MASARYK UNIVERSITY JOURNAL OF LAW AND TECHNOLOGY

VOLUME 14 | NUMBER 1 | SUMMER 2020 | ISSN 1802-5943

PEER REVIEWED

UNIVERSITAS MASARYKIANA BRUNENSIS • FACULTAS IURIDICA •

CONTENTS:

VASIU I | VASIU L | SLUSSAREFF | ŠISLER
OSMANI | ŻOK | NOVOTNÁ | RAMEŠOVÁ

www.mujlt.law.muni.cz

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

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

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

licensed as peer-reviewed scientific journal by the Research and Development
Council of the Government of the Czech Republic
listed in HeinOnline (www.heinonline.org)
listed in Scopus (www.scopus.com)
reg. no. MK ČR E 17653

MASARYK UNIVERSITY JOURNAL OF

LAW AND TECHNOLOGY

VOLUME **14** | NUMBER **1** | SUMMER **2020**

LIST OF ARTICLES

DOI 10.5817/MUJLT2020-1-1

CYBER EXTORTION AND THREATS: ANALYSIS OF THE UNITED STATES CASE LAW

by

IOANA VASIU[*], LUCIAN VASIU[**]

This article presents an analysis of the cyber extortion and threats cases brought to the United States courts. The inquiry employed content analysis to identify important elements and attributes and answers research questions concerning essential attributes, legal elements, and how do the courts interprets these offenses. The article extends the understanding of this phenomenon by providing a thorough discussion of the conceptual issues and characteristics and an analysis of the most important litigation aspects, such as intent, true threats, sentencing, and the insanity defense. The article concludes with recommendations for stakeholders, to more effectively address the phenomenon.

KEY WORDS

Cybercrime, Extortion, Insanity, Intent, Malware, Sentencing, Speech, True Threats

[*] ioanav3@yahoo.com, Prof. Dr., Faculty of Law; Coordinator of the *BBU Faculty of Law's Cybercrime Research Unit*; member of the *BBU Scientific Council*; member of the *Board of Directors* of the *International Association of Penal Law* (2014–2024); and external affiliated member of the *Ostrom Workshop Program on Cybersecurity and Internet Governance, Indiana University*. Expert with the *European Commission* and the *UNDP Romania*; partner and lead researcher on several projects funded by the *European Commission, Dutch Council for the Judiciary* and other entities; co-Chair of the *Management and Delivery of Justice Group* of the *European Group of Public Administration*; and keynote speaker or moderator at numerous professional events organized by prestigious organizations, such as *OECD* or *UNDP/RCPAR*. Her research focuses on cybercrime nature, prevention, and litigation.

[**] lvcianvs@yahoo.com, PhD, MBA, computer scientist, expert in cybercrime prevention and information systems security.

1. INTRODUCTION

"Cyberviolence" involves the use of information systems to

> *"cause, facilitate, or threaten violence against individuals that results in, or is likely to result in, physical, sexual, psychological or economic harm or suffering and may include the exploitation of the individual's circumstances, characteristics or vulnerabilities."*[1]

"Cyberviolence" comprises numerous offenses, among these cyber extortion and threats represent important categories.

Cyber extortion and threats are acts of

> *"conditional speech intended to influence or gain compliance from a target recipient."*[2]

These communications can be effective in gaining the *"feeling of power and control"*[3] over victims.[4] These offenses cover a range of forms, including intimate partner violence (IPV), violence against women and girls (VAWG), cyber dating abuse (CDA) and so on.

It is difficult to quantify the full extent of the phenomenon; however, as it produces significant negative personal, economic, and societal consequences, is regarded as one that needs to be more effectively addressed.[5] This article aims to present an analysis of the phenomenon's

[1] Cybercrime Convention Committee (T-CY). (2018) *Mapping Study on Cyberviolence*. [online] Strasbourg: Council of Europe, 5, Available from: https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914 [Accessed 1 July 2019].

[2] Spitzberg, B.H. and Gawron, J.M. (2016) Toward Online Linguistic Surveillance of Threatening Messages. *Journal of Digital Forensics, Security and Law*, 11, p. 47.

[3] *United States v. Killen.* (2018) No. 15-15001 (11th Cir.), 29 March.

