] Todd, P. and Benbasat, I. (1994) The Influence of Decision Aids on Choice Strategies: An Experimental Analysis of the Role of Cognitive Effort. *Organizational Behavior and Human Decision Processes*, 60 (1).
- [37] *Tyrer v. United Kingdom* (1978) No. 5856/72.
- [38] *UN Universal Declaration of Human Rights proclaimed by the United Nations General Assembly (General Assembly resolution 217 A)*. 10 December 1948. Available from: [http://www.un.org/en/udhrbook/pdf/udhr\\_booklet\\_en\\_web.pdf](http://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf) [Accessed 30 January 2019].
- [39] *United Nations (UN) International Covenant on Civil and Political Rights, adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI)*

of 16 December 1966, entry into force 23 March 1976, in accordance with Article 49, Available from: <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx> [Accessed 30 January 2019].

[40] *Vernillo v. France* (1991) No. 11889/85.

[41] *Victor*. [online] Available from: <http://gpam.unb.br/victor/> [Accessed 30 January 2019].

[42] Vitkauskas, D. and Dikov, G. (2017) *Protecting the right to a fair trial under the European Convention on Human Rights: A handbook for legal practitioners*. [online] 2nd ed. Council of Europe. Available from: <https://rm.coe.int/protecting-the-right-to-a-fair-trial-under-the-european-convention-on-/168075a4dd> [Accessed 30 January 2019].

[43] *Zubac v. Croatia* (2018) No. 40160/12.

DOI 10.5817/MUJLT2019-1-3

## LIVING IN A SPAMSTER'S PARADISE: DECEIT AND THREATS IN PHISHING EMAILS

*by*

KRISTJAN KIKERPILL\*, ANDRA SIIBAK\*\*

*The prevalence of using email as a communication tool for personal and professional purposes makes it a significant attack vector for cybercriminals. Consensus exists that phishing, i.e. use of socially engineered messages to convince recipients into performing actions that benefit the sender, is widespread as a negative phenomenon. However, little is known about its true extent from a criminal law perspective. Similar to how the treatment of phishing in a generic manner does not adequately inform the relevant law, a case-by-case legal analysis of seemingly independent offences would not reveal the true scale and extent of phishing as a social phenomenon. The current research addresses this significant gap in the literature. To study this issue, a qualitative text analysis was performed on (N=42) emails collected over a 30-day period from two email accounts. Secondly, the phishing emails were analysed from an Estonian criminal law perspective. The legal analysis shows that in the period of only one month, the accounts received what amounts to 3 instances of extortion, 29 fraud attempts and 10 cases of personal data processing related misdemeanour offences.*

### KEY WORDS

*Criminal Law, Cybercrime, Legal Analysis, Phishing Emails, Qualitative Text Analysis*

---

\* kristjan.kikerpill@gmail.com, Independent Researcher.

\*\* andra.siibak@ut.ee, Professor of Media Studies, Institute of Social Studies, University of Tartu, Estonia.

## 1. INTRODUCTION

It is suggested that more than 281 billion emails were exchanged daily in 2018.<sup>1</sup> Recent malicious online activity reports suggest that about one in every 2000 of these emails is an attempt at phishing,<sup>2</sup> i.e. a cyber-attack which utilises socially engineered messages to convince recipients into performing actions that benefit the sender. Phishing does not generally constitute a separate offence under substantive criminal law<sup>3</sup> but is an umbrella moniker for the collection of offences initiated or committed, among other channels, via email.<sup>4</sup> Therefore, in addition to facilitating legitimate communication in the email ecosystem, the inbox also acts as a honeypot and staging ground for various forms of criminal offences.

Research from different fields provides a rich background to the study of phishing. For example, phishing has been studied extensively by scholars working in the fields of behavioural sciences, psychology and criminology.<sup>5</sup> However, disciplines external to law treat phishing and other computer-related criminal activities as generic negative phenomena without providing an accompanying legal assessment. Applying the *nullum crimen sine lege* principle, findings from disciplines researching phishing as a phenomenon thus do not enable the effective informing of the relevant law. The central problem here is a lack of connection between phishing attacks and the compendium of formally established offences the attacks

---

<sup>1</sup> Radicati Group. (2018) *Executive Summary*. Available from: <https://www.radicati.com/wp-content/uploads/2018/05/Email-Market-2018-2022-Executive-Summary.pdf> [Accessed 20 November 2018].

<sup>2</sup> Symantec. (2018) *Internet Security Threat Report*. Available from: <https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf> [Accessed 20 November 2018].

<sup>3</sup> In the European Union, this notion might be subject to change and harmonisation depending on future developments (see European Commission 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. (2017/0226) 13 September, Recital 9. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:0489:FIN> [Accessed 20 November 2018]).

<sup>4</sup> While email-based attacks are more common, phishing also appears in other forms such as *smishing* or SMS-phishing and *vishing* or voice-phishing.

<sup>5</sup> For example, in psychology and behavioural sciences see Rajivan, P. and Gonzalez, C. (2018) Creative Persuasion: A Study on Adversarial Behaviors and Strategies in Phishing Attacks. *Frontiers in Psychology*, 135 (9); Williams, E. J., Beardmore, A. and Joinson, A. N. (2017) Individual Differences in Susceptibility to Online Influence: A Theoretical Review. *Computers in Human Behavior*, 72, pp. 412–421; Vishwanath, A. et al. (2011) Why Do People Get Phished? Testing Individual Differences in Phishing Vulnerability within an Integrated, Information Processing Model. *Decision Support Systems*, 51 (3), pp. 576–586; in criminology see Hutchings, A. and Hayes, H. (2009) Routine Activity Theory and Phishing Victimization: Who Gets Caught in the 'Net'? *Current Issues in Criminal Justice*, 20 (3), pp. 433–451; Reyns, B. W. (2015) A Routine Activity Perspective on Online Victimization: Results from the Canadian General Social Survey. *Journal of Financial Crime*, 42 (4), pp. 396–411.



constitute. In contrast, mere case-by-case legal analysis of handpicked examples of seemingly independent offences would only succeed in attaching existing criminal law provisions to objective facts, i.e. solving a clearly delimited criminal case. This approach fails to reveal the scale and impact that phishing as a phenomenon entails in society. For the above reasons, the current paper takes a socio-legal approach to explore the phenomenon of phishing. Firstly, a qualitative text analysis was performed on emails (N=42) received over the course of a month, which had initial indications of being phishing attempts. The analysis focused on how perpetrators craft stories and insert influencing techniques into their text for the purposes of manipulating the recipients' will to act or respond. Secondly, the paper provides a legal assessment regarding the results with an aim to fill the gap currently present in phishing literature as well as provide some insight into the real scale of online crime commission.

## 2. CONTEXTUAL BACKGROUND

To the detriment of the public at large, conventional anti-crime efforts are falling short when it comes to cybercrime, including the phenomenon of phishing. In 2013, a study published by the *United Nations Office on Drugs and Crime* suggested that perhaps only 1 % of actual cybercrime victimisation is reported to law enforcement.<sup>6</sup> The underreporting was stated to derive from a lack of awareness about victimisation and of reporting mechanisms, but also victim shame and embarrassment.<sup>7</sup> Perpetrators increasingly choose to take advantage of their potential victims' natural inclination towards deception and threat susceptibility rather than wasting time and resources on overcoming complex technological barriers. As recent literature suggests, criminal actors often employ social engineering techniques to motivate recipients into giving out personal information or performing specific acts.<sup>8</sup>

In general, influencing techniques,<sup>9</sup> or urgency cues, in fraudulent emails are used for two main reasons. Firstly, the senders aim to elicit emotional

---

<sup>6</sup> United Nations Office on Drugs and Crime. (2013) *Draft Comprehensive Study on Cybercrime*. p. 119. Available from: [https://www.unodc.org/documents/organized-crime/UNODC\\_CCP\\_CJ\\_EG.4\\_2013/CYBERCRIME\\_STUDY\\_210213.pdf](https://www.unodc.org/documents/organized-crime/UNODC_CCP_CJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf) [Accessed 20 November 2018].

<sup>7</sup> Op. cit., p. xxi.

<sup>8</sup> See also Williams, E. J., Beardmore, A. and Joinson, A. N. (2017), op. cit.

<sup>9</sup> Williams, E. J., Hinds, J. and Joinson, A. N. (2018) Exploring Susceptibility to Phishing in the Workplace. *International Journal of Human-Computer Studies*, p. 120.

reactions from the recipients by evoking feelings such as fear or threat,<sup>10</sup> which would inhibit the recipients' ability to process the information under review.<sup>11</sup> Secondly, urgency cues are used to draw the recipients' focus away from other aspects of the text, e.g. spelling errors, which could aid the user in determining the email's authenticity.<sup>12</sup> Previous analyses have also shown the prevalence of urgency cues<sup>13</sup> and visceral appeals, such as money, love or sorrow, in eliciting compliance from the targets.<sup>14</sup> Vishwanath and others also found that attention to urgency cues is positively related to the potential victim's likelihood of responding to the fraudulent email.<sup>15</sup>

The approach is certainly well-founded as the rates of users clicking on links directing them to fake websites or opening attachments infected with malware contained in phishing emails hovers around 10 % on average.<sup>16</sup> These high success rates rank phishing emails as the top attack vector used to bypass technology-centred security efforts and attack the human factor instead. Human beings are not considered particularly adept at detecting deception<sup>17</sup> and their abilities are further inhibited with text-based, less rich media such as email.<sup>18</sup> The issue is compounded by the fact that the people being preyed upon by criminal actors consider themselves to be poorly informed about phishing and other malicious activities facilitated by information technology.<sup>19</sup> Additionally, the way modern electronic communications enable access to potential victims plays right into the hands of the perpetrators. Criminal actors employ mass-

<sup>10</sup> Workman, M. (2008) Wisecrackers: A Theory-grounded Investigation of Phishing and Pretext Social Engineering Threats to Information Security. *Journal of the American Society for Information Science and Technology*, 59 (4), pp. 662–674.

<sup>11</sup> Vishwanath, A. et al. (2011), op. cit.

<sup>12</sup> Jakobsson, M. (2007) The Human Factor in Phishing. *Privacy & Security of Consumer Information*.

<sup>13</sup> Atkins, B. and Huang, W. (2013) A Study of Social Engineering in Online Frauds. *Open Journal of Social Sciences*, 1 (3), pp. 23–32.

<sup>14</sup> Button, M. et al. (2014) Online Frauds: Learning from Victims Why They Fall for These Scams. *Australian & New Zealand Journal of Criminology*, 47 (3), pp. 391–408. See also Langenderfer, J. and Shimp, T. A. (2001) Consumer Vulnerability to Scams, Swindles, and Fraud: A New Theory of Visceral Influences on Persuasion. *Psychology and Marketing*, 18, pp. 763–783.

<sup>15</sup> See Vishwanath, A. et al. (2011), op. cit., p. 582.

<sup>16</sup> Verizon. (2017) *Data Breach Investigations Report*, 10th Ed.

<sup>17</sup> Burgoon, J. K. et al. (1994) Interpersonal Deception: Accuracy in Deception Detection. *Communication Monographs*, 61, pp. 303–325.

<sup>18</sup> Burgoon, J. K. et al. (2003) Detecting Deception Through Linguistic Analysis. In: Hsinchun Chen et al. (eds.). *Intelligence and Security Informatics*, Springer.

<sup>19</sup> European Commission. (2017) *Special Eurobarometer 464a: Europeans' Attitudes Towards Cyber Security*, p. 6.

-targeting not exclusive to a single jurisdiction and are satisfied with relatively insignificant gains per successful action due to the scale of the operation. Using these tactics often ensures little interest from law enforcement as the latter generally have high thresholds before they consider launching an investigation.<sup>20</sup> When an investigation is ultimately launched, problems immediately arise concerning international cooperation mechanisms for accessing evidence in foreign jurisdictions.<sup>21</sup> Acting across jurisdictional borders and the ensuing complexities regarding law enforcement efforts is part of what allows perpetrators to commit computer-related offences with impunity.<sup>22</sup>

### 3. METHODS AND DATA

In order to investigate the prevalence of email-based crime commission in depth, with direct legal relevance, the authors carried out a socio-legal study related to phishing. The phishing emails were received via two email accounts from the sample of the study. The emails were gathered over a 30-day period from mid-August to mid-September in 2018. To study emails received on two accounts, a single email client was used. The second email account provided email data to the email client through forwarding. Employing a single email client, or mail user agent, is justified by considering how an individual interacts with the email ecosystem. Although people use or may use multiple email accounts for different purposes, e.g. personal, work or school, it is common to collect the influx of messages and subsequently view them using a single email client<sup>23</sup> or a single device<sup>24</sup>. This allows to view the client, or device, as the “end-of-route” collection point to which a person receives most, if not all, messages sent to them via email. Hence, the chosen method of data collection

---

<sup>20</sup> Button, M. et al. (2014), op. cit., p. 400.

<sup>21</sup> Osula, A.-M. (2015) Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data. *Masaryk University Journal of Law and Technology*, 9 (1), pp. 43–64.

<sup>22</sup> Cromwell, C. R., Narvaez, D. and Gomberg, A. (2005) Moral Psychology and Information Ethics: The Effects of Psychological Distance on the Components of Moral Behavior in a Digital World. In: Lee Freeman and A. Graham Peace (eds.). *Information ethics: Privacy and intellectual property*. Hershey, PA: Idea Group, pp. 19–37.

<sup>23</sup> Email client market shares suggest *Apple iPhone, Gmail* and *Outlook* to be the most popular mobile, webmail and desktop email clients as of October 2018 (see Litmus Email Analytics. (2018) *Email Client Market Share*. Available from: <http://emailclientmarketshare.com/> [Accessed 20 November 2018]).

<sup>24</sup> Mobile devices are the most popular, followed by laptops, tablets and desktop computers. Fluent. (2017) *The Inbox Report 2017: Consumer Perceptions of Email*, p. 4.

represents the activity occurring over a one-month period in the final collection point for an individual who actively uses the email ecosystem. The inbox has also been used as a source of data to supplement the collection of emails for the analysis of specific scam types.<sup>25</sup> However, opting to collect emails over a certain time-period from a fixed source better represents actual events and potential crime commission “as-is” compared to focussing on specific types of emails the collection of which is not subject to a predetermined time-limit or source, e.g. openly accessible archives can be used.<sup>26</sup> The chosen data collection method has a direct impact on the subsequent application of criminal law provisions, as the raw material for any offence considered in the legal analysis was obtained from the fixed “end-of-route” collection point, i.e. legal analysis was performed on messages in fact received, not on the entire spectrum of possible variations and types available from external sources.

The total amount of emails received during the 30-day period was 297. Of these emails, 70 were automatically received in the spam folder of the email client and no emails with indications of phishing were detected in the primary folder. An initial indication of a phishing attempt includes elements such as unknown sender, grammatical errors, subject lines with upper-case letters throughout as well as ambiguous, generic or overtly out of place topics.<sup>27</sup> The indications were assessed for by quickly scanning, or “eye-balling”, the folders. From the 70 emails received in the spam folder, 28 were assessed to be advertisements from known senders and excluded from subsequent analysis. The remaining 42 emails presented clear initial indications of being a phishing attempt. Hence, the final sample (N=42) for subsequent qualitative text analysis was formed of emails with strong initial indications of being a phishing attempt that were collected over a one-month period in the “end-of-route” email client folders. The emails collected in the “end-of-route” client for the current research amounted to 9.9 emails received per day with the total unsolicited email ratio at 23 % and messages with strong initial indications of phishing at 14.1 %.

Qualitative text analysis was used for analysing the final (N=42) email sample. The analysis started with hierarchical coding as suggested

---

<sup>25</sup> Atkins, B. and Huang, W. (2013), op. cit., p. 27.

<sup>26</sup> See MillerSmiles. *Phishing scam archives*. [online] Available from: <http://www.millersmiles.co.uk/archives.php> [Accessed 20 November 2018].

<sup>27</sup> Jakobsson, M. (2007), op. cit., pp. 3–6.

by *Straus and Corbin*.<sup>28</sup> For the coding process, the guiding concept of “influence and impact on the will to act” was derived from a combination of influencing techniques described in extant literature<sup>29</sup> as well as how certain criminal offences against property are analysed in law. For instance, in extortion cases the offender “bends” the victim’s will to act,<sup>30</sup> while in robberies the victim’s will to act is “broken”, i.e. *vis absoluta* is used. Bending a victim’s will to act means applying significant pressure on the target to perform a specific action, which in extortion cases is expressed by the offender’s goal of ultimately receiving some proprietary gain through the use of threats or violence. The proprietary gain of the offender might be in the form of an object, e.g. smartphone or cash, or in the form of a proprietary right, i.e. a transfer of funds from the victim’s bank account to the offender. What differentiates extortion from robberies and bending the victim’s will to act from breaking it completely, is the presence or absence of the need for a victim to also perform some action. It is possible to assert that extortion-type interactions require an active victim, whilst in robbery type interactions the victim would remain largely inactive (see Figure 1).

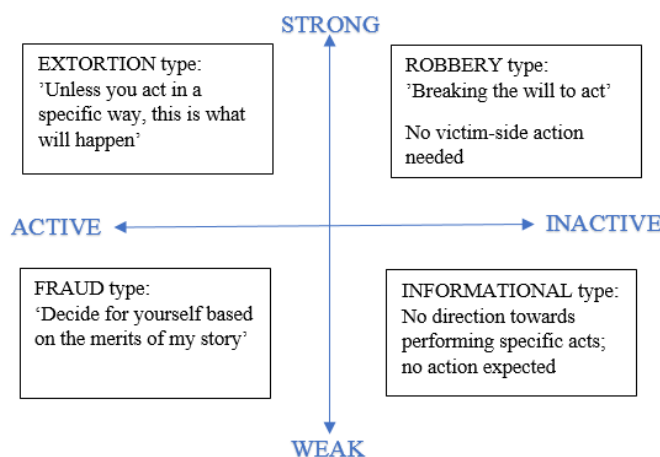


Figure 1: The RIFE (Robbery, Informational, Fraud, Extortion) scale of influence and impact on the will to act

<sup>28</sup> Strauss, A. and Corbin, J. (1998) *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Thousand Oaks, CA: Sage Publications.

<sup>29</sup> Williams, E. J., Beardmore, A. and Joinson, A. N. (2017), op. cit.

<sup>30</sup> Case no. 3-1-1-103-12. (2012) Estonian Supreme Court (Criminal Chamber), 23 November 2012.

However, robbery-type interactions are no longer possible in the email ecosystem,<sup>31</sup> i.e. a person cannot be victimised just by opening an email they have received. In terms of the intensity of impact on the victim's will to act, extortion and robbery type interactions populate the strong impact side of the intensity axis. The other side of the intensity axis, or the weak intensity of impact methods used in influencing a person's will to act, is inhabited by fraud type and purely informational type interactions. In cases of fraud, the victim performs an action freely but based on misconceptions caused by the offender, i.e. due to deception. Purely informational interactions merely convey a message from the sender and thus would not achieve the effects that criminal actors desire, e.g. forwarding sensitive personal information, credit card information, getting the recipient to transfer funds or open file attachments. As the intensity of impact can be considered weak in both fraud and purely informational types, distinguishing between the two derives from the presence or absence of cues directing the recipient to take action in a manner suggested by the sender. In fraud type messages, a bogus storyline is often presented to the recipient with the intention of getting the user to act in a specific way, e.g. visit a website or forward credit card information. Informational type messages do not direct the recipient towards taking specific action. It follows then that informational messages are also void of any guidance on how the recipient should go about performing an action, e.g. providing links to external websites or contact information in the form of email addresses and phone numbers. Therefore, the first order coding used the *RIFE scale* to assess emails received in the client. The initial coding resulted in 3 extortion type phishing emails and 39 fraud type emails. Hence, phishing emails are inherently actionable, i.e. the senders always have the goal of getting the recipient to act in a specific manner regardless of the intensity of impact present in the message or the methods of influence used in the interaction. The *RIFE scale* provides answers to the question "*What, if anything, are the senders trying to get me to do?*". As the second round of coding only concerns actionable phishing emails, it was designed to answer the question "*How are the senders trying to get me to do it?*". In the second round of coding, the extortion and fraud type emails were

---

<sup>31</sup> Hoffman, G. (2016) *Why You Can't Get Infected Just by Opening an Email (Anymore)*. [online] Available from: <https://www.howtogeek.com/135546/htg-explains-why-you-cant-get-infected-just-by-opening-an-email-and-when-you-can/> [Accessed 20 November 2018].

assessed based on four binary categories derived from the final sample of 42 emails (see Table 1).