[4] *Fontana v. United States*. (2020) No. 14-20141 (E.D. Mich.), 17 April; Bumb, M. L. (2017) Domestic Violence Law, Abusers' Intent, and Social Media: How Transaction-Bound Statutes Are the True Threats to Prosecuting Perpetrators of Gender-Based Violence. *Brooklyn Law Review*, 82 (2), pp. 917–960.

[5] See, e.g. Van Der Wilk, A. (2018) *Cyber violence and hate speech online against women*. PE 604.979. Brussels: European Parliament. Available from: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf [Accessed 1 July 2019]; U.S. Department of Justice. (2016) *The National Strategy for Child Exploitation Prevention and Interdiction*. [online] Washington: U.S. Department of Justice. Available from: https://www.justice.gov/psc/file/842411/download [Accessed 20 October 2019]; Women and Gender Equality Canada. (2019) *New federal investment will help end cyberviolence.* [press release] 27 August. Available from: https://www.canada.ca/en/status-women/news/2019/08/new-federal-investment-will-help-end-cyberviolence.html [Accessed 3 December 2019]; European Institute for Gender Equality. (2017) *Cyber violence against women and girls*. Available from: https://eige.europa.eu/sites/default/files/documents/cyber_violence_against_women_and_girls.pdf [Accessed 3 December 2019]; Peterson, J. and Densley, J. (2017) Cyber Violence: What Do We Know and Where Do We Go From Here?. *Aggression and Violent Behavior*, 34, pp. 195–196; Cybercrime Convention Committee (T-CY). (2018) *Mapping*

attributes and of the most important litigation aspects. The analysis is based on a large corpus of data, consisting of several hundred cases brought to the U.S. courts. This inquiry employed content analysis to identify and group important elements and issues. The article answers the following research questions: What are the attributes of the phenomenon? What are the elements of cyber extortion and threats that the legal system addresses? How do the courts interprets these crimes?

The article proceeds in three Sections. The next Section discusses the attributes of the cyber extortion and threats phenomenon. Section 3 outlines the legal framework for these offenses. Section 4, based on the comprehensive study of cases brought to federal courts in violation of the federal threat statute, 18 U.S.C. § 875 (c) & (d), presents an analysis of important litigation aspects: intent, "true threats", sentencing aspects, and the insanity defense. The article concludes with recommendations for stakeholders, to more effectively address the phenomenon.

2. ATTRIBUTES OF THE PHENOMENON

2.1. THREATS

A "threat" is

> *"an avowed present determination or intent to injure presently or in the future."*[6]

There are two main forms of threats: interpersonal and impersonal. Interpersonal threats, which can be encountered in cases of direct relations, in a variety of contexts, are transmitted with a view to obtain recipient's compliance. Impersonal threats target groups of people (for instance, members of law enforcement agencies, civil liberties organizations, minority groups, etc.)[7] or leaders, and can be encountered in cases of perceived

Study on Cyberviolence. T-CY(2017)10. Strasbourg: Council of Europe, 4, Available from: https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914 [Accessed 1 July 2019]; European Union Agency for Law Enforcement Cooperation (Europol). (2017) *Internet Organised Crime Threat Assessment*. The Hague: Europol. Available from: https://www.europol.europa.eu/sites/default/files/documents/iocta2017.pdf [Accessed 1 June 2018].

[6] *United States v. Alkhabaz.* (1997) 104 F.3d 1492 (6th Cir.), 29 January.

[7] See, e.g. *United States v. Jordan.* (2017) No. 16-CR-93-FPG-HKS-1 (W.D.N.Y.), 24 October (the defendant posted on *Facebook* the message *"Lets Start Killin Police Lets See How Dey Like It."*); *United States v. Carrillo.* (2020) No. 1: 19-cr-01991 KWR (D.N.M.), 8 April (the defendant, via *Facebook*, communicated a threat to injure ACLU personnel); *United States v. Doggart.* (2020) 947 F.3d 879 (6th Cir.), 15 January (the defendant planned to destroy a religious community in New York state).

distress or coercion, created by certain pressures (e.g. political, economic, or social).