	A	B
Relationship	Establishing	Assumed
Action	Implicit	Explicit
Influence	Persuasion-type	Threat-type
Dominance	Recipient Controlled	Sender Controlled

Table 1: The RAID (Relationship, Action, Influence, Dominance) categories present in phishing emails

The first category considered sender-recipient relationships, i.e. whether the email assumed an existing relationship between the two or tried to establish one. For example, a previous relationship would be assumed if the senders masquerade as employees of a company the services of which the recipient uses or might have used in the past. In contrast, establishing a relationship would be premised by an apologetic opening, e.g. *"You do not know me, but here is my story"*. The second category concerned whether the reference to the action desired by the recipient was explicit or implicit, e.g. *"pay the amount to this account"* versus *"the funds can only be released after your payment"*. The third category concerned the choice in influencing techniques, i.e. persuasion-influencing or presenting an enticing story based on bogus facts and threat-influencing or evoking the emotions of fear and urgency regarding the potential consequences of non-compliance. The fourth category pertained to the balance of control, or dominance, in sender-recipient interaction. In a sender-dominant communication, the interaction is controlled by the initiator, e.g. in extortion type interactions. In contrast, a recipient-dominant communication leaves it open for the recipient to choose whether to act or respond, e.g. in fraud type interactions. The *RAID (Relationship; Action, Influence, Dominance) model* was developed for a more in-depth analysis of the choices made by the senders in composing their phishing messages.

## 4. FINDINGS

### 4.1. PHISHING EMAILS: TEXT ANALYSIS

With most messages, the sender information displayed in the mandatory email headers (From; Date) did not match the information available from the full email header. For example, an email apparently originating from

*Shauna*, sent from *admin@localuniversity.ee*, in fact, has a return-path, or the address where non-delivery receipts – also called bounce messages – are sent, of *admin@alisonparkerg.com*. This instance is made problematic for email recipients who are less informed about the technological underpinnings of the email ecosystem. Judging by the mandatory email headers displayed, the message seems to originate from *Shauna* and the local university. However, without looking at the full email header, the rest of the information remains hidden to the recipient. The malicious practice of sending communication from an unknown source disguised as a source known to the sender is called “spoofing” and email spoofing is one of the most common versions of it. Central to the issue here is whether an end-user possesses the know-how to scrutinise the available information further or obtain additional information. *Shauna* working for the administration of an international university is certainly possible. Due to the name, however, local users’ attention is likely to become activated based on the discrepancy between what is observed and what is expected.<sup>32</sup> In other instances, the claimed sender and the email address were visibly mismatched. For example, different senders claimed to be from the U.S. Department of Homeland Security, the U.S. Federal Reserve Bank as well as from JPMorgan Chase Bank, but all messages were sent via mail-servers in Japan with reply-to addresses registered in *Gmail*. Within the context of processing an email, sender information spoofing is usually the first attempt at social engineering. The above examples used the perceived authority of the sender to elicit compliance from the recipient.<sup>33</sup> Additionally, senders tried to establish legitimacy by describing their reputable business (“EVANS THOMAS LAW FIRM SOLICITORS & ADVOCATES”) or position (“I’m Mohamed Usman, a delegate from the united nation office”).

In an email message, greetings can be considered a separate group of recipient activators. Common openings can range from generic (“Hi”) to out-of-place ones (“Dearly Beloved,”) but also include overtly shrill examples like “GOOD DAY LUCKY ONES, DEAR EMAIL OWNER”. When no suspicions arose regarding sender information, then generic greetings

---

<sup>32</sup> Grazioli, S. (2004) Where Did They Go Wrong? An Analysis of the Failure of Knowledgeable Internet Consumers to Detect Deception over the Internet. *Group Decision and Negotiation*, 13, pp. 149–172.

<sup>33</sup> Office of Fair Trading. (2009) *The Psychology of Scams: Provoking and Committing Errors of Judgement*.



direct the recipient to continue on to the body of the message. Conversely, markedly out-of-place or overemphasised openings seem counterproductive to the sender's intentions as it draws all attention to the discrepancy in the greeting, even if nothing about sender information was particularly alarming. The major difference between less sophisticated *phishing* emails and *spear phishing* emails seems to be based on the understanding that everything up to the body of the email is about maintaining neutrality about the legitimacy of the message, not actively establishing it. This notion was abided by in the *Shauna* example, as the email had no alarming qualities in the sender information, skipped the opening entirely and started with the text body. Legitimate "cold emails", or emails sent without prior contact between the sender and recipient, are a common occurrence in business environments.<sup>34</sup> For this reason, it's not always possible for people to outright disregard emails they were not expecting to receive, unless they are put off by a non-sensical subject line or a shrill greeting.

An additional category of openings, which at times also simultaneously feature on the email's subject line, are the senders who explicitly require attention from the recipients ("*ATTENTION CARD HOLDER*"; "*Attention Dear Esteemed Beneficiary*"; "*Attention my old friend*"). However, expressions of influencing techniques do not necessarily have to be explicit in the messages to still be effective. In well-timed *spear phishing*<sup>35</sup> emails used in *Business Email Compromise (BEC)* scams – sometimes also called *whale phishing* because of the high-value target – perpetrators collect more background information about the person they will be impersonating as well as the one to be victimised prior to submitting the email. A message with spoofed sender information, legitimacy derived from the employment relationship between the perceived sender and recipient, an excuse for spelling mistakes in the form of "*sent from a mobile device*" as well as stating that they cannot be currently reached are all a build-up to the persuasion. Requiring the recipient to make a wire transfer the same day and given that such emails are often sent an hour or less before the close of business, creates a sense of urgency from context. The choices left to the recipient are

---

<sup>34</sup> Krause, M. and Kulkarni, A. (2015) Predicting Sales E-Mail Responders Using a Natural Language Model. In: *Conference on Human Computation & Crowdsourcing 2015*, San Diego, USA.

<sup>35</sup> A more advanced form of phishing emails that can be highly sophisticated, targeted and personalised.

to either go against the direct instructions of their superior or, using pre-existing knowledge about BEC scams, still try and verify the transaction through channels other than the one used to send instructions.

Based on the body text of the emails in the sample, two distinct ways of eliciting compliance from the recipients can be brought out: persuasions and threats. There were three instances of threatening emails that followed an almost identical *modus operandi*, so these will be analysed collectively based on one example. The message started with priming the recipient with a suggestion to prepare oneself and establishing relevancy without a greeting (*"Take a deep breath and read very carefully do not ignore this e-mail !!"*). The next line of the email was a failed attempt at legitimising the subsequent threat by exhibiting that the sender knows something about the sender (*"It appears that, (), is your password. Will possibly not know me and you are probably wondering why you are getting this e-mail, right?"*). The closed brackets in the message are a placeholder for a password related to the email address or account that the message was received on. In preparation for sending these emails, the perpetrators often scrape online resources to find data dumps or published lists of accounts and respective passwords for the purposes of adding perceived legitimacy to their threats.<sup>36</sup> After presenting what was intended to be a real password for an account, the email continued to describe specific ways the sender had gained access to the recipient's personal device that leads to:

*"my computer software obtained all your contacts from the Messenger, Microsoft outlook, FB, in addition to emails it created a backdoor so i accessed and downloaded all of the data which includes all videos, photographs and records in it".*

Instructions are then provided to the recipient on how to avoid the ensuing embarrassment by paying the sender in *Bitcoin* cryptocurrency:

*"Important: You have 1 day to make the payment. (I have a completely unique pixel within this e mail, and at this moment I am aware that you've read through this email message). If I do not get the BitCoins, I will certainly send your video recording to all of your contacts including relatives, co-workers, and so forth".*

<sup>36</sup> Jaeger, D. et al. (2016) Analysis of Publicly Leaked Credentials and the Long Story of Password (Re-)use. In: *11th International Conference on Passwords (PASS-WORDS2016)*, Germany: Springer.

The email concludes by attempting to evoke a feeling of helplessness in the recipient by stating:

*"It is a non-negotiable offer, that being said don't waste my personal time and yours by responding to this message".*

The same scenario with slight differences in wording was played out in three separate emails. Aside from trying to coerce the target into following specific payment instructions, there was an evident attempt on the part of the sender to confuse the recipient by adding as many technical terms to their activity description as possible. For example, the sender included both an abbreviation of a term and its explanation in the message:

*"During the time you were watching videos, your internet browser began operating as a RDP (Remote Access) which gave me accessibility of your computer screen".*

Thus, the *modus operandi* in these three cases was first to assert legitimacy by trying to display a real password and confuse the recipient with an overload of technical terms. This was followed by evoking a feeling of fear and embarrassment in the user by claiming to possess images and videos of a sensitive nature. The email was concluded by presenting a demand and threatening the recipient.

In contrast to the threatening emails, most of the messages in the sample employed persuasive tactics to get the recipient to follow instructions. The main actions suggested to the user were to forward their personal information so that a large payment could be released to them, or alternatively to pay a small amount of money to obtain access to outrageous riches. To establish rapport with the recipient, a common opening was detailed regarding the sender's person and described the hard times they had fallen on:

*"I am Mrs. Iris J. Stobbs from Sao Tome and Principe, I was married to late Mr. Patrick Stobbs the CEO of PATCAT Oil Mining & Exploration, I am 58 years old, I am suffering from a long time cancer of the breast which has affected my talking & hearing lately".*

By referring to the impaired speaking and hearing abilities, the sender is trying to persuade the user that the received email was perhaps the only viable way for them to establish contact. The story continues to describe the sender and their late husband as “true Christians” who unfortunately were not able to have a child, which is why the sender

*“sold all my inherited belongings and deposited all the sum of USD10,300,000.00 with a Bank”.*

Claiming a religious affiliation is intended to provide a motivational basis for what the sender would like to see happen to the money once the recipient has received it:

*“It is my last wish to see that this money is invested in any Charitable Organization of your choice and distributed each year among the Charity organizations and Orphanages, so I want a good humanitarian to use this money to fund Churches, Needy and Widows in São Tomé and Príncipe or in your Country but preferably in São Tomé and Príncipe”.*

The message concludes with the sender reasserting previous claims about her failing health and expects a reply to an email address that does not match the sender’s. The reply would be considered an indication that the recipient is willing to carry out the sender’s final wish. In a final attempt to describe her conditions, the sender adds:

*“As soon as I receive your reply I shall use the little money I have for my drugs and Medi-care to procure and issue you a letter of authority which will prove that you are the new beneficiary of my funds and I shall release the contact of the Bank to you”.*

Thus, if the recipient is willing, they would ultimately receive an outrageous sum of money while the sender languishes with next to nothing. Should the recipient then engage in communication with the sender, it’s likely that somewhere along the way the poor sender would need some financial assistance in releasing the funds. Other variants of the final request included a specific list of personal information required from the recipient upfront, or the request for a small sum of money was indeed already included in the initial email.

#### 4.2. PHISHING EMAILS: LEGAL ANALYSIS

Considering the results presented in the previous section, the following offences will be discussed in the legal analysis: attempt to commit fraud (§ 209 I, § 25 II), extortion (§ 214) as criminal offences under the Estonian Penal Code<sup>37</sup> (hereinafter PC), as well as the violation of personal data processing requirements, which constitutes a misdemeanour under § 42 I of the Personal Data Protection Act<sup>38</sup> (hereinafter PDPA). As provided for in § 209 I of the PC, the *corpus delicti* of general fraud is

*“the causing of proprietary damage to another person by knowingly causing a misconception of the existing facts”*

and the perpetrator must act with the aim of gaining proprietary benefit himself or herself. Causing a misconception or deceiving the potential victim is a necessary element for an offence to be considered under § 209 I. Fraud is a consequence-offence, i.e. the commission of fraud has not fully concluded unless proprietary damage has occurred to the victim. In the sample emails, the senders claimed that

*“You have \$5000 waiting for you at MONEY GRAM now to pick it”*

and followed it by:

*“but before you can pick up the \$5000 you have to pay sum of \$27 for ACTIVATION”.*

The misconception of the existing facts, in this case, would be the fraudulent claim that a fairly large sum of money is waiting for the recipient in a payment system. Yet, to gain access to this money, the recipients would have to pay something first themselves – a sum of USD27 that is small relative to the promised gain. The likelihood of ever receiving the promised sum after payment is non-existent. Therefore, the senders are acting with the aim of gaining proprietary benefit and have also engaged in deceiving or trying to deceive the recipient. Fraud under § 209 I must be an intentional act according to § 15 I of the PC, it cannot be

<sup>37</sup> *Penal Code (Karistusseadustik)* 2001. SI 2001/61, 364. Estonia: Riigi Teataja (State Gazette). In Estonian. English translation available from: <https://www.riigiteataja.ee/en/eli/509072018004/consolide> [Accessed 19 November 2018].

<sup>38</sup> *Personal Data Protection Act (Isikuandmete kaitse seadus)* 2007. SI 2007/24, 127. Estonia: Riigi Teataja (State Gazette). In Estonian. English translation available from: <https://www.riigiteataja.ee/en/eli/507032016001/consolide> [Accessed 19 November 2018].

committed with negligence. In the current case, it would be difficult to claim that the senders submitted the email by being negligent in wording their message or choosing the recipient. Since the recipient never engaged the senders and, more importantly, did not pay the small activation sum, no proprietary damage has occurred. In other words, the necessary consequence has not occurred, and the senders of the email have not committed fraud. However, § 25 I of the PC also establishes the definition of an attempt, which is an intentional act the purpose for which is to commit an offence. We established the intent in the email but were unable to consider the commission of fraud as completed. § 25 II of the PC states that an attempt is deemed to have commenced at the moment when the person, according to the person's understanding of the act, directly commences the commission of an offence. In the example, the senders had submitted the email as-is but had gained no benefit, because the recipient did not fall for the deception. It is characteristic of an attempt to involve all the subjective injustice of an offence but have certain shortcomings in the objective elements,<sup>39</sup> which in the chosen example was both the lack of proprietary benefit gained by the senders and proprietary damage inflicted on the recipient. Based on the facts, the senders might be accountable for an attempt to commit fraud according to § 209 I, § 25 II of the PC.

However, the majority of persuasive emails did not prompt the recipient to pay a certain sum but instead crafted a fraudulent story to obtain personal information. In the following example, the preceding story was similar to the one described previously:

*"We have deposited the check of your fund (\$4.500,000 Million USD) through MONEY",*

which was followed by asking the recipient to forward their name, country, phone number and address to the senders. Alternatively, the recipient could also call the number provided in the email. Since the basis for the collection of personal data from the recipients in the example is fraudulent, the senders might be accountable for the misdemeanour offence of violating other requirements for the processing of personal data under § 42 I of the PDPA. The other requirements that are violated in the cases

---

<sup>39</sup> Sootak, J. (2010) *Karistusõigus. Üldosa*. Tallinn: Juura, p. 474.

of fraudulent emails come mainly from the first and second sentences of § 12 I of the PDPA. Namely, the subject whose personal data would be processed must provide, of their free will, consent for any processing activities. Furthermore, the processor of personal data must also clearly state the purpose for which the subject's personal data is collected. In the example email, the purpose for collecting personal data from the recipient is connected to the release of outrageous sums of money. The likelihood of that basis being legitimate is of course non-existent. If the recipient decides to release their information to the senders based on the bogus premise, the senders would be accountable for the misdemeanour offence. When recipients are asked for personal information and the perpetrators, in fact, manage to obtain it, the most common subsequent course of action on the part of the perpetrators has been to illegally use the identity of the unsuspecting victim to order goods or sign up for services in their name.

Three phishing emails in the sample constituted the commission of extortion according to § 214 I of the PC. Extortion is defined as the coercion of another person to transfer proprietary benefits by the use of threat to restrict the liberty of the person, disclose embarrassing information or destroy or damage property, or by use of violence. The sender threatened to disclose embarrassing videos and pictures of the recipient, unless the recipient paid USD1,200 in Bitcoin cryptocurrency within one day of having received the email. Extortion as a criminal offence has a truncated body of constituent elements, meaning that the criminal act need not, in fact, be entirely completed to hold a person accountable for its commission.<sup>40</sup> Put differently, the necessary elements of extortion were fulfilled once the sender levied the threat accompanied by a demand for proprietary value. Whether the sender ever receives the *Bitcoins* or any other proprietary benefit in relation to the specific case, is irrelevant for prosecution. Similarly, whether the sender of the email really possessed any embarrassing videos or images of the recipient bears no relevance.

Considering that the emails in the sample were collected over a period of just 30 days on two personal email accounts, the total of 3 cases of extortion, 29 attempts to commit fraud as well as ten attempts to obtain

---

<sup>40</sup> Sootak, J. (2010), *op. cit.*, p. 235.

personal information from the recipient is extensive. By comparison, there were only 74 registered cases of extortion nation-wide according to the Estonian crime statistics for 2017.<sup>41</sup> The way modern electronic communications have enabled the convergence of perpetrators and potential victims has created a startling ballooning of the number of offences committed in the course of daily life. The ease with which crimes can be committed by sending a specifically crafted email raises the age-old issue regarding the trustworthiness of registered crime statistics as the reflection of social reality. From an international perspective, when cybercrimes were first included into the crime statistics published by the *Office for National Statistics* for England and Wales in 2016, the numbers nearly doubled compared to the previous year.<sup>42</sup> The experimental statistics on fraud and computer misuse offences have mostly retained their rates since, with some decrease in the commission of computer misuse offences.<sup>43</sup> Derived from the results of the current analysis, a similar spike in crime reporting would take place in Estonia. In terms of their *modus operandi*, criminal offences are no longer in the process of moving from the physical to the digital but have already found a very comfortable home. Yet, these offences are still poorly reported by people and thus also in national statistics, which ultimately results in the obfuscation and to an extent even the downplaying of the ongoing situation. Anti-crime efforts in this specific area must turn the focus to providing people with the necessary know-how of detecting and reporting instances of email-based commission of offences. Traditional law enforcement efforts are severely hindered when it comes to cybercrime due to the speed with which these offences are committed, i.e. it only takes an email and its submission to fulfil the necessary elements of the offences analysed in the sample. With no reasonable way of interjecting traditional protective measures between the offender and victim, the latter need better tools and knowledge to protect themselves – these can be facilitated

---

<sup>41</sup> Ministry of Justice. (2017) *Kuritegevus Eestis 2017*, p.146. In Estonian. Available from: [http://www.kriminaalpoliitika.ee/sites/krimipoliitika/files/elfinder/dokumendid/kuritegevu\\_seestis\\_2017\\_veebi01.pdf](http://www.kriminaalpoliitika.ee/sites/krimipoliitika/files/elfinder/dokumendid/kuritegevu_seestis_2017_veebi01.pdf) [Accessed 5 November 2018].

<sup>42</sup> Office for National Statistics. (2017) *Crime in England and Wales: Year Ending in Dec 2016*. Available from: <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdec2016> [Accessed 5 November 2018].

<sup>43</sup> Office for National Statistics. (2018) *Crime in England and Wales: Year Ending in March 2018*. Available from: <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2018> [Accessed 5 November 2018].



in the form of systematic public campaigns and educational undertakings, e.g. massive open online courses (MOOCs).

## 5. CONCLUSION

This article discussed the current prevalence of email-based commission of crimes and how these offences remain largely hidden, both from the victims and thus also from national statistics. To illustrate the situation, qualitative text analysis was performed on emails (N=42) received from two email accounts as collected in a single “end-of-route” email client. The results of the criminal law analysis showed that over the course of only one month there were 3 cases of extortion, 29 attempts of fraud and 10 personal data processing related misdemeanour offences committed. Contrary to officially available national statistics, the analysis in the current article clearly showed that the real situation in cybercrime commission is much more severe and in need of immediate attention by criminal policy decision-makers. Traditional law enforcement efforts have largely failed due to the speed of crime commission in online environments. The difference between having to bear the negative consequences of email-based extortion, fraud and issues concerning personal data and securely using important modern communications environments lies with the potential victims themselves. By analysing the rates of offending as well as providing an in-depth analysis of how criminals craft their messages, the article has practical implications for decision-makers in their future crime prevention efforts. Specifically, as such efforts approach the dissemination of relevant knowledge necessary for preventing victimisation via email.

## LIST OF REFERENCES

- [1] Atkins, B. and Huang, W. (2013) A Study of Social Engineering in Online Frauds. *Open Journal of Social Sciences*, 1 (3).
- [2] Burgoon, J. K. et al. (1994) Interpersonal Deception: Accuracy in Deception Detection. *Communication Monographs*, 61.
- [3] Burgoon, J. K. et al. (2003) Detecting Deception Through Linguistic Analysis. In: Hsinchun Chen et al. (eds.). *Intelligence and Security Informatics*, Springer.
- [4] Button, M. et al. (2014) Online Frauds: Learning from Victims Why They Fall for These Scams. *Australian & New Zealand Journal of Criminology*, 47 (3).

- [5] Case no. 3-1-1-103-12. (2012) Estonian Supreme Court (Criminal Chamber), 23 November 2012.
- [6] Cromwell, C. R., Narvaez, D. and Gomberg, A. (2005) Moral Psychology and Information Ethics: The Effects of Psychological Distance on the Components of Moral Behavior in a Digital World. In: Lee Freeman and A. Graham Peace (eds.). *Information Ethics: Privacy and Intellectual Property*, Hershey, PA: IdeaGroup.
- [7] European Commission. (2017) *Special Eurobarometer 464a: Europeans' Attitudes Towards Cyber Security*.
- [8] Fluent. (2017) *The Inbox Report 2017: Consumer Perceptions of Email*.
- [9] Grazioli, S. (2004) Where Did They Go Wrong? An Analysis of the Failure of Knowledgeable Internet Consumers to Detect Deception over the Internet. *Group Decision and Negotiation*, 13.
- [10] Hutchings, A. and Hayes, H. (2009) Routine Activity Theory and Phishing Victimization: Who Gets Caught in the 'Net'?. *Current Issues in Criminal Justice*, 20 (3).
- [11] Jakobsson, M. (2007) The Human Factor in Phishing. *Privacy & Security of Consumer Information*.
- [12] Jaeger, D. et al. (2016) Analysis of Publicly Leaked Credentials and the Long Story of Password (Re-)use. In: *11th International Conference on Passwords (PASS-WORDS2016)*. Germany: Springer.
- [13] Krause, M. and Kulkarni, A. (2015) Predicting Sales E-Mail Responders Using a Natural Language Model. In: *Conference on Human Computation & Crowdsourcing 2015*, San Diego, USA.
- [14] Langenderfer, J. and Shimp, T. A. (2001) Consumer Vulnerability to Scams, Swindles, and Fraud: A New Theory of Visceral Influences on Persuasion. *Psychology and Marketing*, 18.
- [15] Litmus Email Analytics. (2018) *Email Client Market Share*. Available from: <http://emailclientmarketshare.com/> [Accessed 20 November 2018].
- [16] MillerSmiles. *Phishing scam archives*. [online] Available from: <http://www.millersmiles.co.uk/archives.php> [Accessed 20 November 2018].
- [17] Ministry of Justice. (2017) *Kuritegevus Eestis 2017*. In Estonian. Available from: [http://www.kriminaalpoliitika.ee/sites/krimipoliitika/files/elfinder/dokumendid/kuritegevuseestis\\_2017\\_veebi01.pdf](http://www.kriminaalpoliitika.ee/sites/krimipoliitika/files/elfinder/dokumendid/kuritegevuseestis_2017_veebi01.pdf) [Accessed 5 November 2018].
- [18] Office for National Statistics. (2017) *Crime in England and Wales: Year Ending in Dec 2016*. Available from: <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeand>

- justice/bulletins/crimeinenglandandwales/yearendingdec2016 [Accessed 5 November 2018].
- [19] Office for National Statistics. (2018) *Crime in England and Wales: Year Ending in March 2018*. Available from: <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2018> [Accessed 5 November 2018].
- [20] Office of Fair Trading. (2009) *The Psychology of Scams: Provoking and Committing Errors of Judgement*.
- [21] Osula, A.-M. (2015) Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data. *Masaryk University Journal of Law and Technology*, 9 (1).
- [22] *Penal Code (Karistusseadustik) 2001*. SI 2001/61, 364. Estonia: Riigi Teataja (State Gazette). In Estonian. English translation available from: <https://www.riigiteataja.ee/en/eli/509072018004/consolide> [Accessed 19 November 2018].
- [23] *Personal Data Protection Act (Isikuandmete kaitse seadus) 2007*. SI 2007/24, 127. Estonia: Riigi Teataja (State Gazette). In Estonian. English translation available from: <https://www.riigiteataja.ee/en/eli/507032016001/consolide> [Accessed 19 November 2018].
- [24] 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. (2017/0226) 13 September. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:0489:FIN> [Accessed 20 November 2018].
- [25] Radicati Group. (2018) *Executive Summary*. Available from: <https://www.radicati.com/wp/wp-content/uploads/2018/05/Email-Market-2018-2022-Executive-Summary.pdf> [Accessed 20 November 2018].
- [26] Rajivan, P. and Gonzalez, C. (2018) Creative Persuasion: A Study on Adversarial Behaviors and Strategies in Phishing Attacks. *Frontiers in Psychology*, 135 (9).
- [27] Reyns, B. W. (2015) A Routine Activity Perspective on Online Victimization: Results from the Canadian General Social Survey. *Journal of Financial Crime*, 42 (4).
- [28] Sootak, J. (2010) *Karistusõigus. Üldosa*. Tallinn: Juura.
- [29] Strauss, A. and Corbin, J. (1998) *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Thousand Oaks, CA: Sage Publications.
- [30] Symantec. (2018) *Internet Security Threat Report*. Available from: <https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf> [Accessed 20 November 2018].

- [31] United Nations Office on Drugs and Crime. (2013) *Draft Comprehensive Study on Cybercrime*. Available from: [https://www.unodc.org/documents/organized-crime/UNODC\\_CCPCJ\\_EG.4\\_2013/CYBERCRIME\\_STUDY\\_210213.pdf](https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf) [Accessed 20 November 2018].
- [32] Verizon. (2017) *Data Breach Investigations Report, 10th Ed.*
- [33] Vishwanath, A. et al. (2011) Why Do People Get Phished? Testing Individual Differences in Phishing Vulnerability within an Integrated, Information Processing Model. *Decision Support Systems*, 51 (3).
- [34] Williams, E. J., Beardmore, A. and Joinson, A. N. (2017) Individual Differences in Susceptibility to Online Influence: A Theoretical Review. *Computers in Human Behavior*, 72.
- [35] Williams, E. J., Hinds, J. and Joinson, A. N. (2018) Exploring Susceptibility to Phishing in the Workplace. *International Journal of Human-Computer Studies*.
- [36] Workman, M. (2008) Wisecrackers: A Theory-grounded Investigation of Phishing and Pretext Social Engineering Threats to Information Security. *Journal of the American Society for Information Science and Technology*, 59 (4).

DOI 10.5817/MUJLT2019-1-4

## THE TALLINN MANUALS AND THE MAKING OF THE INTERNATIONAL LAW ON CYBER OPERATIONS\*

*by*

PAPAWADEE TANODOMDEJ\*\*

*The Tallinn Manuals (the Manuals) attempted to clarify how to apply existing international law to cyber operations. Though the Manuals are non-binding instruments, the Group of International Experts claimed that they reflected the *lex lata* applicable to cyber operations. However, this claim is questionable due to the dominating role of a few Western states in the drafting process and the linked neglect of the practice of “affected states” in cyber operations. This article examines the quality of the Manuals’ drafting process and the composition and impartiality of the experts involved. It focuses on the issue of the prohibition of the use of force. The aim of this examination is not to discuss whether the Manuals provided the right answer to the question of how international law applies to cyber operations. Rather, they function as a case study of how legal scholarship may affect the making of international law. The article concludes that certain rules in the Manuals are marked by NATO influence and overlook the practice of other states engaged in cyber operations. Therefore, the Manuals disregard the generality of state practice, which should be the decisive factor in the formation of customary international law. As far as “political activism” may be involved, the article argues that the role of legal scholars as assistants to the cognition of international law could be compromised.*

---

\* The author would like to thank the reviewers and the members of *Masaryk University Journal of Law and Technology* for their helpful comments and help preparing this article for publication. In addition, the author would like to thank to Professor Kinji Akashi for always inspiring and constant support and Dr. Lasse Schuldt for incessant encouragement.

\*\* papawadee.tanodomdej@gmail.com, LL.D. student, Kyushu University, Japan; lecturer at Chulalongkorn University, Law Faculty, Bangkok, Thailand.

## KEY WORDS

*Cyber Attack, Cyber Operation, International Law-making, Legal Scholarship, Tallinn Manual*

## 1. INTRODUCTION

*“In the 21st Century, bits and bytes can be as threatening as bullets and bombs.”<sup>1</sup>*

The statement made by a former US Deputy Secretary of Defense holds true, since the Internet has extended its role from a means of communication to an enabling technology facilitating almost every aspect of human activities. Not only actors in the private sector rely on information technology, but also government agencies and entities managing critical infrastructures utilize cyber technology to discharge their functions. The fact that states increasingly attach their core functions to the interconnectivity of cyberspace exposes them to this new paradigm of threats. For instance, the DDoS attack on Estonia in 2007 disabled the websites of all ministries, two major banks, several political parties and the parliamentary email server, the credit cards and automatic teller machines (ATMs) leading to the whole nation being halted.<sup>2</sup>

The international community is aware of the rise of cyber threats and attempts to extend the existing international law to regulate cyber operations. *The United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunication in the Context of International Security* (UN GGE) concluded in its 3rd report in 2013 that international law, in particular the Charter of the United Nations (UN Charter), applies to cyberspace.<sup>3</sup> However, there is no consensus neither from the UN GGE nor the whole international community clarifying how exactly international law is applicable to cyber operations. Against this backdrop, the “Tallinn Manual on the International Law Applicable to Cyber Warfare” and the “Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations” (“Tallinn

<sup>1</sup> Lynn, W. J. (2011) *Remarks on the Department of Defense Cyber Strategy as Delivered by Deputy Secretary of Defense William J. Lynn*. [speech] 14 July. Available from: <http://www.defense.gov/speeches/speech.aspx?speechid=1593> [Accessed 12 July 2018].

<sup>2</sup> Tikk, E. Kaska, K. and Vihul, L. (2010) *International Cyber Incidents: Legal Considerations*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, pp. 18–24.

<sup>3</sup> (2013) *UN Doc A/68/98*. pp. 6, 8.

Manuals”) emerged by the articulation of a group of legal scholars and international lawyers. The Tallinn Manuals are the products of the deliberation of the International Group of Experts invited by the *NATO Cooperative Cyber Defence Center of Excellence (CCDCOE)* on how international law applies to cyber operations, but they are non-binding instruments. The Tallinn Manuals cover both cyber operations in armed conflict and peacetime, while at the same time address the law of state responsibility, sovereignty, human rights, air and aviation law, space law and the law of the sea. The publication of the Manuals has not only attracted the states’ attention but has also lead to an academic discussion on cyber operations because of the group’s rather bold statement that the rules in the Manuals, made through the consensus of the International Group of Experts, reflects the *lex lata* applicable to cyber operations and avoids articulating *lex ferenda*.<sup>4</sup> If this claim were true, the Manuals would articulate the international law applicable to cyber operations with unprecedented clarity. Accordingly, this article aims to scrutinize the legitimacy of the Tallinn Manuals as products of legal scholarship contributing to the international law-making on cyber operations. In doing so, this article consists of two parts. Firstly, attention is paid to the role of legal scholarship in law-making. Secondly, the legitimacy of experts involved in the drafting of the Tallinn Manuals will be examined. Furthermore, the article assesses the quality of the Manuals’ drafting process with regard to the prohibition of the use of force, one of the fundamental principles of the UN Charter since it was the starting point of the debate on the suitability of international law as a normative framework for the regulation of cyber operations. The ultimate goal is not to assess the quality of the Tallinn Manuals, but to demonstrate how legal scholarship can affect the making of international law.

## 2. ROLE OF LEGAL SCHOLARSHIP IN LAW-MAKING

The orthodox doctrine views international law-making in terms of sources.<sup>5</sup> Article 38 of the Statute of the International Court of Justice (ICJ) is the main reference to both the sources of international law and its making. However,

---

<sup>4</sup> *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, p. 19; see also *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, p. 3.

<sup>5</sup> Skouteris, T. (2001) *The Force of a Doctrine: Art. 38 of the PCIJ Statute and the Sources of International Law*. In: Fleur Johns et al. (eds.). *Events: The Force of International Law*. New York: Routledge, pp. 69–80.

due to the plethora of actors using and speaking of international law, it is undeniable that communicative practices assimilate themselves to the process of international law-making.<sup>6</sup> In particular, legal scholars and international lawyers play a significant role by interpreting the existing international law to solve the novel global challenges. The main question is to what extent legal scholarship contributes to international law-making.

In order to give a precise response, it is imperative to discuss the relationship between the sources doctrine and Article 38 (1) (d) of the ICJ Statute before addressing the variety of contemporary international-law making theories recognizing communicative practices.

## 2.1 LEGAL SCHOLARSHIP AND ARTICLE 38 (1) (D)

Article 38 (1) (d) of the ICJ Statute stipulates that judicial decisions and the teachings of the most highly qualified publicists are the subsidiary means for the determination of rules of law. This could be read that legal scholarship is the

*“subsidiary means for the determination of law, not a subsidiary source of law”.*<sup>7</sup>

Legal scholarship may thus present evidence of international law through its analysis of collected state practice reflecting certain international legal norms. However, 19th century legal scholars have often referred also to the works of famous men such as *Grotius*, *Pufendorf*, *Westlake* and *Vattel* to validate their arguments.<sup>8</sup> It remains doubtful to what extent legal scholarship can objectively substantiate international practice as evidence of international law. In the joint separate opinion of Judges *Higgins*, *Kooijmans* and *Buerghenthal* in the *Congo v. Belgium* case, the Judges discussed the question whether a state is entitled to exercise jurisdiction over persons having no connection with the forum state when the accused is not present in that state. Despite the contribution of legal scholarship on the question, the Joint Separate Opinion rejected scholarly writings asserting that

---

<sup>6</sup> Venzke, I. (2013) Contemporary Theories and International Law-making. In: Brölmann Catherine and Radi Yannick (eds.). *Research Handbook on the Theory and Practice of International Lawmaking*. Cheltenham: Edward Elgar, pp. 66–73.

<sup>7</sup> Kammerhofer, J. (2013) Lawmaking by Scholars. In: Brölmann Catherine and Radi Yannick (eds.). *Research Handbook on the Theory and Practice of International Lawmaking*. Cheltenham: Edward Elgar, p. 306.

<sup>8</sup> Parry, C. (1965) *The Sources and Evidence of International Law*. Manchester: Manchester University Press, p. 103.



the treaties on crimes and offences are evidence of universality as a ground for the exercise of jurisdiction recognized in international law.<sup>9</sup> The Opinion noted that

*“[t]he assertion [from the writings of eminent jurists] that certain treaties and court decisions rely on universal jurisdiction, which in fact they do not, does not evidence an international practice recognised as custom. And the policy arguments advanced in some of the writings can certainly suggest why a practice or a court decision should be regarded as desirable, or indeed lawful; but contrary arguments are advanced too, and in any event, these also cannot serve to substantiate an international practice where virtually none exists.”*<sup>10</sup>

Although certain scholar writings have been rejected by the ICJ, this does not mean that the role of legal scholars as assistants to the cognition of international is ignored. In the Advisory opinion on *the Construction of a Wall*, the ICJ made reference to and agreed with the views of the editor of *Oppenheim’s* international law.<sup>11</sup>

Accordingly, the ICJ holds full discretion to grasp the legal scholarship which it holds to reflect the applicable international law. Moreover, Article 38 (2) of the Statute of the ICJ allows the ICJ to decide the dispute, if the parties agree, on the ground of any norms not contained in Article 38 (1). It appears therefore that the ICJ is endowed with the power to appreciate any evidence that manifests rules of international law, not limited to legal scholarship or judicial decisions. Against this backdrop, legal scholarship does not have any particular intrinsic epistemic power and could, at best, be deemed as “evidence of the law”.<sup>12</sup>

## 2.2 COMMUNICATIVE PRACTICE

While the normative-positivist considers legal scholarship as mere evidence of the law, many contemporary theories on international law-making take

<sup>9</sup> *Case Concerning the Arrest Warrant of 11 April 2000 (Democratic Republic of Congo v. Belgium)*. The Joint Separate Opinion of Judge Higgins, Kooijmans and Buergenthal, Judgement of 14 February 2002. ICJ Reports 2002. para. 26.

<sup>10</sup> *Op. cit.*, para. 44.

<sup>11</sup> *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*. Advisory Opinion of 9 July 2004, para. 57.

<sup>12</sup> Kammerhofer, J. (2013) *op. cit.*, p. 308; see also Triggs, G. (2005) *The Public International Lawyer and the Practice of International Law. Australian Yearbook of International Law*, 24, pp. 202–205.

into account the potential of the use of international law language contributing to its making.<sup>13</sup> This can be seen, for example, in the debates over the meaning of “force” pursuant to, but undefined by, Article 2 (4) of the UN Charter. Also, the authoritative meanings of “combatant” and “civilian” are derived from the practice of interpreting these terms. International law, in the eyes of contemporary theories, is not only made through the conclusion of treaties but also by way of a communicative process of speaking and using international law by the various actors, which are not only states. Therefore, contemporary theories take into account the multiplicity of actors contributing to international law-making by participating in the interpretative process.

First, the *New Haven School*, including *Michael Reisman*, argues that international law emerges from a communicative process among a multiplicity of actors.<sup>14</sup> In particular, aspects of humanitarian concern have been discussed by a wide range of actors in the international political discourse. Even though humanitarianism is construed as social fact, it can be weighed as a point of reference for legal arguments or normative judgments.

The System Theory supports the communicative process as law-making but distinguishes itself from the *New Haven School* in that it holds that interpretation in international law cannot be diminished to the pursuit of values. *Niklas Luhmann* elaborates *Gunther Teubner's* proposition of “Autopoiesis” to describe the self-reproduction of international law whose communication is presented as referring to its own same system.<sup>15</sup> The validation of the legal claims relies upon legal claims.<sup>16</sup> Against this background, *Teubner* argues that

*“global law will grow mainly from the social peripheries, not from the political centres of nation-states and international institutions”*

and the non-state actors are increasingly important in societal law-making.<sup>17</sup>

---

<sup>13</sup> Venzke, I. (2013), op. cit., p. 66.

<sup>14</sup> Reisman, M. (1981) International Lawmaking: A Process of Communication. *American Society of International Law Proceedings*, 75, pp. 101–120.

<sup>15</sup> Luhmann, N. (1993) *Das Recht der Gesellschaft*. Frankfurt: Suhrkamp, p. 98.

<sup>16</sup> Ibid.

<sup>17</sup> Teubner, G. (1997) Global Bukowina: Legal Pluralism in the World Society. In: *Global Law Without a State*. Hants: Dartmouth, pp. 3–28.

The Governance Theory also acknowledges the rise of non-state actors in law-making.<sup>18</sup> However, according to *Slaughter*, the engagements among domestic regulators, the private sector, technicians and academia resulting in the informal international law-making raises the question of accountability. Since

*“the essence of a network is a process rather than an entity, it cannot be captured or controlled in the ways that typically structure formal legitimacy in a democratic polity.”*<sup>19</sup>

The Global Administrative Law (GAL) theory criticizes that, although the sources doctrine ties international law to the consent of states claiming the legitimate order, it does not capture “everything that matters”.<sup>20</sup> The GAL theory has been established to respond to the accountability deficiency in the international law-making process by introducing general principles of administrative law such as transparency, procedural participation and review. Under the view of GAL, making international law through interpretation is deemed as an exercise of public authority, provided that the interpreters

*“have the capacity to establish their own statements about the law as reference points for legal discourse”*

that others could only escape at a cost.<sup>21</sup>

All in all, contemporary theories consider communicative practices, such as interpretation, as part of international law-making. However, legal arguments claiming to establish legal rules may disguise underlying political agendas. This subjectivity could indeed undermine the legitimacy of the communicative law-making process.

<sup>18</sup> Pauwelyn, J. (2012) Informal International Lawmaking: Framing the Concept and Research Questions. In: Joost Pauwelyn, Ramses Wessel and Jan Wouters (eds.). *Informal International Lawmaking*. Oxford: Oxford University Press, pp. 15–20.

<sup>19</sup> Slaughter, A.-M. (2000) Agencies on the Loose? Holding Government Networks Accountable. In: George Bermann and Peter Lindseth (eds.). *Transatlantic Regulatory Cooperation, Legal Problems and Political Prospects*. Oxford: Oxford University Press, p. 531.

<sup>20</sup> Kingsbury, B. Krisch, N. and Stewart, R. (2005) The Emergence of Global Administrative Law. *Law and Contemporary Problems*, 68, p. 17.

<sup>21</sup> Venzke, I. (2013), op. cit., p. 85.

### 3. THE TALLINN MANUALS AND THE COGNITION OF INTERNATIONAL LAW ON CYBER OPERATIONS

In principle, the Tallinn Manuals written under the International Group of Experts' mandate amount to mere legal scholarship serving as a subsidiary means for identifying the sources of international law on cyber operations. The role of these experts can be approximated to the role of the International Law Commission (ILC) and other independent entities where legal experts are assigned to study and clarify international law.

Michael Schmitt, the Director of the International Group of Experts, states in the introduction of the Manuals that

*"This Manual is meant to be a reflection of law as it existed at the point of the Manual's adoption by the two International Groups of Experts in June 2016. It is not a "best practice" guide, does not represent "progressive development of the law", and is policy and politics-neutral. In other words, Tallinn Manual 2.0 is intended as an objective restatement of the lex lata. Therefore, the Experts involved in both projects assiduously avoided including statement reflecting lex ferenda."*<sup>22</sup>

This statement confirms the self-perception of the International Group of Experts that its task was to not to make law but to articulate the law as it exists. The position of the Group is approximate to the sources doctrine by denying its capacity to make law but accentuating its role as an assistant to the cognition of law. To test the validity of this statement, both the legitimacy of the Group and the use of force rule under the Tallinn Manuals will be discussed.

#### 3.1 LEGITIMACY OF THE INTERNATIONAL GROUP OF EXPERTS

The Group's legitimacy can be discussed from the perspectives of the sources doctrine as well as contemporary theories with a view to the predictability and consistency of international legal rules. The question of objectivity of legal scholars' discourse is intertwined with the legitimacy of the legal scholars themselves.<sup>23</sup> Therefore, both

---

<sup>22</sup> The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, pp. 2–3.