Threats can be also be categorized as reactive, when responding to real or perceived events or threats (for example, as retaliation[8] or reaction for the loss of social status), and proactive, when attempting to achieve certain goals (to "align" the threateners' desires or wishes and the actual reality).[9] A subcategory of the latter is the infliction of fear for threateners' own gratification or enjoyment.[10]

Threats usually aim to determine the recipient to comply with certain requests, rather than actually engaging with them in the course of action described. Nevertheless, these threats have a complex relationship to actual harm. Such communications can inflict

> *"psychological harm on the listener in the direct manner that a physical attack would inflict physical harm."*[11]

Further, the harm

> *"may be real whether or not the individual speaker intended his speech to be received as a threat, and regardless of whether the speaker actually intended to carry out such a threat."*[12]

Cyber extortion and threats are not new offenses. However, cyberspace and social media platforms, in particular, make much more difficult to determine threateners' actual state of mind and what are the actual capabilities of the threateners with respect to carry out the threats. Additionally, technology permits the transmission of threats using a false identity or the identity of another person,[13] and to reach a large number

[8] *United States v. Telfair.* (2020) No. 19-CR-270 (E.D.N.Y.), 3 February (the defendant threatened a witness who testified against the defendant's brother in a criminal case).

[9] See Criminal Complaint, *United States v. Swarbrick.* (2018) Case 3:18-MJ-1214 (M.D. Tenn.), 19 September. Available from: https://www.courthousenews.com/wp-content/uploads/2018/09/EricSwarbrick.pdf (in an attempt to meet with a famous singer, the defendant sent tens of threatening letters and e-mails) [Accessed 1 June 2019].

[10] See, e.g. *United States v. Haileselassie.* (2019) No. 18-1343 (8th Cir.), 10 June (the defendant made bomb threats at a community college).

[11] Han, D.S. (2014) The Mechanics of First Amendment Audience Analysis. *William and Mary Law Review*, 55, pp. 1647, 1659.

[12] Romney, J. (2012) Eliminating the Subjective Intent Requirement for True Threats in United States v. Bagdasarian. *Brigham Young University Law Review*, 2012, pp. 639, 653.

[13] See *United States v. Turrella.* (2012) No. 10-30051 (9th Cir.), 15 March.

of people, potentially amplifying the fear or the anxiety.[14] Even more disturbing, threats can be of the anti-social type, transmitted anonymously,[15] and could reach people (online viewers or followers), who, in turn, may potentially be encouraged or willing to fulfill the call for violent actions, thus producing a spread or proliferation effect.

The communication of threats can be brought about by numerous motivational states, rational or irrational. The threatening content can regard personal honor or dignity, incitement to discrimination, or violent actions against certain people or groups of people. To achieve their objective, threateners use a range of threats: to injure the property, reputation, or the person of another, to kidnap or kill the victims.

The language employed in the communications can be clear, but also implied, veiled, or cryptical.[16] In a number of cases, the language used is truly malignant, sadistic and extreme. To illustrate the point through a few examples, the defendant in *United States v. Wheeler* threatened to

> *"kill cops[,] drown them in the blood of thier [sic] children, hunt them down and kill their entire bloodlines;"*[17]

in *United States v. Cain*, the defendant, in brutal terms, threatened to kill his ex-wife, her mother and her new boyfriend, to send to members of ex-wife's family videotapes showing the victim engaged in sexual acts, and to rape victim's daughter;[18] in *United States v. Heineman*, the defendant, a white supremacy sympathizer, sent to the victim e-mails containing reprehensible statements, such as

> *"slay you, by a bowie knife shoved up into the skull from your pig chin you choke, with blood flooding in your filthily treasonous throat!;"*[19]

in *United States v. Williams*, the defendant threatened to kill a judge,

[14] See Criminal Complaint at 2 et seq., *United States v. Bishop.* (2018) Case 118MJ24LDA (D.R.I.), 23 January (defendant sent hundreds of threatening e-mails to his former girlfriend, her family, and three state prosecutors, victims expressing "extreme fear for their safety").

[15] See, e.g. *United States v. Bagdasarian.* (2011) 652 F.3d 1113 (9th Cir.), 19 July (on a *Yahoo* message board, the defendant posted threats anonymously).

[16] See, e.g. Memorandum Opinion and Order at 18, *United States v. White.* (2010) Criminal Action No. 7:08-CR-00054 (W.D. Va.), 20 January.

[17] See, e.g. *United States v. Wheeler.* (2019) Criminal Case No. 12-cr-0138-WJM (D. Colo.), 9 July.