<sup>23</sup> Schachter, O. (1977) The Invisible College of International Lawyers. *Northwestern University Law Review*, 72, pp. 219–221.

the composition and the authority of the International Group of Experts will be examined.

The International Group of Experts drafting the first version of the Tallinn Manual was composed of 19 experts ranging from international law academics, practitioners, serving or former military officials and technical experts, as well as four observers from the *International Committee of the Red Cross (ICRC)*, NATO and the US Cyber Command who also actively participated in the deliberation.<sup>24</sup> Experts and observers of the Tallinn Manual project came from a few Western countries. Seven experts (including the Director) came from the US. There were no participants from Russia, China, Iran and Israel, all countries which are reportedly involved in cyber operations.<sup>25</sup> The disparity in the experts' countries of origin was criticized for its geographical bias.<sup>26</sup>

When deliberating the Tallinn Manual 2.0, the Group of Experts tried to overturn this critique by emphasizing the appearance of experts from China, Japan, Israel and Thailand.<sup>27</sup> Though the majority of experts still came from Western countries, all experts claimed to participate in their personal capacity,<sup>28</sup> and that their participation in the drafting process did not reflect their affiliation. It has therefore been argued that the lack of experts or participants from certain countries reportedly engaging in cyber operations may not necessarily undermine the authority of the Manuals.<sup>29</sup>

As regards the legitimacy of the individual experts, their selection was based on two factors:

- (1) an impersonal validity claim; and
- (2) the experience and position of the expert.<sup>30</sup>

---

<sup>24</sup> The International Group of Experts is divided into many functional groups, namely, Editorial Committee, Legal Group Facilitators, Legal Experts, Technical Experts.

<sup>25</sup> See the list of International Group of Experts appeared in the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, pp. 6–9.

<sup>26</sup> Fleck, D. (2013) Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the New Tallinn Manual. *Journal of Conflict and Security Law*, 18, p. 331.

<sup>27</sup> There are Professor Zhixiong Huang from Wuhan University, Professor Kazuhiro Nakatani from University of Tokyo, Deborah Housen-Couriel from University of Haifa, and Kriangsak Kittichaisaree, a Member of the ILC from Thailand.

<sup>28</sup> *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, p. 23; see also *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, p. 2.

<sup>29</sup> Roscini, M. (2014) *Cyber Operations and the Use of Force in International Law*. Oxford: Oxford University Press, p. 32.

<sup>30</sup> Kessler, O. and Werner, W. (2013) Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare. *Leiden Journal of International Law*, 26, p. 802.

Firstly, each expert needed to present himself/herself as independent from his/her personal preference and convince the audience that the knowledge he/she produces is validly objective.<sup>31</sup> Secondly, only persons who hold specific skills, knowledge and experience were supposed to be able to satisfy the public trust in producing knowledge.

These two factors seem ambiguous in the International Group of Experts. Regarding the first factor, despite its strong claim to impersonality, the experts cannot escape the criticism as to the dominant position of Western countries. Commentators have therefore not only pointed to the disparity of countries where the experts came from, but also highlighted the sources of evidence used by the experts to justify the existence of *lex lata*.<sup>32</sup> It has been reported that the rules in the Tallinn Manuals are heavily drawn from the military manuals of four countries (Canada, Germany, the United Kingdom, and the United States) with the underlying claim that

*“the international community generally considers these four manuals to be especially useful during legal research and analysis with respect to conflict issues”*.<sup>33</sup>

The word “useful” may have been used to avoid the impression that the military manuals of four NATO states might have served as direct sources of authority. Against this background, it is problematic that the International Group of Experts audaciously asserted that the Tallinn Manuals, which in effect stand for the opinions of a few Western states, represent the international community as a whole.<sup>34</sup>

As Mégret has asserted, international humanitarian law today is still attached to the Western image of statehood and the corresponding understanding of international law’s nature and function.<sup>35</sup> While most international lawyers support the function of humanitarian law as regulating warfare, the realist or the anti-colonialist might perceive

---

<sup>31</sup> Ibid.

<sup>32</sup> Fleck, D. (2013), op. cit., pp. 331–351; see also Kessler, O. and Werner, W. (2013), op. cit., pp. 793–810.

<sup>33</sup> Fleck, D. (2013), op. cit., p. 335.

<sup>34</sup> Kessler, O. and Werner, W. (2013), op. cit., p. 803.

<sup>35</sup> Mégret, F. (2005) From ‘Savage’ to ‘Unlawful Combatant’: A Postcolonial Look at International Humanitarian Law’s Other. In: Anne Ordord (ed.). *International Law and Its Others*. Cambridge: Cambridge University Press. Available also from: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=918541](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=918541)

the role of the law of armed conflict as a tool to reinforce the “unshakeable grip” of dominant states.<sup>36</sup> However, it would also be unfair to label the Tallinn Manuals as products of neo-colonialism.<sup>37</sup> Nonetheless, the flaws in the drafting process have an inherent potential to undermine their authoritative degree.

The second factor in the selection process was the reputation of the experts. The pertinent element to be examined is the criteria to select the qualified experts to participate in the Tallinn Manuals project. From the start, the Tallinn Manuals were initiated and sponsored by the NATO CCDCOE which confided the task to select the members of the International Group of Experts to the Director, *Michael Schmitt*, Chair of the international law department at the US Naval War College and author of widely quoted articles related to cyber operations.<sup>38</sup> *Schmitt* enjoyed full discretion in composing the group of experts.<sup>39</sup> Neither *Schmitt* nor the Tallinn Manuals explain the selection process. The Tallinn Manuals merely describe the composition with reference to the various personal backgrounds: international law academics, practitioners, serving or former military officials and technical experts. Though there exists no determinative rule under international law how to decide who is a highly qualified publicist or legal expert, the selected experts assume an important status: Their comments were captured in the Tallinn Manuals to which the audience can make a reference. If one compares the role of experts to judges at the International Court of Justice, though they enjoy different competences, one can observe that the Court’s judgments enjoy more credibility and authority as they are made by a representatively composed body, rather than by a “like-thinking” group of experts.<sup>40</sup> Therefore, to firmly reject the critique over the bias of experts, the transparency of the selection process of experts is advisable. Only then can the validity of the claim that the Tallinn Manuals reflect *lex lata* be assessed.

<sup>36</sup> Ibid.

<sup>37</sup> Kessler, O. and Werner, W. (2013), op. cit., p. 803.

<sup>38</sup> *Michael Schmitt* produces many articles related to cyberwarfare, especially during and after being the Director of the Tallinn Manual and the Tallinn Manual 2.0. But the article before involving in the Tallinn project that triggers the debate on the legal aspects of cyberwar appears in Schmitt, M. (1998–1999) Computer Network Attacks: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*, 37, pp. 885–935.

<sup>39</sup> The quote is taken from a presentation by *Michael Schmitt* on the Tallinn Manual CyCon 2012 organized by the NATO CCDCOE (see US Naval War College. (2012) *Cycon 2012 Michael Schmitt: Tallinn Manual Part I*. [online video] Available from: <http://www.youtube.com/watch?v=wY3uEo-Itso> (1:40) [Accessed 20 July 2018].

<sup>40</sup> Schachter, O. (1977), op. cit., p. 222.

### 3.2 IMPOSITION OF THE CONVENTIONAL USE OF FORCE ON CYBER OPERATIONS

In this section, the focus is shifted to the drafting process of the Tallinn Manuals. To decide whether the Tallinn Manuals secure the status as an instrument objectively providing evidence of international law on cyber operations, one must observe how the rules have been established in the Manuals.

Due to the limited space and the large number of rules inscribed in the Tallinn Manuals, it is impossible to analyze the drafting process of each rule. The rules related to the use of force is selected for the analysis because it represents the cornerstone linking the existing international law with the novel threat of cyber operations.

The most vital aspect of the application of the law on the use of force to cyber operations is:

*“under what conditions cyber operations can constitute the use of force prohibited by Article 2 (4) of the UN Charter and customary international law”.*

The International Group of Experts attempts to extend the existing prohibition of the use of force to cover also cyber operations by referring to the ICJ's statement in the *Nicaragua* case that distinguished *“the most grave forms of the use of force from other less grave”*.<sup>41</sup> The Group concludes that, despite the lack of a definition of “use of force”, the difference between use of force and an armed attack relies upon “scale and effect”.<sup>42</sup> Rule 11 of the first version of the Tallinn Manuals and Rule 69 of the Tallinn Manual 2.0 stipulate that

*“a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.”*

According to this assertion, the consequences of cyber operations are a vital factor to distinguish “cyber operations” that qualify as the use of force from those that do not. The Tallinn Manuals also acknowledge

---

<sup>41</sup> *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)*. Judgement of 27 June 1986. ICJ Report 1986, para. 191.

<sup>42</sup> Schmitt, M. (2015) *The Use of Cyber Force and International Law*. In: Marc Weller (ed.), *The Oxford Handbook of the Use of Force in International Law*. Oxford: Oxford University Press, pp. 1111–1114.



the different qualitative level between use of force and an armed attack, whereas only cyber operations reaching the threshold of an armed attack trigger the right to self-defense of the victim state.<sup>43</sup>

However, the adoption of the “scale and effect” threshold leaves much room for interpretation.<sup>44</sup> The Group, therefore, adopted an approach comprising eight factors, to assist states in determining when the international community would likely characterize a cyber operation launched against them, or that they conducted, as a use of force.

- (1) *Severity*. A cyber operation causing death or injury of persons is sufficiently severe to qualify as a use of force, while a psychological operation in cyberspace generating irritation or inconvenience would never qualify as such.
- (2) *Immediacy*. The negative consequences of a cyber operation shall be immediately visible to be qualified as a use of force. Unlike the less visible and delayed consequences, there will be more opportunities to mitigate those consequences or resolve the situation peacefully.
- (3) *Directness*. The causation chain of a cyber operation and its effect shall be examined. The closer the link between a cyber operation as cause and its effect, the more likely that the cyber operation will be characterized as a use of force.
- (4) *Invasiveness*. This refers to the conventional concept of use of force where there exists an intrusion into the target state’s border. A cyber operation will be more invasive if it intrudes into the secured system of the target state without its consent. For example, the attack on domain names belonging to critical public agencies such as .gov, .mil is more invasive than the attack directed at non-state specific domain names such as .com.
- (5) *Measurability of effects*. Typically, the effect of the use of armed force is measurable. However, in cyberspace, the consequences may be less apparent. If the consequences of a cyber operation can be assessed in specific terms such as the percentage of servers disabled and the amount of data corrupted, it is likely to be considered as a use of force.

<sup>43</sup> Rule 69 of *The Tallinn Manual on the International Law Applicable to Cyber Warfare* and Rule 71 of *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.

<sup>44</sup> Schmitt, M. (2015), op. cit., p. 1114.

- (6) *Military character*. A cyber operation that occurs in a military context increases the likelihood to be constituted as a use of force.
- (7) *State involvement*. If there is evidence that a state is involved in the cyber operation, the chance that the cyber operation amounts to a use of force will be higher.
- (8) *Presumptive legality*. Under international law, it is generally accepted that the application of violence is unlawful, unless authorized – such as in self-defence. Psychological operations and economic coercion are not expressly prohibited. Therefore, the cyber operation holding a similar characteristic as economic pressure or psychological operations is less likely to be equated as a use of force.

Although the “scale and effect” approach embraces the material aspect of violence similar to the implicit notion of force in the conventional use of force, the application of the eight-factor rule on cyber operations is not without problems.

Firstly, the eight-factor rule was based in essence on *Michael Schmitt’s* original work written in 1999 in which he gathered these factors based on his observation of what arguments have influenced states in assessing whether or not a use of force has taken place.<sup>45</sup> However, no hard evidence of state practice or *opinio juris* related to the eight-factor rule appears neither in *Schmitt’s* original work nor in the Tallinn Manuals. It appears to be based on the author’s intuition, disguised as an empirical method.

Secondly, certain criteria from the eight-factor rule allow certain kinds of cyber operations to escape legal regulation as the characteristics of cyber operations are not fully captured. For instance, the “invasiveness” criterion is not compatible with DDoS Attacks, where the targeted computer system or network is not penetrated, but thousands of requests flood the target system to paralyze its function. The “measurability of effects” of cyber operations is notoriously arduous since the effect-based approach does not clarify which standards of proof is valid. There are various standards of proof to choose from: “beyond any doubt”<sup>46</sup>, “convincing evidence”<sup>47</sup>, “*prima facie* evidence”<sup>48</sup>, and “sufficiently convincing”<sup>49</sup> evidence. *D’Aspremont* points out that, due to such a wide choice, the International

---

<sup>45</sup> For further detail of the eight-factor background see Schmitt, M. (1998–1999), op. cit., p. 921.

Group of Experts may be tempted to maximize the efficacy of evidencing, for instance by lowering the standard of proof.<sup>50</sup> As to “presumptive legality”, the logic on what is not prohibited is permitted is obsolete, as noted by Judge Simma:

“[The fact that] the international legal order might be consciously silent or neutral on a specific fact or act has nothing to do with non liquet, which concerns a judicial institution being unable to pronounce itself on a point of law because it concludes that the law is not clear. The neutrality of international law on a certain point simply suggests that there are areas where international law has not yet come to regulated, or indeed, will never come to regulate.”<sup>51</sup>

Accordingly, there is a possibility that certain acts might be tolerated which does not mean that the act is legal.

It is understandable why the International Group of Experts asserted their authority to identify the current *lex lata* and to avoid articulating *lex ferenda*. Had the experts decided to claim the role of international law legislator, it would have contradicted their own orthodox understanding of international law-making, which relies on the consent of states, and would have undermined their legitimacy. They, thus, chose a modest strategy conceiving of themselves as assistants who merely displayed the current state of international law by ostensibly using the classic legal tools.

<sup>46</sup> This is the standard used by the ICJ in the Genocide case in relation to demonstrating the full knowledge of the intent to perpetrate genocide by the leaders of the army of the Republic Srpska for the sake of complicity within the meaning of Article 3 (e) of the Genocide Convention (see *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment of 26 February 2007, ICJ Report 2007, para. 422).

<sup>47</sup> *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US)*, op. cit., paras. 24, 29, 62, 109; *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of Congo v. Uganda)*, op. cit., paras. 72, 91, 136.

<sup>48</sup> This is the standard that some scholars have extracted from the WTO panel decision (see Waincymer, J. (2002) *WTO Litigation: Procedural Aspects of Formal Dispute Settlement*. London: Cameron May, p. 568).

<sup>49</sup> Greenwood, C. (1987) *International Law and the United States, Air Operations Against Libya*. *West Virginia Law Review*, 89, p. 935.

<sup>50</sup> D’Aspremont, J. (2016) *Cyber Operations and International Law: An Interventionist Legal Thought*. *Journal of Conflict & Security Law*, 21, pp. 581–582.

<sup>51</sup> Declaration of Judge Simma, *Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo*, Advisory Opinion, 22 July 2010. ICJ Reports 2010, para. 9.

As long as the criticism regarding the transparency of the expert selection process and the flaws on the articulation of Rules, in particular pertaining to the use of force, are not casted out, the degree of the authority of the Tallinn Manuals as reflecting *lex lata* is questioned. Still, they are the products of a communicative process which will undoubtedly influence the making of international law on cyber operations. If the immobility of the traditional international law-making process – whether in form of universal conventions or judgments from authoritative tribunals indicating customary international law – cannot be overcome, this communicative practice will definitely contribute to future international law-making.

#### 4. CONCLUSION

International law-making at times involves the opinions of legal scholars and international lawyers. The Tallinn Manuals are no different in this respect. However, the claim that the Tallinn Manuals present the existing international law is debatable due to the imbalanced composition of the drafters, their questionable authority and the opaque drafting process. This article addressed the question to what extent legal scholarship plays a role in international law-making. Based on communicative practices, it argues that legal scholarship has a significant influence on the formation and interpretation of international law. The role of legal scholars contributing to the international law-making has been particularly relevant during the absence of concrete and specific international legal rules on cyber operations. The article argues that significant parts of the Tallinn Manuals have been shaped by the intuition of legal scholars, however, without disclosing this fact. As scholars will continue to play a significant role in the making of international law, this article argues that, in this process, issues of legitimacy need to be addressed more thoroughly by future scholarship.

#### LIST OF REFERENCES

- [1] (2013) UN Doc A/68/98.
- [2] *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*. Judgement of 26 February 2007. ICJ Report 2007.

- [3] *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)*. Judgement of 27 June 1986. ICJ Report 1986.
- [4] *Case Concerning the Arrest Warrant of 11 April 2000 (Democratic Republic of Congo v. Belgium)*. The Joint Separate Opinion of Judge Higgins, Kooijmans and Buergenthal, Judgement of 14 February 2002. ICJ Reports 2002.
- [5] D'Aspremont, J. (2016) Cyber Operations and International Law: An Interventionist Legal Thought. *Journal of Conflict & Security Law*, 21.
- [6] Declaration of Judge Simma, *Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo*, Advisory Opinion, 22 July 2010. ICJ Reports 2010.
- [7] Fleck, D. (2013) Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the New Tallinn Manual. *Journal of Conflict and Security Law*, 18.
- [8] Greenwood, C. (1987) International Law and the United States, Air Operations Against Libya. *West Virginia Law Review*, 89.
- [9] Kammerhofer, J. (2013) Lawmaking by Scholars. In: Brölmann Catherine and Radi Yannick (eds.). *Research Handbook on the Theory and Practice of International Lawmaking*. Cheltenham: Edward Elgar.
- [10] Kessler, O. and Werner, W. (2013) Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare. *Leiden Journal of International Law*, 26.
- [11] Kingsbury, B. Krisch, N. and Stewart, R. (2005) The Emergence of Global Administrative Law. *Law and Contemporary Problems*, 68.
- [12] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*. Advisory Opinion of 9 July 2004, ICJ Reports 2004.
- [13] Luhmann, N. (1993) *Das Recht der Gesellschaft*. Frankfurt: Suhrkamp.
- [14] Lynn, W. J. (2011) *Remarks on the Department of Defense Cyber Strategy as Delivered by Deputy Secretary of Defense William J. Lynn*. [speech] 14 July. Available from: <http://www.defense.gov/speeches/speech.aspx?speechid=1593> [Accessed 12 July 2018].
- [15] Mégret, F. (2005) From 'Savage' to 'Unlawful Combatant': A Postcolonial Look at International Humanitarian Law's Other. In: Anne Ordord (ed.). *International Law and Its Others*. Cambridge: Cambridge University Press.
- [16] Parry, C. (1965) *The Sources and Evidence of International Law*. Manchester: Manchester University Press.

- [17] Pauwelyn, J. (2012) Informal International Lawmaking: Framing the Concept and Research Questions. In: Joost Pauwelyn, Ramses Wessel and Jan Wouters (eds.). *Informal International Lawmaking*. Oxford: Oxford University Press.
- [18] Reisman, M. (1981) International Lawmaking: A Process of Communication. *American Society of International Law Proceedings*, 75.
- [19] Roscini, M. (2014) *Cyber Operations and the Use of Force in International Law*. Oxford: Oxford University Press.
- [20] Schachter, O. (1977) The Invisible College of International Lawyers. *Northwestern University Law Review*, 72.
- [21] Schmitt, M. (1998–1999) Computer Network Attacks: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*, 37.
- [22] Schmitt, M. (2015) The Use of Cyber Force and International Law. In: Marc Weller (ed.). *The Oxford Handbook of the Use of Force in International Law*. Oxford: Oxford University Press.
- [23] Skouteris, T. (2001) The Force of a Doctrine: Art. 38 of the PCIJ Statute and the Sources of International Law. In: Fleur Johns et al. (eds.). *Events: The Force of International Law*. New York: Routledge.
- [24] Slaughter, A.-M. (2000) Agencies on the Loose? Holding Government Networks Accountable. In: George Bermann and Peter Lindseth (eds.). *Transatlantic Regulatory Cooperation, Legal Problems and Political Prospects*. Oxford: Oxford University Press.
- [25] Teubner, G. (1997) Global Bukowina: Legal Pluralism in the World Society. In: *Global Law Without a State*. Hants: Dartmouth.
- [26] *The Tallinn Manual on the International Law Applicable to Cyber Warfare*.
- [27] *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operation*.
- [28] Tikk, E. Kaska, K. and Vihul, L. (2010) *International Cyber Incidents: Legal Considerations*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.
- [29] Triggs, G. (2005) The Public International Lawyer and the Practice of International Law. *Australian Yearbook of International Law*, 24.
- [30] US Naval War College. (2012) *Cycon 2012 Michael Schmitt: Tallinn Manual Part I*. [online video] Available from: <http://www.youtube.com/watch?v=wY3uEo-Itso> (1:40) [Accessed 20 July 2018].
- [31] Venzke, I. (2013) Contemporary Theories and International Law-making. In: Brölmann Catherine and Radi Yannick (eds.). *Research Handbook on the Theory and Practice of International Lawmaking*. Cheltenham: Edward Elgar.

- [32] Waincymer, J. (2002) *WTO Litigation: Procedural Aspects of Formal Dispute Settlement*. London: Cameron May.





## WEB-PAGE SCREENSHOTS AS AN EVIDENCE IN CIVIL PROCEDURE OF UKRAINE\*

by

NELLI GOLUBEVA\*\*, KRISTINA DROGOZIUK\*\*\*

*Currently the question about the possibility of including a screenshot of a web-page to the base of evidence in civil procedure of Ukraine remains open. The problem is a lack of systematic rules for determining procedures for obtaining electronic evidence, in particular, screenshots, in Ukrainian legislation, as well as possibilities for their use while considering civil cases. Various electronic evidence should correspond various admissibility criterias, and therefore the admissibility of electronic evidence should be examined separately according to each type of evidence.*

*Separate issues of investigation, fixation and certification of web-screenshots as evidence in civil procedure of Ukraine are considered in this article. The analysis of legal regulation and problems of the practical implementation of use of web-pages screenshots in Ukrainian civil procedure are carried out. The ways of implementation of recommendation rules for registration and fixation of web-screenshots in civil procedure, which can be applied for all European states, are proposed.*

### KEY WORDS

*Civil Procedure, Civil Procedure of Ukraine, Electronic Documents, Electronic Evidence, Means of Proof, Proving, Screenshots, Website*

---

\* The authors would like to express their gratitude to the reviewers, MUJLT Editor-in-Chief *Jakub Harašta* and editor *Lenka Pastušková*, who immensely helped to improve the quality of the manuscript.

\*\* nelli@email.ua, Professor, Head of the Department of Civil Procedure, Faculty of Civil and Commercial Justice, National University "Odesa law academy", Ukraine.

\*\*\* kristina.drogoziuk@gmail.com, Senior Lecturer, Faculty of Civil and Commercial Justice, National University "Odesa law academy", Ukraine.

## 1. INTRODUCTION

In time of information technology an important problem in protection of rights and interests is provision of collection, fixation and certification of evidence obtained from the Internet.

Electronic devices which are used every day for solving domestic, life, professional and other issues, due to their prevalence among users and functionalities, may also contain evidence, and sometimes this means of proof may be the only evidence in case, or have more probative value in comparison with other evidence during consideration and resolving of a particular civil case.<sup>1</sup>

The relevance of the chosen topic is due to increase in digital information and its systematic use in various spheres of life, which determines the need for further scientific research and a clearer legislative regulation of use of electronic evidence in civil procedure, as well as introduction of optimal approaches to information technologies in proving in civil procedure of Ukraine.

The judicial practice of recent years has shown that there are categories of civil cases in which the dispute has arisen over information posted on the Internet. In this category of cases, courts are forced to add to the case some files and investigate information received from the Internet.

Focusing on this topic is related to the fact that recently Ukrainian law has significantly developed in the question of electronic evidence, whiles currently there are many European states that either do not have such rules for electronic evidence.

The purpose of this research is to suggest some improvements to the mechanism of investigation, fixation and certification of web-screenshots in civil litigation, which can be useful both in Ukraine and in European countries.

## 2. ELECTRONIC EVIDENCE IN UKRAINE

It should be mentioned that the Internet is a way of placing and disseminating information that may involve a wide variety of civil cases which are connected with the illegal use or distribution of intellectual

---

<sup>1</sup> Laz'ko, O. (2015) Prospects for the development of electronic (technical) means of proof in the civil process of Ukraine. *Evropeyski perspektivy*, 1, pp. 125–129.

property objects; with protection of honor, dignity, business reputation; with breach of consumer rights protection, etc.

It should be emphasized that in theory of civil procedural law of Ukraine, the main criteria for the admissibility of “computer evidence” were determined in 1999. In particular, the following criteria were formulated: a document that was issued by a computer when it was used continuously for the accumulation and processing of information in any type of activity that was carried out at the same time; during this period the information was sent to the computer in the usual order; the whole period of work with the document computer functioned properly; the information in the document reflected the information that came to the computer in the usual way.<sup>2</sup> One of the main criteria for electronic evidence is the ability to identify the source by which this evidence was obtained.

Until adoption of the Law of Ukraine No 2147-VIII of October 3, 2017, which was significantly amended Civil Procedure Code of Ukraine (hereinafter referred to as *CPC of Ukraine*), no one normative legal act provided a special procedure for investigation and use of evidence placed on the Internet. In current CPC of Ukraine Part 7 of Art. 85 was included, according to which the court, on the application of the participant of the case or on its own initiative, may inspect the website, other places of data storage on the Internet in order to establish and fix its content.<sup>3</sup> Consequently, under the current CPC of Ukraine, a court has judicial authority to investigate the global network directly for the presence of certain facts that are in the subject of evidence in the case.

However, despite of such positive developments, CPC of Ukraine still does not sufficiently regulate issues regarding procedure for submission and certification of originals and copies of electronic evidence, order and peculiarities of the investigation and evaluation of such evidence by the court. Obviously, the lack of the normative regulations of the highlighted issues may lead to ambiguous judicial practice and make difficulties in use of electronic evidence in civil procedure.

<sup>2</sup> Reshetnikova, I. and Yarkov, V. (1999) *Grazhdanskoe pravo I grazhdanskiy process v sovremennoy Rossii* [Civil law and civil process in modern Russia]. Moscow: Izdatelstvo Norma, p. 178.

<sup>3</sup> Pavlova, Iu. (2017) Some aspects of the admissibility of electronic evidence in the civil procedural procedure law of Ukraine. *Prykarpatskyi yurydychnyi visnyk*, 5 (20), pp. 83–87.

As *Petrenko* emphasizes, that problems of legal regulation and the use of electronic evidence are parts of a wider problem of introduction of electronic and information technologies in litigation as a whole. In the legislation of many countries there were rules governing the use of electronic technologies in the consideration and resolution of cases by the court. Some countries already have a great deal of practical experience in using and standardizing electronic technologies at the trial.<sup>4</sup> For example:

- in Germany – Informations-und Kommunikationsdienste-Gesetz of June 13, 1997;
- in Australia – An Act to facilitate electronic transactions, and for other purposes, 1999;
- in the USA – Electronic Signatures in the Global and National Commerce Act, which came into force on October 1, 2000;
- in the UK – Electronic Communications Act 2000;
- in Canada – The Personal Information Protection and Electronic Documents Act of 2000 and the Canada Business Corporations Act, the Canada Cooperatives Act of 2001.

Paying attention to ways of ensuring the admissibility of electronic evidence, it is possible to note that in 1983 in the US a court has determined that in order to recognize the electronic evidence as admissible, it should be based on scientific knowledge and facilitate the understanding or verification of the facts by a judge or jury.<sup>5</sup>

### **3. WEB-SCREENSHOTS AND ISSUES OF ITS' USE IN CIVIL PROCEDURE OF UKRAINE**

Web-screenshot is a picture of the selected area of the screen of the device that displays the relevant web-page at the time of fixation of this image.

Web-page screenshots as evidence in litigation can be used for fixation:

- the fact of placing information on the Internet that does not correspond to reality or violates exclusive rights;

---

<sup>4</sup> Petrenko, V. (2018) Electronic evidence as an element of information technology in civil justice. *Molodyi vchenyi*, 1 (53), pp. 111–115.

<sup>5</sup> *Daubert v. Merrell Dow Pharmaceuticals Inc.*, U.S. Supreme Court. *United States Reports*, vol. 509, pp. 579–601, 1983.

- the confirmation of the fact of information on the Internet that infringes copyrights;
- the confirmation of improper performance or non-fulfilment of contractual obligations by other party in a case;
- another legally relevant information posted on the Internet.

However, there are many issues while using this type of evidence.

Firstly, any page on the Internet may be changed or, in general, deleted; also access to it may be blocked. There is a question of technical review of the page and access to information about its state in a retrospective, at the particular moment in the past.

Secondly, there is a complexity of identifying the person who disseminated negative information on the network or proving his (her) involvement in such dissemination. Given the specifics of the existence and operation of the Internet, any person may carry out various insulting messages and remain unknown at this time, which creates the procedural impossibility of filing a lawsuit for the plaintiff in light of norms of Art. 175 of CPC of Ukraine. Other important problems are *fixation of commission of an offense* and *fixation of a date of commission of an offense*.

Thirdly, *the absence of an official sample of a screenshot*, which would indicate the compliance with the document form, or the systematic rules of execution a screenshot and lodging it with the court, significantly complicates its use as evidence in a case.

Fourthly, sometimes non-recognition of a screenshot as evidence is due to *the inability to reproduce it in the original*.

The rapid development of computer technology and appearance of a variety of new programs facilitates counterfeiting, distortion or even destruction of information in electronic form, which will make it impossible or significantly difficult to investigate and evaluate electronic evidence by court. Consequently, a court may take into account false evidence and establish the circumstances of the case in a wrong way. This problem is only partially regulated by Art. 423 of CPC of Ukraine by consolidating such basis for reviewing of case with newly discovered circumstances as the falsehood of electronic evidence. However, CPC of Ukraine does not contain a mechanism for protecting electronic evidence from distortion or destruction.

#### 4. WEB-SCREENSHOTS OBTAINED FROM SOCIAL NETWORKS

A particular attention should be paid to the issue of the admissibility of web-screenshots obtained through social networks. Considering the ability of social networks to bring information about a large number of people, it is particularly essential to use data from social networks during consideration of cases about honor, dignity and business reputation protection, or about false information.<sup>6</sup>

Social network accounts in fact are reflections of a person's personality, and therefore in everyday life actions in social networks are considered to be committed on behalf of that person. Meanwhile, the abovementioned statement does not find its normative substantiation, which makes it difficult to recognize web-screenshots from social networks permissible. For example, in social networks like *Facebook*, *Instagram*, *Twitter*, anyone can register with any name and distribute false information. The connection between person and false information in social networks is hard to prove.

That is, the problem of the permissibility of screenshots obtained from social networks is to ensure the identification process of the person who created or distributed certain information in the social network.

Usually, defendants in cases where it is necessary to use electronic evidence from social networks, make the permissibility of such evidence doubtful, referring to the fact that no identification processes are carried out during the registration of the social network accounts, and therefore any person could register under the name of the defendant and do anything.

The use of false accounts was the subject of investigation by the *High Specialized Court of Ukraine for Civil and Criminal Cases* in a judgment of 22. 2. 2017 in the civil case *No 761/13156/16-ts*, during which the court of cassation noted that providing a legal assessment of the printed screenshot of a person's Facebook page, the *Court of Appeal* proceeded from impossibility to identify holders of accounts, located on resources/links in Facebook and the possibility of creating a fake account on this network. However, the *Court of Appeal* did not pay attention that some of the information on the defendant's Facebook page contained placemarks,

---

<sup>6</sup> Pavlova, Iu. (2017), op. cit.

confirmation of his location at a certain time at a particular place and a personal nature of certain information, rather than publicly available.<sup>7</sup>

In this case, the court examined not only content of a particular record, in which the information, according to the plaintiff, contained inaccurate information, but also the account as a whole on the availability of personal information, indicating the inextricable interconnection between the identity of the defendant and the relevant account in social network.<sup>8</sup>

Although the position of the cassation court raises certain procedural concerns, it is worth recognizing that this position is rather progressive, forms separate criteria for the permissibility of electronic evidence obtained from social networks, and in future may serve as a case law for lower courts.

## 5. FEATURES OF USING OF AN ELECTRONIC DIGITAL SIGNATURE IN WEB-SCREENSHOT

While Ukraine has accumulated a rather low experience in legal regulation of electronic document management and e-commerce, in the UN system and in the European Union these relations have already gained a significant development. The Association Agreement between the EU and Ukraine provides the harmonization of national legislation with EU law, therefore, it is worth to pay attention on the following legislative acts.

Two Model Laws: on Electronic Commerce (MLEC, 1996)<sup>9</sup> and Electronic Signatures (MLES, 2001)<sup>10</sup> have been created by the *United Nations Commission on International Trade Law – UNCITRAL*. These laws promoted legal status of electronic documents.

Art. 6 and 7 of the UNCITRAL Model Law on Electronic Commerce states that if the law requires written information, that requirement is met by a data message, if the information contained therein is accessible so as to be usable for subsequent reference.

<sup>7</sup> Decision of the High Specialized Court of Ukraine for the consideration of civil and criminal cases from 22. 2. 2017, Case No 761/13156/16-ц. [online] Available from: <http://www.reyestr.court.gov.ua/Review/65038960> [Accessed 17 January 2019].

<sup>8</sup> Pavlova, Iu. (2017) Some aspects of the admissibility of electronic evidence in the civil procedural procedure law of Ukraine. *Prykarpatskyi yurydychnyi visnyk*, 5 (20), pp. 83–87.

<sup>9</sup> UNCITRAL Model Law on Electronic Commerce (1996). [online] Available from: [https://www.uncitral.org/pdf/english/texts/electcom/05-89450\\_Ebook.pdf](https://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf) [Accessed 17 January 2019].

<sup>10</sup> UNCITRAL Model Law on Electronic Signatures (2001). [online] Available from: <http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf> [Accessed 17 January 2019].

Where law requires a signature of a person, that requirement is met in relation to a data message if:

- 1) the method is used to identify that person and to indicate that person's approval of the information contained in the data message;
- 2) the method is as reliable as was appropriate for the purpose data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

However, this statement is sufficiently general because it does not establish criteria for the method's compliance with the listed requirements. The answer, and further guarantees of the legal validity of information in electronic form (validity of the proposal, acceptance, and electronic evidence) can not be included.

In view of this, UNCITRAL Model Law on Electronic Signatures, which clarified a number of important issues, was further created. It specified more detailed requirements for electronic signature.

Firstly, it was stated that an electronic signature should be directly related to the person who signed the document. This means that the signature should exclude ambiguity with regard to the person.

Secondly, signing, at the moment when it is carried out, must be controlled only by the signatory. It is assumed that the person, expressing his (her) will, signs the document, and no one can put his (her) signature without his (her) knowledge. If anyone acts on behalf of another person(s), the general rules of representation are applied.

Thirdly, any change in the electronic signature made after signing must be available for identification. This requirement, firstly, does not affect the changes to the signed document, and secondly, does not mean that the changed signature is no longer valid. The fact is that all changes must be known to the counterparty, which will make a decision. This requirement, that signatures are made using cryptography tools is standard for EDS, but not necessary for other types of electronic signature. Therefore, drafters of the law have introduced a restrictive condition for the application of this requirement.



Two directives have also been adopted in the European Union: The Electronic Signatures Directive 1999/93/EC (no longer in force)<sup>11</sup> and The Electronic Commerce Directive 2000/31/EC<sup>12</sup>.

On 1 July 2016 The Electronic Signatures Directive 1999/93/EC was repealed by eIDAS (electronic IDentification, Authentication and trust Services). It was established in the Regulation (EU) No 910/2014 of 23 July 2014<sup>13</sup>. The regulation has applied directly to EU Member States and establishes a common standard for electronic signatures, electronic stamps, time stamps, eDelivery services and website authentication certificates in the internal market.

All organizations delivering public digital services in EU member state must recognize electronic identification from all EU member states from 29 September 2018.

It would seem that the regulation is an internal matter of the EU, but in reality, it is also used by foreign contractors who deal with European organizations. Although each country has its own identification and electronic digital signature (EDS) standards, eIDAS is a set of “best practices” that guarantees EDS compatibility at the European level, because all public organizations of the EU are obliged to recognize qualified EDS from other countries. In future, it is likely that eIDAS will expand its operation beyond the EU.

The Electronic Commerce Directive establishes a general requirement for the recognition of documents signed by electronic signature: EU member states should ensure that restrictions related to the use of electronic signatures should not significantly impede contractual relations between parties and deprive documents signed by an electronic signature of equal legal force in relation to traditional documents.

<sup>11</sup> Directive 1999/93/EC of European Parliament and of Council of 13 December 1999 on a Community Framework for Electronic Signatures (Electronic Signatures Directive). *Official Journal of European Communities*. L 13. [online] Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31999L0093> [Accessed 17 January 2019].

<sup>12</sup> Directive 2000/31/EC of European Parliament and of Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in Internal Market (Directive on electronic commerce). *Official Journal of European Communities*. L 178. [online] Available from: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031> [Accessed 17 January 2019].

<sup>13</sup> Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. *Official Journal of European Communities*. [online] Available from: <https://eur-lex.europa.eu/eli/reg/2014/910/oj> [Accessed 6 May 2019].

Currently, the use of electronic signatures in Ukraine is regulated by Laws of Ukraine: *On Electronic Trust Services*, *On Electronic Documents and Electronic Document Transfers*, *On E-Commerce*, and others.

The Law of Ukraine *On Electronic Trust Services* includes such concepts as “electronic signature”, “advanced electronic signature” and “qualified electronic signature”.

To become an owner of electronic digital signature it is necessary to apply to an accredited centre of key certification (ACKC). There are several dozen centres in Ukraine today. The activity of ACKC is carried out on the basis of the relevant license and certificate. The activity of the ACKC, as a commercial entity, is controlled by the *Central Certification Body* (Ministry of Justice of Ukraine) – a state organization that regulates relations in the field of electronic signature.

It should be noted that according to Part 2 of Art. 100 of CPC of Ukraine, Art. 1 of the Law of Ukraine *On Electronic Trust Services* and Part 1 of Art. 5 of the Law of Ukraine *On electronic documents and electronic document circulation*, electronic evidence or its copy without electronic digital signature, equivalent to a personal signature, cannot be considered as a reliable evidence. This means that the signing of electronic evidence by EDS is mandatory in the Ukrainian legislation.

It can be concluded that electronic evidence must be created using a specific system, access to which is obtained through a special electronic key issued by the authorized body.

In electronic correspondence, correspondence in messengers or social networks login and password to the system can be seen as simple electronic signature (as the system is holding the logs of the steps which were made under the login – thus e.g. in e-commerce platforms, we can talk about signing the electronic document when, for example, goods are ordered by clicking on the virtual buttons).

Evidence, if the document (log) belongs to some person, are thus incorporated in the metadata, which are held by the system provider. The reason for that is that simple electronic signature is very broadly described in Art. 3/10 eIDAS Regulation as

*“data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign”.*

Article 1/12 of the Law of Ukraine *On Electronic Trust Services* reproduces the specified norm and states that electronic signature is the electronic data, which is added by the signer to other electronic data or logically connected with them and used by him (her) as a signature.

In practice it becomes clear that until e-mail services, social networks, messengers do not require a copy of passport to register a new page, there is no evidence of belonging of them to a specific person and unscrupulous participants of litigation can use fake names. Thus, a judge has to decide on the relevance of such evidence.

## 6. WEB-SCREENSHOT – AN ORIGINAL OR A COPY OF ELECTRONIC EVIDENCE?

According to possibility of unobstructed copying of electronic evidence without limiting the number of copies and without any loss of their qualitative characteristics in the process of copying, it is possible to predict appearance of certain practical problems for the participants of the case, regarding the separation of the original electronic evidence from its copy, as well as the certification of electronic copies and paper copies of electronic evidence.<sup>14</sup>

Thus, there is still a question what can be considered as the original of electronic evidence. As a result, the court may have questions about the permissibility and legal assessment of the evidence. For example, will be considered as the original a video or a screenshot, filed on a CD or on a flash memory card or other media, if it was made with the help of a webcam, then saved on the Internet and then copied to a CD or a flash memory card? Similar questions may arise regarding videos, sound recordings, or screenshots made during a live stream on the *Youtube* service and, accordingly, saved on the server of this service. *Petrenko* emphasizes that the subsequent copying of such a video or photo on a CD will not be considered as an original.<sup>15</sup>

Part 3 of Art. 100 of CPC of Ukraine establishes that parties of the case have the right to submit electronic evidence in paper copies certified in accordance with the procedure prescribed by law. That is, civil procedural law defines web-screenshot as a copy of electronic evidence.

<sup>14</sup> Petrenko, V. (2018) Electronic evidence as an element of information technology in civil justice. *Molodyi vchenyi*, 1 (53), p. 113.

<sup>15</sup> Ibid.

At the same time, participant, who submits a copy of electronic evidence, must indicate who has an original electronic evidence. If original electronic evidence is not filed and party of the case or court has some doubts on the conformity of submitted copy of an original, such evidence is not taken into account at the trial. However, as noted above, information that is posted on the Internet can be easily changed or even deleted.

To solve this problem, an amendment was added to CPC of Ukraine, which is on the possibility of carrying out an inspection of electronic evidence at their location in case of impossibility of its delivery.

## 7. CARRYING OUT AN INSPECTION OF ELECTRONIC EVIDENCE AT ITS LOCATION

In accordance with Part 7 and 8 of Art. 85 of CPC of Ukraine, the court on the application of a participant of the litigation or on its own initiative, may inspect the website, other places of data storage on the Internet in order to establish and record their contents.

The applying of evidence inspection at its location is possible on condition that the electronic evidence has not been removed from the place of data storage. It happens quite often, when in a case a court does not have access to the original of electronic evidence. Due to the lack of a clear definition of the concept of “original electronic evidence” there may be doubts about its permissibility in the case when it has been copied to a CD or other information carrier, since in this case evidence can be considered as an electronic copy, not the original.<sup>16</sup>

To resolve these contradictions, it seems advisable to amend CPC of Ukraine with Article 100-1 in which to define the concept of “original electronic evidence” and “copy of electronic evidence” as follows:

*The original electronic evidence* is information in electronic form that has a set of mandatory requisites and/or properties that makes such information unique and different from other similar electronic evidence. Graphic (digital) images, videos and recordings saved on various electronic information carriers are used as originals of electronic evidence and can not be considered as electronic copies, except when the source of such objects is the Internet (created directly on the Internet).