[18] *United States v. Cain.* (2018) No. 1: 16-cr-00103-JAW (D. Me.), 1 June.

[19] *United States v. Heineman.* (2014) 767 F.3d 970, 972 (10th Cir.), 15 September.

> *"sodomize the corpse, chop it into pieces, and mail one piece of the corpse to the courthouse each week."*[20]

The inclusion of unsettling images, as means to make the "message" more powerful, can also be noted: in *United States v. Vandevere*, for instance, the defendant sent a "tweet" that contained a lynching picture.[21]

There are numerous threat communication means, mainly e-mail;[22] telephone;[23] online call spoofing services;[24] and social media platforms. In *United States v. Michael*, to illustrate the latter, the defendant posted on *Facebook* threats to *"kidnap and injure DEA agents and personnel"* and that it's

> *"time we answered their crimes with bloodshed and torture."*[25]

In *Commonwealth v. Knox*, for another example, the appellant recorded and uploaded to *YouTube* a rap song titled *"F--k the Police"*.[26] The song's lyrics expressed hatred and contained

> *"descriptions of killing police informants and police officers."*[27]

The court held that the

> *"threats to the officers were real, specific and violent, with nothing of record to indicate that the threats should not be taken seriously"*

[20] *United States v. Williams.* (2018) No. 17-2454 (8th Cir.), 26 October.

[21] *United States v. Vandevere.* (2019) No. 1: 19-cr-63-MOC (W.D.N.C.), 16 September.

[22] See, e.g. *United States v. White.* (2017) Criminal Action No. 7: 13CR00013 (W.D. Va.), 31 May (the defendant sent several e-mails, threatening to injure his ex-wife, if she did not send him "alimony" payments); *United States v. Gillenwater.* (2014) 749 F.3d 1094 (9th Cir.), 11 April (defendant sent an e-mail threatening the life of another); *United States v. McCrudden.* (2015) No. CR-11-061 (DRH) (E.D.N.Y.), 16 March (defendant sent an e-mail claiming that he hired people to kill the victim).

[23] See, e.g. Criminal Complaint, *United States v. Lisnyak.* (2015) Case No. 15-04179MJ-PCT-DMF (D. Ariz.), 16 July; *United States v. Champ, United States v. Wood.* (2006) 459 F. Supp. 2d 451 (E.D. Va.), 29 September.

[24] See, e.g. Criminal Complaint, *United States v. Kadar.* (2017) Case No. 6:17-mj-1361 (M.D. Fla.), 4 April at 4.

[25] *United States v. Michael.* (2012) No. 2: 12-cr-1-WTL-CMM (S.D. Ind.), 9 October.

[26] *Commonwealth v. Knox.* (2018) 190 A.3d 1146, 1149 (Pa.), 21 August.

[27] Op. cit., at 1149.

or that the defendants would not be able to *"carry them out."*[28] The fervency of threats can be increased through repeat communications and the use of multiple means.[29]

2.2. EXTORTIONATE THREATS

"Extortion" encompasses numerous forms and has multiple definitions. The Florida law definition, for instance, includes, among other things, the use of threats to injure a person's reputation, to expose another to disgrace, or to reveal *"any secret affecting another"* for the purpose of compelling the victim

> *"to do any act or refrain from doing any act against his or her will."*[30]

According to the *U.S. Sentencing Guidelines (U.S.S.G.),* "extortion" refers to

> *"obtaining something of value from another by the wrongful use of (A) force, (B) fear of physical injury, or (C) threat of physical injury."*

"Something of value" includes money, property, an advantage, or even a sexual relationship.[31]

Extortionate threats cover the making or implying of threats that intend to induce the belief that victim's power, wealth, social standing, personal or job security, or self-esteem are or could be endangered. The extortionist must use threats with a view to "obtain" or "acquire" property, not just to deprive or dispossess the victim of it.[32] An important element of extortion is

> *"that of obtaining property from another 'with his consent' induced by wrongful use of threats."*[33]

Professor Steven Shavell, the Director of the *John M. Olin Center for Law, Economics, and Business* at the *Harvard Law School,* explains that threateners

[28] Op. cit., at 1174.