---

<sup>16</sup> Ibid.

*Copy of electronic evidence* is created by electronic (digital) means or reproduced on paper, and corresponds to the original and certified in accordance with the procedure established by the law.

It is worth emphasizing that the difference of information on the website of the provided copy of the screenshot is not an obstacle to use it as evidence, since in this case it is already a question of either faking the screenshot or changing the website, which should be established by appropriate expertise.

## 8. COMPUTER-TECHNICAL EXPERTISE FOR SETTING AND FIXING THE CONTENT OF THE WEBSITE

It should be underlined that today we can talk about the problem of the low level of training judges for work with software and hardware complexes and complex software shells. It is impossible to obtain equivalent knowledge after reading books or having communication with a specialist. In this regard, the involvement of a specialist while working with electronic evidence is mandatory, since the least unskilled action can lead to the loss of important evidence or guidance information.<sup>17</sup>

The court has a right to appoint a computer and technical expertise to establish and record the content of the website, other places of data storage on the Internet, on condition – if it requires special knowledge and can not be carried out by the court independently or with the specialist's participation.

According to Art. 1 of the Law of Ukraine *On Forensic Examination*, forensic examination is a research on the basis of special knowledge in the field of science, technology, art, crafts, etc. concerning objects, phenomena and processes in order to provide an opinion on questions that are or will be the subject of judicial review. According to the results of computer-technical expertise, the expert will be able to determine the actual location of the server, which provides the activity of the offender, as well as to investigate the contents of the server itself, even to recover deleted files, determining the date of their creation and placement.<sup>18</sup>

There is no doubt that electronic evidence obtained through the Internet, examined in the order prescribed by Art. 85 of CPC of Ukraine, will fully

<sup>17</sup> Tsehan, D. (2013) Digital evidence: the concept, features and place in evidence system. *Naukovyi visnyk Mizhnarodnogo humanitarnogo universytety. Iurisprudencia*, 5, pp. 256–260.

<sup>18</sup> Ibid.

comply with the requirements for the permissibility of electronic evidence, and therefore can be used in civil disputes resolution.

Expert examinations are carried out by certified court experts in relevant specialties, which are included in the register of court experts of the Ministry of Justice of Ukraine.<sup>19</sup>

During an expert research on the object of intellectual property that is contained on the website occurs:

- domain name verification, installation of DNS servers;
- checking the IP address matching;
- fixing the display of the content of the site, the display of the main page, transitions to pages of interest to the applicant;
- determining the time of creating a web page;
- research data are recorded in the research part of the conclusion, the survey results (web-pages, photographs, screenshots, etc.) are made by the inspection report with the indication date.

## 9. NOTARY CERTIFICATION OF WEB-SCREENSHOTS

In order to use electronic information as evidence in Ukrainian civil procedure there were some attempts to substantiate the position regarding the possibility of providing screenshots to the court, certified by a notary as evidence. However, this practice is not widespread and in most cases plaintiffs provide simple printouts of information from the website to the court.<sup>20</sup>

In CPC of Ukraine all cases of notarial certification of copies of documents are allocated separately. Art. 95 of CPC of Ukraine states that the party has a right to provide a copy of written evidence, certified by his (hers) own signature. However, Art. 100 of CPC of Ukraine states that a written copy of electronic evidence is not a written evidence. From this it turns out that Art. 95 of CPC of Ukraine does not regulate the issue of how a paper copy of electronic evidence should be certified.

Consequently, the question arises in which way a paper copy of electronic evidence is required to be certified, what is generating a gap

---

<sup>19</sup> Okhromeev, Yu. (2012) Collection of evidence base in cases of violation of rights in the Internet. [online] Available from: [http://uba.ua/documents/text/27\\_01\\_2012\\_Okhromeev.pdf](http://uba.ua/documents/text/27_01_2012_Okhromeev.pdf) [Accessed 17 January 2019].

<sup>20</sup> Lezhuh, T. (2013) The use of electronic evidence in cases relating to the protection of honor, dignity and business reputation. *Viche*, 16, pp. 13–15.

in the law. Because of this, judges do not know how to comply with such an ambiguous rule of law and could apply it incorrectly; besides, they will not take responsibility, because formally the violation of the process will not take place because of a gap in the procedural law. Sometimes, because of this gap in the law, electronic evidence is unlawfully unconnected, and, conversely, some evidence is added contrary to the law. In such cases, the rights of participants in the process concerning the accession of evidence and the basis of legal proceedings are violated, and with it parties' rights to a fair trial.<sup>21</sup>

Therefore, it is no accident, that the question of the possibility or impossibility of fixation by the notary of information obtained from the Internet is considered sufficiently debatable among lawyers. Since some scholars think that a notary can provide evidence from the Internet,<sup>22</sup> while others put forward technical and legal objections.<sup>23</sup>

The scholar *Kucher* states that the necessary confirmation of the execution of a transaction is the introduction of the relevant information in the register, their perception by the notary or reproduction through the use of computer technology products.<sup>24</sup> Indeed, for the purpose of committing important notarial actions by the notaries today, it is necessary to check the absence of prohibitions of alienation of real estate objects, the existence of state registration of ownership of a specific owner, etc., which are contained directly on the Internet, but such important information may be distorted or specifically presented in a distorted form on computer of a specific notary.

Considering this issue from the standpoint of the notarial process, we can set a threat to ensure not only the notarial secrecy, but also the reliability of the information that notaries receive through the Internet for the commission of notarial actions. *Badila* emphasizes that for the investigation of this type of evidence it should be provided a legal and

<sup>21</sup> Draft Law on Amendments to Article 100 of the Civil Procedural Code of Ukraine (regarding the certification of copies of electronic evidence). [online] Available from: [http://w1.c1.rada.gov.ua/pls/zweb2/webproc4\\_1?pf3511=63876](http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=63876) [Accessed 17 January 2019].

<sup>22</sup> Yacenko, O. (2013) Providing evidence by notaries, or neighboring experience, which is lacking in Ukrainian lawyers. *Yurydychnyi zhurnal*, 5 (131), pp. 60–67.

<sup>23</sup> Afyan, A. (2013) The role of the notary in the process of proving the facts regarding information in the Internet. *Civilisticheskaya processualnaya musul'. Mezhdunarodnyi zbornik nauchnykh statey*, 2, pp. 119–125.

<sup>24</sup> Kucher, T. (2013) Features of the application of evidence created with the help of computer technologies in the notarial process. *Civilisticheskaya processualnaya musul'. Mezhdunarodnyi zbornik nauchnykh statey*, 2, p. 153.

technical expertise to answer questions regarding the possibility of notaries to secure evidence, which are available on the Internet.<sup>25</sup>

Art. 75 of the Law of Ukraine *On Notary* determine that notaries, officials of local self-government bodies who carry out notarial actions, certify the fidelity of copies of documents issued by enterprises, institutions and organizations, provided that these documents do not contradict the law, have a legal value and certification of their loyalty copies which are not prohibited by the law.

However, now Ukrainian notaries refuse to implement the protocol for reviewing the web-page due to the lack of such a notarial action in the Law of Ukraine *On Notary* and in the Order of notarial actions by notaries of Ukraine.

Consequently, a situation arises when a person can provide a court with a printout from a website where false or insulting information has been disseminated, and then, after receiving a statement of claim, the person who distributed it can easily remove it, making impossible to prove its existence. On the one hand, in such a situation, the plaintiff can apply for confirmation the existence of information to a person providing hosting services (placing a website on the Internet) or to the Internet service provider. And on the other hand, such information may not always be collected by such person. In addition, it often takes a lot of time to receive it (for example, assignment of orders to the courts of other states).

Sometimes, plaintiffs try to claim through a court reference from providers in the form of log-files (with a list of actions of users and placement of data), since obtaining such a reference in pre-trial order is virtually impossible. According to the Law of Ukraine *On Telecommunications*, operators and providers of telecommunications are obliged to provide and carry responsibility for the security of information about the telecommunication services provided, including the receipt of services, their duration, content, routes, etc.

Consequently, Ukrainian law emphasizes that personal information may be disseminated either in the presence of a written consent of the consumer, or at the request of the inquiry authority, investigator, prosecutor or court within the bounds of a criminal or operative-investigative affair.

---

<sup>25</sup> Badila, O. (2014) Evidence and the need to provide them with a notary and a court: topical issues. *Nashe pravo*, 4, pp. 156–161.



Recently, a draft law No 8281 dated April 17, 2018 *On Amendments to Article 100 of CPC of Ukraine (regarding the certification of copies of electronic evidence)* was registered in Verkhovna Rada of Ukraine, which is an unconditional positive step towards the settlement of the use of screenshots in civil procedural law.

Adoption of the bill will provide an opportunity to deal more quickly with cases in which electronic evidence is present. Judges will not have to question the correctness of the application of certain rules of law. The implementation of the bill will remove doubts as to the compliance of the original of attached materials with cases and copies of electronic evidence. As a result of adoption of the bill, the procedural rights of citizens will be ensured.<sup>26</sup>

A notary, as a person authorized by law, will be in position to assume responsibility for the fact that paper copy has been taken from a certain electronic evidence. In addition, the notary has the technical ability and access to all necessary registries for such certification. At the same time, the notary will take the responsibility for the false information of the certified data.

It also seems advisable to regulate the rules and requirements for drawing up a screenshot in civil procedure law of Ukraine. One of the forms of fixing information on the Internet in the world is the notarial certificate of the content of the electronic page.

In connection with the lack of procedures for the provision of electronic evidence by notaries in Ukrainian legislation, if there is a reason to think that filing evidence will subsequently become impossible or complicated, Ukrainian lawyers will have to turn to the notaries of the Russian Federation, whose legislation provides such a notarial action.

Articles 102–103 of the Fundamentals of Legislation on the Notary of the Russian Federation provide the implementation of notaries' activities to provide evidence.<sup>27</sup> As a part of its activity to provide evidence, notary often conducts a review of the website or content of the e-mail. Notary inspect a site and describes its content in detail. The result is a protocol

<sup>26</sup> Draft Law on Amendments to Article 100 of the Civil Procedural Code of Ukraine (regarding the certification of copies of electronic evidence). [online] Available from: [http://w1.c1.rada.gov.ua/pls/zweb2/webproc4\\_1?pf3511=63876](http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=63876) [Accessed 17 January 2019].

<sup>27</sup> Fundamentals of the legislation of the Russian Federation on notary, Federal Law of 11. 2. 1993, No 4462-1. [online] In Russian. Available from: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_1581](https://www.consultant.ru/document/cons_doc_LAW_1581) [Accessed 17 January 2019].

of reviewing a website, which is fixed by a notary's seal. Also Article 103.9 regulates the certification of the equivalence of the document on a paper medium and an electronic document. It consists in confirming the identity of the content of the submitted electronic document to the notary in the contents of a paper notarized document.

A document made on a paper carrier made by a notary has the same legal validity as an electronic document, the equivalence of which is certified by a notary. The electronic document submitted to the notary must be signed by a qualified electronic signature.

*Tripulsky* stresses that this norm can also be used in Ukraine in accordance with Art. 12 of the Convention on Legal Assistance and Legal Relations in Civil, Family and Criminal Matters (October 7, 2002), which is valid both for Ukraine and for Russian Federation.<sup>28</sup> Thus, documents, which are issued or certified by the competent authority or by the specifically authorized person within its competence and in the prescribed form and affixed by the stamp in the territory of one of the Contracting Parties, are accepted on the territories of the other Contracting Parties without any special certificate. Documents which are considered as official documents in the territory of one of the Contracting Parties use evidence power of official documents in the territories of other Contracting Parties.<sup>29</sup>

Website review by the notary of Russian Federation consists of the following steps:

- verification of the domain name, installation of DNS-servers;
- verification of IP-address;
- checking the accuracy of displaying the content of the website with a browser to which it refers;
- displaying referrals to pages, which are interesting for the applicant.

---

<sup>28</sup> Minsk Convention on Legal Assistance and Legal Relations in Civil, Family and Criminal Matters (7. 10. 2002). [online] Available from: <http://cisarbitration.com/wp-content/uploads/2017/02/Minsk-Convention-on-Legal-Assistance-and-Legal-Relations-in-Civil-Family-and-Criminal-Matters-english.pdf> [Accessed 17 January 2019].

<sup>29</sup> Tripulskiy, G. (2015) Some aspects of the admissibility of evidence obtained on the Internet in the civil process. *Tsyvil'ne sudochynstvo u svitli sudovoi reformy v Ukraini: materialy mizhn. nauk.-pract. konf. im. Yu. S. Chervonogo* [Civil Justice in the Light of Judicial Reform in Ukraine: materials of the int. scient. and pract. conf. Yu.S. Chervonogo], Odessa, 18 December, Ukraine: National University "Odessa law academy", p. 75.

Each stage is recorded in the narrative part of the protocol, the results of the review (web-pages, photos, screenshots) are printed and filled to the protocol. In addition, the protocol describes the inspected web pages, the content of evidence, the place and time of the notarial action, information about the persons who are interested in, and the notary. That is, the notaries of Russian Federation make appropriate protocols, which do not require any legalization. They are translated into Ukrainian and submitted to court as evidence. However, this method takes a lot of time.

Taking into account the existence of the problem of certification of electronic copies of electronic evidence, there is a need to amend the Law of Ukraine *On Notary*, adding in Art. 34 "Notarial Acts Performed by Notaries", the following provisions:

*"certify the fidelity of electronic and paper copies of electronic documents".*

It seems appropriate that in order to solve the problem regarding notarization of web-screenshots, it is necessary to develop a remote system of automated notarization of copies of the Internet pages, websites and data in the Internet at a certain point in time, which will be the same for all EU countries and, in particular, for Ukraine.

Providing of such remote system of automated notarization is possible with the following algorithm:

- 1) identification of the Internet resource, which has a destructive character, making a decision on fixing the content and certifying it notariially;
- 2) choosing in the special online resource (e.g. for Ukraine – the online resource of Ministry of Justice of Ukraine) the necessary type of remote automated notarization of information posted on the Internet;
- 3) filing online application for notarization of Internet pages with the data on: the address (URL) of the web-resource, which contains data that the user intends to certify notariially; personal data of the customer services (first name, last name, number and series of passport, e-mail, etc.);
- 4) on-line fulfilment of the application for notarization of information placed on the Internet, by its processing by a special automated software and hardware complex

in automatic mode (verification of the accuracy of displaying the content of the site, displaying the main page, moving to the necessary pages, checking the domain name, determining DNS servers, checking the IP address matching, etc.);

- 5) providing the customer check-card with information on the fulfilment of the application (or the impossibility of the fulfilment) and individual order code in an automatic on-line regime;
- 6) payment of the service by the customer in accordance with the tariff;
- 7) obtaining by an individual order code at the notary (private or public) paper materials, certified by a notary's seal, or electronic materials, certified by an electronic digital signature of the notary.

Thus, the normalization and introduction of a common mechanism for notarization of information from the Internet will promote:

- 1) increasing of the responsibility of the Internet users for the reliability, truthfulness of information and data placed on the Internet;
- 2) reducing the level of trust in fake information (from unconfirmed sources);
- 3) significantly expanding the scope of legal instruments for the protection of the rights and freedoms of a citizen and state authorities from the dissemination of false and defamatory information, the illegal collection and dissemination of confidential information, personal data, etc.;
- 4) timely response of the state to challenges related to the dissemination of confidential and information of an extremist nature, illegal interference with the operation of state electronic information resources, unauthorized copying, modification, destruction or blocking of information processes in state electronic information resources.

Unfortunately, in judicial practice there are cases when the judge denied parties to provide evidence. Therefore, a person, if he (she) considers the actions of the court illegitimate, should have the right to apply

to the notary for providing evidence, as the shortcomings of the legislation of Ukraine may adversely affect his (her) rights. Thus, the *Pechersk District Court of Kiev* indicated that a simple screenshot, in which the web-page was opened in the browser window, and the printout of its contents are not valid and admissible evidence in this case (Decree of 1. 4. 2016 in case number 757/13905/16<sup>30</sup>, Decision of 24. 5. 2017 in case number 757/43218/16<sup>31</sup>).

Thus, as was mentioned above, Ukraine currently does not have a well-defined mechanism for fixing information obtained from the Internet at a certain point in time. The implementation of this system, as an additional way of fixing such information, will expand the scope of information technology use in the judicial process, improve the process of providing notarial services, protect rights of participants of civil procedure and optimize the costs of both participants of the case and the state.

## 10. OTHER WAYS TO ENSURE ELECTRONIC EVIDENCE

*Kalamaiko* offers another way of extrajudicial ensuring of evidence, namely, access to independent organizations that provide services for fixing information on web pages. There are resources that allow taking a “snapshot” of information posted on a website at a certain point in time (*archive.is*, *peeps.us*). Such a file is saved on the server of the organization and placed in public access, so that the court can directly verify the existence of such information.<sup>32</sup>

Also, there is an *Mayback Machine Internet Archive* (*archive.org*), an independent resource that saves copies of web pages at different times, depending on their popularity. It belongs to a non-profit organization and has the legal status of a library. Due to this, it is already actively used all over the world and its proven force was recognized by design in the case *Telewizja Polska USA, Inc. v. Echostar Satellite* from 15. 10. 2004.<sup>33</sup>

<sup>30</sup> Decision of Pechersk District Court of Kyiv from 1. 4. 2016 in case No 757/13905/16. [online] In Ukrainian. Available from: <http://www.reyestr.court.gov.ua/Review/56950422> [Accessed 17 January 2019].

<sup>31</sup> Decision of Pechersk District Court of Kyiv from 24. 5. 2017 in case No 757/43218/16. [online] In Ukrainian. Available from: <http://www.reyestr.court.gov.ua/Review/66859813> [Accessed 17 January 2019].

<sup>32</sup> Kalamayko, A. (2015) The Internet Network as a Source of Evidence in the Civil Process. *Yurydychna Ukraina. Civilnyi proces*, 4 (50), p. 120.

<sup>33</sup> Ibid.

Nowadays Ukrainian courts accept data from this independent resource as appropriate evidence. For example, in the decision of *Goloseevsky District Court of Kyiv* from 10. 10. 2015 in case No 752/9476/15, the Court explained why it trusts this source:

*“Snapshots of web-pages made with the help of online services for storing web-page content, are carried out using software hosted on the server of non-interested person. The corresponding file with the snapshot is also stored on the server of such person and placed in public access on the Internet. Together with the snapshot, the original web-page address and the exact time when it was made are recorded. In this case, the information that on a web-page is copied directly, instead of displaying it on the user’s screen. In this way, the possibility of modifying the original content of web-page is virtually eliminated, since all operations related to fixing content of web-page and its storage are carried out without interference by any interested parties”.*<sup>34</sup>

However, there are certain technical limitations for fixing the contents of a web-page: objects larger than 10 MB in size are not saved; pages with restricted access are not saved also. In addition, at the request of the website owner, data from this web archive can be deleted.

Consequently, there are *several ways of investigation, fixation and certifying web-screenshots*:

- 1) inspection of evidence by the court at its location (review of the website, or other places of data storage on the Internet);
- 2) review and certification of the web-page by a notary;
- 3) use of *InternetArchive*, *WaybackMachine* services;
- 4) conducting an expert examination 10.17 – examination of telecommunication systems (equipment) and facilities.

There are other ways of fixing web-screenshots, however, the question of relevance and admissibility of such methods remains controversial.

The abovementioned rules for drawing up screenshots allow evaluating them as evidence in the case. A simple printout of the screenshot without reference of the date, time, website from which it was executed, without

---

<sup>34</sup> Decision of *Goloseevsky District Court of Kyiv* from 10. 10. 2015 in case No 752/9476/15. [online] In Ukrainian. Available from: <http://reyestr.court.gov.ua/Review/52726541> [Accessed 17 January 2019].

the signature and initials of the executor can not be considered as proper evidence.

Screenshots can be used with other evidence if they correspond all the requirements. When giving a screenshot as evidence, it is necessary to provide the following information:

- 1) time and date of the photo (to confirm the relevance of the information provided);
- 2) the address and the name of the photographed site;
- 3) the name, signature and position of the person who made the screenshot;
- 4) translation of information in a foreign language into Ukrainian;
- 5) notarization of the screenshot.

It is also important to save a screenshot of the web-page on computer's hard drive or on portable storage devices, which will ensure that such evidence can not be lost.

## 11. CONCLUSIONS

Electronic forms of communication, first of all, social networks and the Internet, have reached great level of influence on public life, so they became an important source of information, and therefore there is a need of normative settlement of its using in the process of resolving of civil cases by a court.