[29] See Criminal Complaint, *United States v. Leach.* (2017) Case No. 2:17mj-44-1 (D. Vt.), 21 April (the defendant transmitted repeated death threats, via *Facebook*, e-mail, and telephone).

[30] 2019 Florida Statutes 836.05 Threats; extortion. In English. Available from: http://www.leg.state.fl.us/Statutes/index.cfm?App_mode=Display_Statute&URL=0800-0899/0836/Sections/0836.05.html [Accessed 1 July 2019].

[31] *United States v. Petrovic.* (2012) 701 F.3d 849 (8th Cir.), 13 December.

[32] *Scheidler v. National Organization for Women.* (2003) 537 U.S. 393, 26 February.

[33] Green, S.P. (2005) Theft by Coercion: Extortion, Blackmail, and Hard Bargaining. *Washburn Law Journal,* 44, p. 553 (the consent is *"coerced when it is obtained by threat or force"*).

must make credible threats, so that the victims would believe that there is

> *"significant chance that the threat will be carried out if and only if he does not accede to it,"*

and, if the threateners are rewarded, the victim

> *"will gain thereby and not merely set himself up for further threats."*[34]

Nevertheless, as seen in a number of cases, the victims that gave in to extortionate threats are likely to be suffer continued, repeated demands from the perpetrators, a situation that can become a prolonged or extended dominance-subordination relationship.

Threats to commit an unlawful act amount to "extortion" if the threat *"is to be carried out in the future."*[35] To extort their victims, perpetrators may threaten to, for instance, damage the victim's property or reputation (for example, by releasing damaging photos and videos[36] or libelous material), or even falsely accuse the victim.[37] Some of the main forms of extortion include the influence of justice, sextortion,[38] sexual coercion and extortion (SCE), reputation damage,[39] etc. In *White v. United States*, for illustration, the defendant, with the intent to extort the dismissing of the state charges against members of a white supremacist group, threatened to *"kidnap, rape, and murder"* a judge, the State Attorney, and a federal agent, to behead them, and to paint on walls with their blood.[40]

In a number of cases, as the result of the extortion of victims, perpetrators aimed to obtain self-generated explicit materials (SGEM) or self-generated indecent material (SGIM).[41] In *United States v. Fontana*, for example, the defendant, posing as a minor boy on a chat website, asked

[34] Shavell, S. (1993) An Economic Analysis of Threats and Their Illegality: Blackmail, Extortion, and Robbery. *University of Pennsylvania Law Review*, 141, p. 1878.

[35] Berman, M.N. (1998) The Evidentiary Theory of Blackmail: Taking Motives Seriously. *University of Chicago Law Review*, 65, pp. 795, 853.

[36] See *United States v. Gomez.* (2020) No. 18-12089 (11th Cir.), 14 February.

[37] *United States v. Avenatti.* (2020) No.(S1) 19 Cr. 373 (PGG) (S.D.N.Y.), 14 January.

[38] This form of extortion is characterized by threats that aim to humiliate the victim by posting online compromising sexual images or recordings. For instance, the distribution of videos, unless the suspects receive monetary compensation, see, e.g. *In the Matter of Search of a Residence in Oakland.* (2019) Case No. 4-19-70053 (N.D. Cal.), 10 January.

[39] See *United States v. Coss.* (2012) 677 F.3d 278 (6th Cir.), 16 April: threatening to injure someone's reputation, the threat must be "wrongful" but it need not be independently illegal.

[40] *White v. United States.* (2019) No. 6: 17-cv-689-Orl-28GJK (M.D. Fla.), 14 February.

[41] *United States v. Killen.* (2018) No. 15-15001 (11th Cir.), 29 March.

a minor female to take off her shirt.[42] Without the victim's knowledge, the defendant recorded the act and subsequently threatened to publish online of the recording, in order to "take over" the victim's life and force her to

> *"perform more, increasingly invasive sexual acts, which he recorded and used as additional leverage."*[43]

In *United States v. Abrahams*[44], the defendant, to hide his identity and to obtain nude photos and videos, used malware and other computer tools, to operate remotely the victims' web cams, without their consent. The perpetrator made extortionate threats of publicly posting the compromising photos or videos to the victims' social media accounts, unless the latter sent more nude photos or videos.[45]

3. LEGAL FRAMEWORK

Depending on the circumstances surrounding each case, several federal threat statutes can be applicable, such as 18 U.S.C. § 115 (influencing, impeding, or retaliating against a Federal official by threatening or injuring a family member);[46] 18 U.S.C. § 248 (freedom of access to clinic entrances);[47] 18 U.S.C. § 871 (threats against the President and successors to the Presidency);[48] 18 U.S.C. § 1512 (tampering with a witness, victim, or an informant);[49] 18 U.S.C. § 2332a (use of weapons of mass destruction).[50]

[42] *United States v. Fontana.* (2017) No. 16-2208 (6th Cir.), 15 August.

[43] Ibid.

[44] Complaint. *United States v. Abrahams.* (2013) No. 8:13-mj-00422 (C.D. Cal.), 17 September. See also *United States v. Chansler.* (2010) No. 3:10-cr-00100 (M. D. Fla.), 15 April. (the defendant enticed the victim to send him sexually explicit images and videos, then threatened to injure the victim's reputation through the release of the materials online or to the victims' friends or family, unless he received more such materials).

[45] Ibid.

[46] See *United States v. Cruz.* (2017) No. 15-3139 (3d Cir.), 8 November (threatening to assault and kill a United States Department of Homeland Security agent).

[47] See *United States v. Dillard.* (2011) 835 F. Supp. 2d 1120 (D. Kan.), 21 December.

[48] See *United States v. Dutcher.* (2017) 851 F.3d 757 (7th Cir.), 22 March (the defendant announced on *Facebook* his plan to assassinate President *Obama*); *United States v. Christy.* (2019) No. 3: 18-CR-223 (M.D. Pa.), 14 February (the defendant posted on *Facebook* that he was *"going to shoot President Donald J. Trump in the head"*).

[49] See, e.g. *United States v. Springer.* (2018) No. 17-15584, Non-Argument Calendar (11th Cir.), 26 October [the defendant, sympathizer of a terrorist organization, threatened to assault and murder a judge, in violation of 18 U.S.C. § 115(a)(1)(B); attempted to obstruct justice, in violation of 18 U.S.C. §§ 1503 and 2; and attempted to tamper with witnesses, in violation of 18 U.S.C. §§ 1512(b)].

[50] *United States v. Parr.* (2008) 545 F.3d 491 (7th Cir.), 18 September (the defendant threatened to use a weapon of mass destruction against a federal government building).

Most cases of electronic threats are brought to courts in violation of 18 U.S.C. § 875(c):

> *"Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both."*

Extortionate threats, on the other hand, following the manner in which they are committed, can be prosecuted in violation of a number of sections, such as 18 U.S.C. § 875(b) (interstate communications with intent to extort);[51] 18 U.S.C. § 1030(a)(7) (transmitting, with intent to extort, communication containing threat to cause damage);[52] 18 U.S.C. § 1951 (interfering with commerce by robbery, extortion, threats or violence); 18 U.S.C. § 844(e) (making interstate threats related to explosives).[53] Most often, however, cyber extortion cases are brought to courts in violation in violation of 18 U.S.C. § 875(d):

> *"Whoever, with intent to extort from any person, firm, association, or corporation, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to injure the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime, shall be fined under this title or imprisoned not more than two years, or both."*

4. LITIGATION ASPECTS

Cyber-extortion and threats can be encountered in many forms and contexts, thus allowing interpretations at numerous levels, as well as interesting arguments and viewpoints to emerge. The following subsections illustrate aspects concerning intent, "true threats", sentencing, and the insanity defense.

[51] See *United States v. Smith.* (2017) 878 F.3d 498 (5th Cir.), 28 December; *United States v. Williams.* (2012) 693 F.3d 1067 (9th Cir.), 7 September.

[52] See, e.g. *United States v. Fowler.* (2010) Case No. 8:10-cr-65-T-24 AEP (M.D. Fla.), 25 October (upon being fired, the defendant accessed victim's computers and changed employees' and the firewall passwords); *United States v. Ivanov.* (2001) 175 F. Supp. 2d 367 (D. Conn.), 6 December (the defendant gained unauthorized control over victim's computer network, then threatened the victim with the destruction of its computer systems).

[53] See Criminal Complaint, *United States v. Kadar.* (2017) 6:17-mj-1361 (Fla.), 4 April.