Summarizing, we must state that in practice many questions arise about the possibility of using information from websites as evidence. Normative regulation of electronic evidence provided by the current Ukrainian legislation is limited and does not allow the participants to fully realize their obligation to prove all the circumstances on which they refer to both their claims and objections, as well as their rights on effective judicial protection, guaranteed the Constitution of Ukraine and the European Convention on Human Rights.

In the context of the ever-increasing use of various information technologies in public relations, electronic correspondence, the emergence and rapid development of e-commerce, electronic means of payment, there is a need for a normative regulation of the use of web-screenshots as a means of proof in civil procedure.

Screenshots contain information about the facts on the basis of which the court can establish: the circumstances on which arguments of parties are based; presence or absence of violation; guilt and other circumstances relevant to the case. Thus, screenshots can serve as evidence in court during consideration of civil cases, however, they must be drawn up and issued in a documented order.

It seems appropriate to regulate on legislative level a list of ways of fixing the information, placed on the Internet, accessible to the participants of the case. It is proposed to expand their capabilities by providing notaries with a separate authority regarding certification of such evidence, which in practice will help to avoid collisions, as well as filling the existing gaps in the legislation regarding electronic evidence.

The only way to resolve this problem is adopting amendments to the current CPC of Ukraine, creating a remote system of automated notarization of copies of the Internet pages, websites and data on the Internet at a certain point in time, which will be the same for all EU countries and establishing obligation for the Internet providers to keep information placed on their electronic resources [within one year (as it is legally established for appealing to a court with a claim of refutation inaccurate information that was posted in the media)]. But, nonetheless, it should not be forgotten that Ukrainian legislation emphasizes that personal information can only be extracted in individual cases in special order.

## LIST OF REFERENCES

- [1] Afyan, A. (2013) The role of the notary in the process of proving the facts regarding information in the Internet. *Civilisticheskaya processualnaya musul'. Mezhdunarodnyi zbornik nauchnykh statey*, 2.
- [2] Badila, O. (2014) Evidence and the need to provide them with a notary and a court: topical issues. *Nashe pravo*, 4.
- [3] Decision of Goloseevsky District Court of Kyiv from 10. 10. 2015 in case No 752/9476/15. [online] In Ukrainian. Available from: <http://reyestr.court.gov.ua/Review/52726541> [Accessed 17 January 2019].
- [4] Decision of Pechersk District Court of Kyiv from 1. 4. 2016 in case No 757/13905/16. [online] In Ukrainian. Available from: <http://www.reyestr.court.gov.ua/Review/56950422> [Accessed 17 January 2019].



- [5] Decision of Pechersk District Court of Kyiv from 24. 5. 2017 in case No 757/43218/16. [online] In Ukrainian. Available from: <http://www.reyestr.court.gov.ua/Review/66859813> [Accessed 17 January 2019].
- [6] Decision of the High Specialized Court of Ukraine for the consideration of civil and criminal cases from 22. 2. 2017, Case No 761/13156/16-П. [online] Available from: <http://www.reyestr.court.gov.ua/Review/65038960> [Accessed 17 January 2019].
- [7] Directive 1999/93/EC of European Parliament and of Council of 13 December 1999 on a Community Framework for Electronic Signatures (Electronic Signatures Directive). *Official Journal of European Communities*. L 13. [online] Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31999L0093> [Accessed 17 January 2019].
- [8] Directive 2000/31/EC of European Parliament and of Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in Internal Market (Directive on electronic commerce). *Official Journal of European Communities*. L 178. [online] Available from: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031> [Accessed 17 January 2019].
- [9] Draft Law on Amendments to Article 100 of Civil Procedural Code of Ukraine (regarding the certification of copies of electronic evidence). [online] Available from: [http://w1.c1.rada.gov.ua/pls/zweb2/webproc4\\_1?pf3511=63876](http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=63876) [Accessed 17 January 2019].
- [10] Fundamentals of the legislation of the Russian Federation on notary, Federal Law of 11. 2. 1993, No 4462-1. [online] In Russian. Available from: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_1581](https://www.consultant.ru/document/cons_doc_LAW_1581) [Accessed 17 January 2019].
- [11] Chornyi S. and Antoniyuk O. (2018) Electronic evidence in civil proceedings: problems of practical application. *Visnyk students'kogo naukovogo tovarystva DonNU imeni Vasylya Stusa*. [online] Available from: <http://jvestnik-sss.donnu.edu.ua/article/download/5468/5495> [Accessed 17 January 2019].
- [12] Kalamayko, A. (2015) The Internet Network as a Source of Evidence in Civil Process. *Yurydychna Ukraina. Civilnyi proces*, 4 (50).
- [13] Kucher, T. (2013) Features of the application of evidence created with the help of computer technologies in the notarial process. *Civilisticheskaya processualnaya musul'*. *Mezhdunarodnyi zbornik naychnukh statey*, 2.
- [14] Laz'ko, O. (2015) Prospects for the development of electronic (technical) means of proof in civil process of Ukraine. *Evropeyski perspektivy*, 1.
- [15] Lezhuh, T. (2013) The use of electronic evidence in cases relating to the protection of honor, dignity and business reputation. *Viche*, 16.

- [16] Minsk Convention on Legal Assistance and Legal Relations in Civil, Family and Criminal Matters (7. 10. 2002). [online] Available from: <http://cisarbitration.com/wp-content/uploads/2017/02/Minsk-Convention-on-Legal-Assistance-and-Legal-Relations-in-Civil-Family-and-Criminal-Matters-english.pdf> [Accessed 17 January 2019].
- [17] Okhromeev, Yu. (2012) Collection of evidence base in cases of violation of rights in the Internet. [online] Available from: [http://uba.ua/documents/text/27\\_01\\_2012/Okhromeev.pdf](http://uba.ua/documents/text/27_01_2012/Okhromeev.pdf) [Accessed 17 January 2019].
- [18] Pavlova, Iu. (2017) Some aspects of the admissibility of electronic evidence in the civil procedural procedure law of Ukraine. *Prykarpatskyi yurydychnyi visnyk*, 5 (20).
- [19] Petrenko, V. (2018) Electronic evidence as an element of information technology in civil justice. *Molodyi vchenyi*, 1 (53).
- [20] Procedure for certifying the authenticity of copies of documents, Ukraine. [online] Available from: <http://www.minjust.gov.ua/15101> [Accessed 17 January 2019].
- [21] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. *Official Journal of European Communities*. [online] Available from: <https://eur-lex.europa.eu/eli/reg/2014/910/oj> [Accessed 6 May 2019].
- [22] Reshetnikova, I. and Yarkov, V. (1999) *Grazhdanskoe pravo i grazhdanskiy process v sovremennoy Rossii* [Civil law and civil process in modern Russia]. Moscow: Izdatelstvo Norma.
- [23] Tripulskiy, G. (2015) Some aspects of the admissibility of evidence obtained on the Internet in the civil process. *Tsyvil'ne sudochynstvo u svitli sudovoi reformy v Ukraini: materialy mizhn. nauk.-pract. konf. im. Yu. S. Chervonogo* [Civil Justice in the Light of Judicial Reform in Ukraine: materials of the int. scient. and pract. conf. Yu.S. Chervonogo], Odessa, 18 December, Ukraine: National University "Odessa law academy".
- [24] Tripulskiy, G. (2015) The possibility to provide evidence in the case by notaries. *Tsyvil'ne Sudochynstvo u svitli sudovoi reformy v Ukraini: materialy „kruglogo stolu“* [Civil justice in the light of judicial reform in Ukraine: materials of the "round table"], Odessa, 16 May. Ukraine: National University "Odessa law academy".
- [25] Tsehan, D. (2013) Digital evidence: the concept, features and place in evidence system. *Naukovyi visnyk Mizhnarodnogo humanitarnogo universytetu. Iurisprudencia*, 5.

- [26] U.S. Supreme Court, *Daubert v. Merrell Dow Pharmaceuticals Inc.*, United States Reports, vol. 509, 1983.
- [27] UNCITRAL Model Law on Electronic Commerce (1996). [online] Available from: [https://www.uncitral.org/pdf/english/texts/electcom/05-89450\\_Ebook.pdf](https://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf)  
[Accessed 17 January 2019].
- [28] UNCITRAL Model Law on Electronic Signatures (2001). [online] Available from: <http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf>  
[Accessed 17 January 2019].
- [29] Yacenko, O. (2013) Providing evidence by notaries, or neighboring experience, which is lacking in Ukrainian lawyers. *Yurydychnyi zhurnal*, 5 (131).

<<< ARTICLES

BOOK REVIEWS >>>

DOI 10.5817/MUJLT2019-1-6

## RETHINKING THE JURISPRUDENCE OF CYBERSPACE. REED, C.; MURRAY, A.

by

DOMINIKA GALAJDOVÁ \*

*Reed, C.; Murray, A. (2018) Rethinking the Jurisprudence of Cyberspace. Cheltenham: Edward Elgar Publishing, 235 p.*

*Rethinking the Jurisprudence of Cyberspace* is the joint work of Chris Reed and Andrew Murray which follows their previous contribution on the topic of legal theory and cyberspace.<sup>1</sup> The book aims to provide an answer to one of the most fundamental questions which law is applicable in cyberspace? The authors have considered through the whole book the elementary ideas of jurisprudence in the online environment, such as authority, legitimacy and rule of law. The book reflects on the recognised previous work on this topic by different commentators (*Lessig, Johnson and Post, Reidenbers*) and continues with its own concluding remarks and considerations.

The book is divided into three parts which contain together 8 chapters. Each part also includes a semi-conclusion at the end, which is helpful and practical for readers. The first part is focused on the authority in cyberspace and discusses various lawmakers, their role and rules in cyberspace. The second part provides a complex analysis of how rules actually operate in the online environment. The last part reflects the conclusion of previous parts as well as providing an answer to the question of how subjects should

---

\* dominika.galajdova@mail.muni.cz, Ph.D. student at the Institute of Law and Technology on Masaryk University, Brno, the Czech Republic.

<sup>1</sup> Reed, C. (2012) *Making Laws for Cyberspace*. Oxford: Oxford University Press; Murray, A. (2007) *The Regulation of Cyberspace: Control in the Online Environment*. Abingdon: Routledge; Murray, A. (2011) Nodes and Gravity in Virtual Space. *Legisprudence*, 5 (2), pp. 195–221; Murray, A. (2008) Symbiotic Regulation. *John Marshall Journal of Computer & Information Law*, 26 (2), pp. 207–228.

respond if they wish to achieve the legitimate authority and rule of law in cyberspace.

*Part I "Law and authority in cyberspace"* is divided into three chapters which are devoted to the three main cyberspace rule makers: i) states, ii) transnational and technical rule makers, iii) communities or private lawmakers. All three chapters describe the source of authority of each aforementioned lawmaker and explore the limits of their authority and its application in cyberspace. Further considerations provide a detailed description of rulemaking of each subject as well as how they communicate these rules to the community and individual cyberspace actors. The authors have built their argumentation upon the distinguished works of *Johnson and Post*<sup>2</sup>, and *Goldsmith*<sup>3</sup> as well as on the relevant case law<sup>4</sup> in considering the state as lawmaker. The first chapter describes the fundamental legal theory for the question of the authority of the state.<sup>5</sup> The authors concluded that the authority of the state has been originally viewed from the perspective of its authority within its own territory; however, this approach is very simplistic and undermines the role of the legitimating community which is in the case of cyberspace significant. In the following chapter, the main focus is on non-state rule makers which are demonstrated by example of subjects having control over technical infrastructure (e.g. *Internet Society*, *Internet Engineering Task Force*, *Internet Architecture Board*, *ICANN*, etc.). The analysis of various theories (e.g. strict constitutional theory, constitutional pluralism, solid/liquid approach) related to legal pluralism in regards to a transnational non-government system is also included.<sup>6</sup> Lastly, the community and its role in cyberspace is examined in-depth. The rule of recognition of validity of claim is stated by the authors as a principle in the online environment and helps to understand the authority of claims of different lawmakers to both the community and individual cyberspace actors.<sup>7</sup> This part concludes that in the case of the online environment, authority of different lawmakers and its rules can be appropriately assessed only for the individual rules of law

---

<sup>2</sup> Johnson, D. R.; Post, D. G. (1996) Law and Borders – The Rise of Law in Cyberspace. *Stanford Law Review*, 48 (5), pp. 1367–1402.

<sup>3</sup> Goldsmith, J. (1998) Against Cyberanarchy. *Chicago Law Review*, 65 (4), pp. 1199–1250.

<sup>4</sup> See pp. 10–11 of the book.

<sup>5</sup> See pp. 14–18 of the book.

<sup>6</sup> See pp. 27–37 of the book.

<sup>7</sup> See pp. 63–66 of the book.

not the law as a whole system. Furthermore, it is pointed out that the role of the community increases in cyberspace.

*Part II* moves forward and focuses on how rules actually work in the online environment. The fourth chapter starts at the very bottom and describes law as a coercive system where the author pointed out the actual control of human behaviour by law. The authors also involved studies of behavioural scientists to support their arguments which provides added value from interdisciplinary perspectives.<sup>8</sup> The subsection 4.2 enters into the considerations of the impact of technology on the behaviour of cyber actors and its potential for application of law. This subsection engages with the familiar work of *Lawrence Lessig*<sup>9</sup> and confronts his work. The authors highlighted that there are two flaws in *Lessig's* thesis: i) misunderstanding of the ways in which the modalities of regulation interact; ii) belief in perfection of control which is possible via code.<sup>10</sup> Following this, an examination of these observations is conducted. The interaction between modalities of regulation is in *Lessig's* view a linear one, while the authors suggested that there is a continuous communication and interaction between them as well as there is a huge impact of the mass of cyberspace users.<sup>11</sup> The perfection of code's control is also examined and refused mainly based on two reasons: i) the nature of design-based controls to regulate without discourse and in an *ex-ante* fashion (presumption that the individual has no social choice to act differently in an environment with design-based controls); ii) the plasticity of code (that code can be rewritten or redesigned). These assumptions are also complemented by other arguments such as the importance and impact of social norms and the market on the regulation of cyberspace and on code.<sup>12</sup> The weakness of code control is demonstrated by several examples (e.g. spam filters, digital rights management, or change of policy of *Facebook*).<sup>13</sup> This in-depth evaluation is very important since *Lessig's* work proves to be very popular in the academic sphere as well as with the general public where some misunderstanding and misinterpretation of *Lessig's* thesis occurs.

---

<sup>8</sup> See pp. 83–84 of the book.

<sup>9</sup> Lessig, L. (1999) *Code and Other Laws of Cyberspace*. New York: Basic Books; Lessig, L. (2006) *Code Version 2.0*. New York: Basic Books.

<sup>10</sup> See p. 88 of the book.

<sup>11</sup> See p. 91 of the book.

<sup>12</sup> See p. 97 of the book.

<sup>13</sup> See pp. 94–99 of the book.

Following the conclusion of previous chapter, the authors have entered into a discussion of the different norms of cyberspace in the fifth chapter. The introduction is devoted to the three theories of social normative compliance, namely rational choice theory, evolutionary theory and social rationality theory. The discussion brings together observations about the community and its role in cyberspace from the previous part with a conclusion that the prevailing importance of social rationality is due to the nature of online communities.<sup>14</sup> Another subsection then describes different sources of norms in the online environment which are identified as norms of service providers, norms based on user interactions and technical norms. In the conclusion to this chapter, the competition between different norms of cyberspace is decided based on authority of different claims and thus the various communities obey their norms via acceptance of such authority. Furthermore, the understanding of such competition of different norms in cyberspace can provide lawmakers with helpful guidance within the lawmaking process to follow the established norms of cyberspace.

The last chapter of *Part II* is focused on a broader perspective covering the topic of regulation and governance in cyberspace. The discussion starts with an understanding of the relationship between technology, regulation and governance while providing a description of *Actor-Network Theory* and *Science and Technology Studies*.<sup>15</sup> In the following, the authors have opened up debates on the fundamental streams regarding governance of cyberspace, cyberlibertarianism and cyberpaternalism.<sup>16</sup> The authors reminded us of the noted works of *John Perry Barlow*<sup>17</sup> and *Johnson and Post*<sup>18</sup>, and confronts it with the *Cyberpaternalist School*<sup>19</sup> and concept of a "*Lex Informatica*"<sup>20</sup>, which argues that there are several new models and sources of rules in the online environment. The debate is completed by *Murray's*

---

<sup>14</sup> See p. 107 of the book.

<sup>15</sup> See pp. 141–144 of the book.

<sup>16</sup> See pp. 144–152 of the book..

<sup>17</sup> Barlow, J. P. (1996) *Declaration of Independence of Cyberspace*. [online] Davos: EFF. Available from: <https://www.eff.org/cyberspace-independence> [Accessed 5 February 2019].

<sup>18</sup> See footnote 2.

<sup>19</sup> Winner, L. (1997) *Cyberlibertarian Myths and the Prospect for Community*. [online] Troy: RPI. Available from: <http://homepages.rpi.edu/~winner/cyberlib2.html> [Accessed 5 February 2019]; Jones, R. (1996) Critique of Barlow's "A Declaration of Independence of Cyberspace". *Extropy: Journal of Transhumanist Solution*, 17 (8).

<sup>20</sup> Reidenbers, J. (1998) *Lex Informatica: The Formation of Information Policy Rules Through Technology*. *Texas Law Review*, 76 (3), pp. 553–593.



concept of the *Network Communitarianism and Symbiotic Regulation* which leans towards soft determinism that sees technology as an enabling rather than a constraining force.<sup>21</sup> *Part II* is closed by concluding remarks on the role of various platforms and gatekeepers in cyberspace. The content of the longest part of the book is very detailed and complex and so, gives readers great insight into the fundamental ideas in jurisprudence as well as famous concepts and considerations in regards to cyberspace. This part forms the core of the book. The theoretical parts are also accompanied by various examples and case law which help to better understand the theoretical background.

The last part of the book is focused on the question of what lawmakers need to do to establish legitimacy of their claims and to achieve the rule of law in the online environment. The seventh chapter concentrates on the issue of legitimacy which in the authors' view cannot fully secure authority in the online environment. However, the rule of legitimacy as itself has the same importance as in the offline environment.<sup>22</sup> The authors pointed out that individual claims can be either legitimate or illegitimate and the level of their legitimacy can vary.<sup>23</sup> The authors viewed the legitimacy of an individual claim from the *Païement* perspective<sup>24</sup> to consider the input, throughput and output aspects of lawmaking when reflecting on the specific nature of cyberspace. The authors concluded that output aspects which are based on the quality of the norms are the most important in terms of legitimacy in cyberspace. This is the very difference between online and offline environments where the legitimacy is primarily derived from constitutions.

In further text, the authors have identified that three factors are important for obedience or disobedience of the law's authority claim: i) the extent to which the law claim is perceived to being addressed to the cyberspace user; ii) how far the law claim is compatible with the rest of the environment in which the cyberspace user acts; iii) the observed fairness and justice of the claim. The first factor is demonstrated by the case C-101/01<sup>25</sup> in connection with the failure to communicate law claims and

<sup>21</sup> See p. 155 of the book.

<sup>22</sup> See p. 173 of the book.

<sup>23</sup> See p. 174 of the book.

<sup>24</sup> Païement, P. (2013) Paradox and Legitimacy in Transnational Legal Pluralism. *Transnational Legal Theory*, 4 (2), pp. 197–226.

<sup>25</sup> Judgement of 6 November 2003, Bodil Lindqvist, C-101/01, EU:C:2003:596.

an analogy with reception theory is highlighted. The crucial element is though communication of such claims for their legitimacy. The compatibility of law claims with the online environment is viewed as the difference between behaviour required and imposed by law and actual reality of the environment in which the law applies.<sup>26</sup> It is concluded that more radical change of behaviours set by laws usually requires stronger justification of their legitimacy. One of the challenges for lawmakers in such a context is to make laws for cyberspace that are congruent with the norms applied to similar physical world activities when the principle of technological neutrality and principle of equivalence are highlighted. Lastly, the fairness and justice of claims are described. The authors addressed the challenge that lawmakers faced in cyberspace as balancing the interest and rights of different groups, especially conflict between the minority and majority.<sup>27</sup> The suggestion is that a lawmaker might prove the legitimacy of a claim if a lawmaker demonstrates and explains how the balance of such rights and interests was evaluated.

The last chapter of the book deals with the concept of the rule of law in cyberspace. The beginning of the chapter provides the reader with a brief overview of various concepts of the rule of law from Fuller<sup>28</sup> to Bingham<sup>29</sup> or Waldron<sup>30</sup>. The authors have produced their own version, the “laundry list” of the rule of law which is examined in the further text. This “laundry list” consists of six principles: i) law must be set forth in advance (be prospective); ii) law must be made public; iii) law must be general; iv) law must be clear; v) law must be stable and certain; vi) law must be applied to everyone according to its terms.<sup>31</sup> In the following text, the authors examined all of aforementioned principles and whether they are established in cyberspace. The text demonstrates several obstacles and difficulties (e.g. the amount of laws, cost of digitisation of information and clarity of laws, to meet these principles in the online environment). In conclusion, the rule of law can be viewed from the perspective of acceptance by cyberspace users rather than application of different legal systems.

---

<sup>26</sup> See pp. 183–194 of the book.