4.1. INTENT

Criminal liability arises only when if a person, during the perpetration of the offense, had a guilty state of mind.[54] The *U.S. Model Penal Code* lists four levels of intent: purpose,[55] knowledge,[56] recklessness,[57] and negligence[58] (from greatest to least culpability).

"Intent" has numerous meanings,[59] the judicial outcome depending upon the meaning embraced by the court.[60] As underlined in *United States v. Heineman*[61], background norms for construing criminal statutes, which

> *"presume that intent [i.e. something more than negligence] is the required mens rea in criminal laws."*

Clearly, without the unambiguous determination of a defendant's criminal intent, there can be unintended consequences.

The determination of "intent" offers interesting arguments and examinations. In *United States v. Wheeler*, for example, the court held that

> *"it is not necessary to show that a defendant intended to or had the ability to actually carry out the threat."*[62]

However, in *United States v. Gossett*[63], the defendant argued that evidence that he intended or had the ability to carry out the threats is relevant, as it *"may bear on the requisite mens rea,"* and the court agreed.

[54] See Collins, E. (2018) Insane: James Holmes, Clark v. Arizona, and America's Insanity Defense. *Journal of Law and Health*, 31, p. 33; Kachulis, L. (2017) Insane in the Mens Rea: Why Insanity Defense Reform is Long Overdue. *Southern California Interdisciplinary Law Journal*, 26, pp. 357, 362.

[55] *U.S. Model Penal Code*, General Requirements of Culpability, § 2.02(2)(a)(i). Philadelphia: American Law Institute. In English.

[56] *U.S. Model Penal Code*, General Requirements of Culpability, § 2.02(2)(b)(ii). Philadelphia: American Law Institute. In English.

[57] *U.S. Model Penal Code*, General Requirements of Culpability, § 2.02(2)(c). Philadelphia: American Law Institute. In English.

[58] *U.S. Model Penal Code*, General Requirements of Culpability, § 2.02(2)(d). Philadelphia: American Law Institute. In English.

[59] See, e.g. Crump, D. (2010) What Does Intent Mean? *Hofstra Law Review*, 38, p. 1059 (arguing that the appropriate definition of "intent" *"should depend upon factors such as the likely availability of proof, the seriousness of the offense or tort, its severity within a hierarchy of other offenses, and the difficulty of otherwise distinguishing innocent conduct"*).

[60] Op. cit., p. 1061.

[61] *United Stated v. Heineman.* (2014) 767 F.3d 970, 986-7 (10th Cir.), 14 September (citing *Judge Sutton's* dubitante opinion).

[62] *United States v. Wheeler.* (2015) 776 F.3d 736, 743 (10th Cir.), 15 January.

[63] *United States v. Gossett.* (2019) No. 1: 19-cr-00081 WJ (D.N.M.), 7 May.

An important decision can be found in *Elonis v. United States*[64], a case that received very significant attention from the legal commentators.[65] Elonis raised important questions regarding convictions under 18 U.S.C. § 875(c): whether proof of the defendant's subjective intent to threaten and proof of a defendant's subjective intent to threaten are required. The *Supreme Court* held that, even though there is no required mental state specified in the statute, it *"does not mean that none exists"*.[66] Further, the *Supreme Court* underlined that convictions under Section 875(c) cannot be based solely on a reasonable person's interpretation of the defendant's communication, however, it did not specify what *mens rea* is required under this section, reasoning only that the simple negligence standard should be construed unconstitutional.[67] Since "intent" may not be proven directly, in order to make a determination, the courts often examine the circumstances and the context associated with the defendants' actions.

Unlike Section 875(c), Section 875(d) does contain a required mental state: the intent to extort, consequently *Elonis* does not apply to prosecutions under Section 875(d). Extortion generally refers to the intent to obtain money or other thing of value with a person's consent induced by the wrongful use of actual or threatened fear, violence, or force.[68]

In order to prove the intent to extort, prosecutors must demonstrate that the defendant, through wrongful conduct, did have the intent to procure something of value,[69] without the need to demonstrate that the defendant actually intended to carry out the threats communicated. As the court in *United Stated v. Killen* held,

[64] *Elonis v. United States.* (2015) 135 S. Ct. 2001, 575 U.S., 192 L. Ed. 2D 1, 1 June.