<sup>27</sup> See pp. 195–197 of the book.

<sup>28</sup> Fuller, L. L. (1969) *Morality of Law*. New Haven: Yale University Press.

<sup>29</sup> Bingham, T. (2010) *The Rule of Law*. London: Penguin.

<sup>30</sup> Waldron, J. (2011) The Rule of Law and the Importance of Procedure. In: James E. Fleming (ed.). *Getting to the Rule of Law: NOMOS L*. New York: NYU Press, pp. 3–31.

<sup>31</sup> See p. 206 of the book.

The book as a whole presents a comprehensive discussion of the legal theory as well as findings in regards to cyberspace. While the text leans significantly on a body of literature on the topic, there are interesting and novel conclusions made by the authors which add value for this book. The authors viewed the regulation of cyberspace from perspective of competing rules and authorities. The book emphasises the importance of social norms in cyberspace and considers the ability of an authority to impact those norms. The authors considered that any significant deviation from social norms would impair authority and legitimacy of law claims of rule makers. The key takeaways from the book are the question of sources of authority (states vs. communities), the identification of jurisprudence, the role of social and other norms and their competition with the authority of law, and the necessity to establish legitimacy of law claims of authority. Also, a significant advantage of the book is definitely the language which is very understandable and clear for readers. The book can then serve as a fundamental introduction to the jurisprudence of cyberspace as well as a new perspective on this challenging topic. The book advances the discussion on various aspects of cyberspace and its regulation and provides some conclusions in this area, however, unresolved questions remain. The book therefore can be recommended to the great spectrum of readers with interest in fundamental questions related to the regulation of cyberspace.

## LIST OF REFERENCES

- [1] Barlow, J. P. (1996) *Declaration of Independence of Cyberspace*. [online] Davos: EFF. Available from: <https://www.eff.org/cyberspace-independence> [Accessed 5 February 2019].
- [2] Bingham, T. (2010) *The Rule of Law*. London: Penguin.
- [3] Fuller, L. L. (1969) *Morality of Law*. New Haven: Yale University Press.
- [4] Goldsmith, J. (1998) Against Cyberanarchy. *Chicago Law Review*, 65 (4).
- [5] Johnson, D. R.; Post, D. G. (1996) Law and Borders – The Rise of Law in Cyberspace. *Stanford Law Review*, 48 (5).
- [6] Jones, R. (1996) Critique of Barlow's "A Declaration of Independence of Cyberspace". *Extropy: Journal of Transhumanist Solution*, 17 (8).
- [7] Judgement of 6 November 2003, Bodil Lindqvist, C-101/01, EU:C:2003:596.
- [8] Lessig, L. (1999) *Code and Other Laws of Cyberspace*. New York: Basic Books.
- [9] Lessig, L. (2006) *Code Version 2.0*. New York: Basic Books.

- [10] Murray, A. (2007) *The Regulation of Cyberspace: Control in the Online Environment*. Abingdon: Routledge.
- [11] Murray, A. (2008) Symbiotic Regulation. *John Marshall Journal of Computer & Information Law*, 26 (2).
- [12] Murray, A. (2011) Nodes and Gravity in Virtual Space. *Legisprudence*, 5 (2).
- [13] Paiement, P. (2013) Paradox and Legitimacy in Transnational Legal Pluralism. *Transnational Legal Theory*, 4 (2).
- [14] Reed, C. (2012) *Making Laws for Cyberspace*. Oxford: Oxford University Press.
- [15] Reidenbers, J. (1998) Lex Informatica: The Formation of Information Policy Rules Through Technology. *Texas Law Review*, 76 (3).
- [16] Waldron, J. (2011) The Rule of Law and the Importance of Procedure. In: James E. Fleming (ed.). *Getting to the Rule of Law: NOMOS L*. New York: NYU Press.
- [17] Winner, L. (1997) *Cyberlibertarian Myths and the Prospect for Community*. [online] Troy: RPI. Available from: <http://homepages.rpi.edu/~winner/cyberlib2.html>  
[Accessed 5 February 2019].

DOI 10.5817/MUJLT2019-1-7

3D PRINTING AND BEYOND:  
INTELLECTUAL PROPERTY AND REGULATION.  
MENDIS, D.; LEMLEY, M.; RIMMER, M. (EDS.).\*

by

PAVEL LOUTOCKÝ\*\*

*Mendis, D.; Lemley, M.; Rimmer, M. (eds.). (2018) 3D Printing and Beyond: Intellectual Property and Regulation. Cheltenham: Edward Elgar Publishing, 432 p.*

Even though the technology connected with 3D printing provides new development, it cannot be considered as anything purely original in the area of intellectual property law;<sup>1</sup> it just brings more possibilities and makes creating of any imaginable shapes easier and more accessible.

*“3D printing [has] two essential characteristics [...]: It radically reduces the cost of production and distribution of things, and it separates informational content of those things (the design) from their manufacture. [...] The role of IP in such a world is both controverted and critically important.”<sup>2</sup>*

Even if the technology itself in this area did not bring anything purely new, the legal point of view is constantly struggling with it, it hardly finds

---

\* The review was written within the project MUNI/A/1006/2018 (Law and Technology VII).

\*\* loutocky@law.muni.cz, legal specialist and post doc at the Institute of Law and Technology of the Faculty of Law, Masaryk University, Brno, the Czech Republic. He is also Head of the Legal Department of the Technology Transfer Office of Masaryk University. He also works as a lawyer at the Centre for Excellence for Cybercrime, Cyber Security and Critical Information Infrastructure Protection at Masaryk University.

<sup>1</sup> For the overview of some relevant literature and description of the history of regulation and possible approaches see e.g. Tran, J. L. (2015) The Law and 3D Printing. *The John Marshall Journal of Information Technology & Privacy Law*, 31 (4), p. 510 et seq.

<sup>2</sup> See p. 31 of the book.

proper legal analogies<sup>3</sup> and moreover, there is a constant lack of decent literature in this area despite the fact that we have been already talking about this topic for a few decades.<sup>4</sup>

This improper situation and also the important role of IP rights was understood also by the authors of the book *3D Printing and Beyond: Intellectual Property and Regulation*, who in 2015 set out to create a collection focused on the issue of 3D printing with the main task to think about the technological challenges associated with this area in the long term horizon and to change the rigid approach that is still evident.<sup>5</sup> The book was published in 2019 by *Edward Elgar Publishing*.

The need for a quick change of the approach to 3D printing and revision of legislation especially in the area of IP rights has been understood in various countries. Whole structure of the book is focused only on three territories – the United Kingdom, the United States of America and Australia. The editors justify the choice of those three territories in the introductory chapter by the fact, that (i) these three selected countries are active in development of 3D printing and they position themselves as world leaders,<sup>6</sup> (ii) these countries are supporting progressive IP policy reforms in the legislation of 3D printing and additive manufacturing technologies and (iii) these countries share the common law tradition.<sup>7</sup> Even though such an explanation is understandable, the choice of those three countries and the argument on it does not fully stand in our opinion. It seems more that these three territories have been selected mainly based on the fact, that the editors (and overall the authors) have somehow been related to this area. The editors have unfortunately did not consider deeper

---

<sup>3</sup> The importance of legal revision in the area of 3D printing was highlighted recently by the European Parliament in Draft report on three-dimensional printing, a challenge in the fields of intellectual property rights and civil liability in the beginning of year 2018 (see Committee on Legal Affairs. European Parliament. (2018) Draft report on three-dimensional printing, a challenge in the fields of intellectual property rights and civil liability (2017/2007(INI)). [online] Available from: [http://www.europarl.europa.eu/meetdocs/2014\\_2019/plmrep/COMMITTEES/JURI/PR/2018/06-20/1146633EN.pdf](http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/PR/2018/06-20/1146633EN.pdf) [Accessed 9 May 2019]).

<sup>4</sup> *Yanisky-Ravid and Kwan* are arguing that legal environment was and still is being caught totally unprepared. This doesn't by their opinion mean that 3D printing should bring new concepts, some legal instruments however must adapt to new situations (see Yanisky-Ravid, S. and Kwan, K. S. (2017) 3D Printing the Road Ahead: The Digitization of Products When Public Safety Meets Intellectual Property Rights – A New Model. *Cardozo Law Review*, 38 (3), pp. 921 and 936 et seq).

<sup>5</sup> See p. 2 of the book.

<sup>6</sup> Between the other countries the editors mention Germany, Japan, South Korea or China (see p. 8 of the book).

<sup>7</sup> See p. 8 of the book.

explanations which are contradictory to the mentioning that the book offers holistic insight into IP implications of 3D printing.<sup>8</sup> This however only indicates that the methodology of the choice was not well chosen or justified, but it cannot in itself indicate that the publication is of poor quality. On the contrary. From a general point of view, a relatively careful selection of authors and areas of their interest is clearly visible in the book. Those are described later.

Before the book starts to assess the particularities in the above-mentioned territories, *Lemley* introduces the main impact of 3D printing – IP in a world without scarcity. The main intent of *Lemley* is to introduce the fact that

*“3D printing exacerbates the public goods problem of IP theory by making it much cheaper to imitate than to create.”<sup>9</sup>*

He stresses out that similar arguments are used when talking about the impact of the Internet on IP law.<sup>10</sup> What we then see as something additional in 3D printing is the material aspect of the technology. *Lemley* then broadly concludes on the topic of scarcity, that there is a fight of IP owners for scarcity (limited amount of products), which will be in his opinion lost. He stresses out that IP owner’s loss is (mostly) innovation’s success.<sup>11</sup> He thus believes that legal regulation should be more open and not protective only towards the IP owners. This chapter thus serves as a theoretical introduction of what 3D printing brings to the classical concepts of IP right. The author correctly identified the similarities to the issues we are dealing with the Internet regulation, thus it is logical outcome.

The first part of the book focuses on the issues of 3D printing connected to the territory of the United Kingdom. The area is opened by the article ‘Back to the future’? *From engravings to 3D printing – implications for UK copyright law*, which focuses on the history of regulation on 3D printing in the UK and its practical implications. *Mendis* sees the biggest issues in the question if new and innovative regulation is really needed. This question is not clearly answered. However the author states that

---

<sup>8</sup> Ibid.

<sup>9</sup> See p. 39 of the book.

<sup>10</sup> Ibid.

<sup>11</sup> See p. 50 of the book.

clarification of the legal mechanisms, better enforcement and a new approach to business models is the key to support further development of 3D printing.<sup>12</sup> Margoni in the article *Design rights and 3D printing in UK: balancing innovation and creativity in a (dis)harmonised and fragmented legal framework* specifies some reforms of legal approaches and stresses the necessity to establish a better relationship between copyright and design protection. Following two articles *Digital trade mark infringement and 3D printing implications: what does the future hold?* by Hong and Bradshaw and *3D printing and patent law – a UK perspective: apt and ready?* by Mimler are both analysing the readiness of industrial protection mechanisms in connection with 3D printing. While the authors of the first of these articles argue in favour of the existing regulation, which they believe is ready for the advancement of modern technology,<sup>13</sup> the situation is rather different in the case of patent law. Mimler highlights the necessity to protect the role of intermediaries offering space to share the blueprints as they seem to be beneficiary to the society. He is also quite sceptical about massive patent infringement by regular users as the technological possibilities of 3D printing are not that precise to copy often complicated inventions protected by patent.<sup>14</sup> The last article in the first chapter *Transformative technologies and responsive legal scholarship* by Brownsword highlights the important role of pragmatic approach while regulating issues of 3D printing. This article is rather theoretical and basically follows the methodological approach which is generally used when dealing with legal regulation of modern technologies. He thus also mentions the need for involvement of smart rules and approach based on the empirical experience, not only on the basis of impression.<sup>15</sup>

The second part is focused on the legal issues of 3D printing in the USA. The first article *3D printing and US copyright law: implications for software, enforcement and business strategies* by Mennel and Vacca identifies main issues in copyright law focused mainly on software and law enforcement. They argue, that when applying legal regulation, we can use some analogies, but the biggest challenge is, in fact, that the area brings whole new opportunities to product manufacturing and design business, consumers,

<sup>12</sup> See pp. 76–77 of the book.

<sup>13</sup> The authors are mainly focusing on practical process of 3D printing which is realized through vector CAD files.

<sup>14</sup> See p. 130 et seq. of the book.

<sup>15</sup> See p. 152 et seq. of the book.



designers, etc. Such a relatively simple statement is however supported by some practical examples of how the transformative power of modern technologies (and 3D printing) works together with classical legal mechanisms (such as enforcement issues in connection with Digital Millennium Copyright Act or DRM protection).<sup>16</sup> Following two articles *Integrating a classical tool for a modern challenge: US design patents implication for 3D printing* by Ferrill, MacKichan, McKinley and Horn and *Remedies for digital patent infringement: a perspective from the USA* by Holbrook are both focused on patent protection and design patents. The authors of the first article argue for practical applicability of design patents in case of protecting graphical user interface and predict the rise of such instrument in the protection of the rights.<sup>17</sup> In the second article focused on patent infringement the author tries to provide the first effort at predicting how the remedies work in this area and states that

*“when digital downloading’s impact on the copyright system is a harbinger of what the patent system will face, the difference between the two regimes means that the patent system will struggle even more to combat digital infringement”*.<sup>18</sup>

Desai in his article *How 3D printing disrupts trade dress protection* then deals with the dress protection and points out that the ability to make something easy with 3D printing is not the same as guaranteeing that this good is made with safe materials – so the companies are by their mass production guaranteeing the quality and the source. 3D printing thus pushes (and will push) companies to improve the overall quality of mass-produced goods.<sup>19</sup> The last contribution to the chapter by the same author deals with the issue of *How democratized production challenges society’s ability to regulate*. He concludes that

*“democratizing technology can unleash great benefits while also removing the chance of meaningful management and regulation by society”*.<sup>20</sup>

<sup>16</sup> See p. 170 et seq. of the book.

<sup>17</sup> See p. 199 et seq. of the book.

<sup>18</sup> See p. 232 et seq. of the book.

<sup>19</sup> See p. 214 et seq. of the book.

<sup>20</sup> See p. 250 et seq. of the book.

This, however, cannot be taken as negative effect leading to overregulation and then to suffocation of newly developing technology; the right balance is needed. *Desai* is however not indicating the level of regulation. Thus, we are left without the answer where the balance is needed – this is, however, unfortunately, the outcome of many academic works which are dealing with the issues of regulation of modern technologies and the enforcement.

The last big chapter is focused on the territory of Australia and follows a similar pattern as in previously introduced chapters. This chapter is, similarly to the previous chapters, opened with general article *Makers Empire: Australian copyright law, 3D printing and the 'Ideas Boom'* by Rimmer. He stresses out that

*"Australia's copyright exceptions for libraries, galleries, archives, and museums are anachronistic and ill-adapted for an age of 3D printing,"*<sup>21</sup>

thus there is only limited interest in investments to 3D printing.<sup>22</sup> This conclusion is also supported by *Berger* in the article *'Substantial similarity' under Australian design law* in connection with design regulation. He also adds that even though the rise of 3D printing technology has some disruptive impacts on the authors/producers, the positive impacts must be assessed more carefully.<sup>23</sup> *Scardamaglia* in connection with trademark protection relatively simply concludes that it is probably more important

*"to pause and reflect on some more troubling aspects of trade mark law that have long warranted further attention, but have not yet received it..."*<sup>24</sup>

in the article *Trade mark controversies in 3D printing*. We have to agree with her on the point that keeping the pragmatic approach and to mute hysteric overregulation<sup>25</sup> is the key for this industry. Basically, the same idea is followed more generally with concluding article of the chapter called *Don't believe the hype? Recent 3D printing developments for law and society* by *Daly*, where she stresses that in the current state 3D printing is not prevalent enough yet to be disruptive for law or for society (despite the potential).<sup>26</sup> As each chapter of the book is trying to offer the place to similar areas

<sup>21</sup> See p. 293 et seq. of the book.

<sup>22</sup> Ibid.

<sup>23</sup> See p. 302 et seq. of the book.

<sup>24</sup> See p. 324 of the book.

<sup>25</sup> Ibid.

<sup>26</sup> See p. 359 et seq. of the book.

of the interest, *Nielsen and Nicol* are focusing on patent protection in the article *The reform challenge: Australian patent law and the emergence of 3D printing*. Even though they are supporting legislative changes in the area which were made by Australian legislators,<sup>27</sup> they are pointing out that it was not done conceptually, and the main problem is that the legislators did not focus on infringement of patent law. This thus leads to problematic applicability of described legal regime and difficult (if even possible) enforcement.<sup>28</sup>

It is apparent from the above-described that the individual chapters within the three mentioned territories do not overlap as much. The authors rather focused on the topics that were more suitable to them than to follow general pattern of the book. Thus, the areas specifically examined in some territory are not always covered in the other, which leads to some fragmentation of the book as a whole and overall impression that the book does not “hold together” (the book is giving the impression that it is more of assemblage of essays). Thus, the reader’s orientation in the text can be in some parts more difficult. However, the contributions themselves are of sufficient quality, so if the reader is looking for information about 3D printing in a given territory, the book will offer him a nice overview. This is also supported by the fact that the articles were not written only by academics but also by practising lawyers.

The whole book is after three big parts enclosed with the article from the editors called *The future of printcrime: intellectual property, innovation law, and 3D printing*. They are mainly concluding previous findings and add valuable chapter on future research. Unfortunately, they are however focusing only on new areas where 3D printing can be used, such as food printing, robot law, medicine, space missions (and many other areas) without any deeper focus on legal issues (which is somewhat the anticipation from the legal text). The last chapter more focuses on the possibility of technology and not the possibility of legal regulation, which would be more expected by the reader.<sup>29</sup> The editors are only concluding that it is always necessary to balance legal regulation with a possible limitation of the technology, which is however nothing new. We think that it is not the era of assessment of legal regulation in the area of 3D

<sup>27</sup> See more on the legislation at p. 340 et seq. of the book.

<sup>28</sup> See p. 343 et seq. of the book.

<sup>29</sup> See p. 386 et seq. of the book.

at the moment (in our opinion general assessment has been done sufficiently for last decade), but we should move to the point of more exact proposals and improvements of the legal framework related to 3D printing. This hesitant approach to propose anything “revolutionary” is apparent from the whole book and we see it as the wasted potential of the publication. This should however not imply that the book itself does not bring anything new – what we are trying to say is that it should have possibly brought a bit more especially in terms of more specific proposals how to contribute to appropriate regulation of the area of 3D printing.

## LIST OF REFERENCES

- [1] Draft report on three-dimensional printing, a challenge in the fields of intellectual property rights and civil liability in the beginning of year 2018. Committee on Legal Affairs. European Parliament. (2018) Draft report on three-dimensional printing, a challenge in the fields of intellectual property rights and civil liability (2017/2007(INI)). [online] Available from: [http://www.europarl.europa.eu/meetdocs/2014\\_2019/plmrep/COMMITTEES/JURI/PR/2018/06-20/1146633EN.pdf](http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/PR/2018/06-20/1146633EN.pdf) [Accessed 9 May 2019].
- [2] Tran, J. L. (2015) The Law and 3D Printing. *The John Marshall Journal of Information Technology & Privacy Law*, 31 (4).
- [3] Yanisky-Ravid, S. and Kwan, K. S. (2017) 3D Printing the Road Ahead: The Digitization of Products When Public Safety Meets Intellectual Property Rights – A New Model. *Cardozo Law Review*, 38 (3).



**MUJLT Official Partner (Czech Republic)**



ROWAN LEGAL, advokátní kancelář s.r.o.  
[www.rowanlegal.com/cz/](http://www.rowanlegal.com/cz/)

Cyberspace 2018 Partners



Vodafone Czech Republic  
[www.vodafone.cz](http://www.vodafone.cz)



Wolters Kluwer

Wolters Kluwer ČR  
[www.wkcr.cz](http://www.wkcr.cz)

*Zákony pro lidi.cz*

Zákony pro lidi - AION CS  
[www.zakonyprolidi.cz](http://www.zakonyprolidi.cz)



**CODEXIS®**

CODEXIS - ATLAS consulting  
[www.codexis.cz](http://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

<b>Robert Müller-Török:</b> The Principles Established by the Recommendation CM/Rec(2017)5 on Standards for E-voting Applied to Other Channels of Remote Voting .....	3
<b>Maria Dymitruk:</b> The Right to a Fair Trial in Automated Civil Proceedings .....	27
<b>Kristjan Kikerpill, Andra Siibak:</b> Living in a Spamster's Paradise: Deceit and Threats in Phishing Emails .....	45
<b>Papawadee Tanodomdej:</b> The Tallinn Manuals and the Making of the International Law on Cyber Operations .....	67
<b>Nelli Golubeva, Kristina Drogoziuk:</b> Web-page Screenshots as an Evidence in Civil Procedure of Ukraine .....	87

## LIST OF BOOK REVIEWS

<b>Dominika Galajdová:</b> Rethinking the Jurisprudence of Cyberspace. Reed, C.; Murray, A. ....	115
<b>Pavel Loutocký:</b> 3D Printing and Beyond: Intellectual Property and Regulation. Mendis, D.; Lemley, M.; Rimmer, M. (eds.). ....	123