[65] See, e.g. Quek, J.X. (2016) Elonis v. United States: The Next Twelve Years. *Berkeley Technology Law Journal*, 31, p. 1109; Brusco, M.A. (2016) Read This Note or Else!: Conviction Under 18 U.S.C. § 875(c) for Recklessly Making a Threat. *Fordham Law Review*, 84, p. 2845; Barney, D. (2016) Elonis v. United States: Why the Supreme Court Punted on Free Speech. *Pepperdine Law Review*, 2016, p. 1; Roark, M.M. (2015) Elonis v. United States: The Doctrine of True Threats: Protecting Our Ever-Shrinking First Amendment Rights in the New Era of Communication. *Pittsburgh Journal of Technology Law & Policy*, 15, p. 197; Pierce, M. (2015) Prosecuting Online Threats After Elonis. *Northwestern University Law Review*, 110, p. 51; Geha, G. (2016) Think Twice Before Posting Online: Criminalizing Threats Under 18 U.S.C. § 875(c) After Elonis. *John Marshall Law Review*, 50, p. 167.

[66] *Elonis v. United States.* (2015) 135 S. Ct. 2001, 575 U.S., 192 L. Ed. 2d 1 at 2009, 1 June.

[67] Op. cit., at 2012–13.

[68] U.S. Department of Justice. (2010) *Prosecuting Computer Crimes*. [online] Washington: Office of Legal Education Executive Office for United States Attorneys, p. 53. Available from: https://justice.gov/criminal/cybercrime/docs/ccmanual.pdf [Accessed 30 October 2012].

[69] See *United Stated v. Killen.* (2018) No. 15-15001, 11th Cir., 29 March.

> *"[e]xtortion only works if the [victim] fears that not paying will invite an unsavory result,"*
>
> *"to intend to extort one must necessarily intend to instill fear of harm."*[70]

The court further argued that

> *"it would be passing strange, indeed impossible, for a defendant to intend to obtain something by communicating [...] a threat [to injure the property or reputation of another or a threat to accuse another of a crime] without also intending, understanding, or, possibly, recklessly disregarding that the communication would be perceived as threatening."*[71]

4.2. TRUE THREATS

The First Amendment stipulates that

> *"Congress shall make no law [...] abridging the freedom of speech."*[72]

There are, however, categories of speech which do not fall under this protection, such as

> *"advocacy intended and likely to incite imminent lawless action, obscenity, defamation, child pornography, fighting words, fraud, true threats, speech integral to criminal conduct, and speech presenting a grave and imminent threat the government has the power to prevent."*[73]

These aspects were analyzed extensively by numerous legal commentators.[74] The prosecution, nonetheless,

> *"is not permitted to punish speech merely because the speech is forceful or aggressive."*[75]

For instance, if a person suggests "revenge", this does not necessarily imply breach of any law.[76] To further complicate things, many harms that could be

[70] Ibid.

[71] Ibid.

[72] *The Constitution of the United States 1788 (Amendment I)*. United States of America. In English.

[73] Harawa, D.S. (2014) Social Media Thoughtcrimes. *Pace Law Review*, 35, pp. 366, 380.

[74] See, e.g. Volokh, E. (2016) The Freedom of Speech and Bad Purposes. *UCLA Law Review*, 63, p. 1366; Coenen, D.T. (2017) Freedom of Speech and the Criminal Law. *Boston University Law Review*, 97, p. 1533.

[75] *United States v. Schweitzer.* (2017) No. 4: 17CR3094 (D. Neb.), 28 November.

[76] See Strasser, M. (2011) Advocacy, True Threats, and the First Amendment. *Hastings Constitutional Law Quarterly*, 38, p. 339.

caused by threats, might also be caused by advocacy, for instance, certain political messages are *"threatening and should nonetheless be protected"*.[77]

The true threats prohibition *"protect[s] individuals from the fear of violence"* and *"from the disruption that fear engenders,"* and protects people

> *"from the possibility that the threatened violence will occur"*.[78]

A communication can be considered "threat" if

> *"it expresses an intention to inflict harm, loss, evil, injury, or damage on another."*[79]

Nevertheless, numerous factors are taken into consideration in the determination of "true threats," for instance,

> *"the reaction of the recipient of the threat and of other listeners; whether the threat was conditional; whether the threat was communicated directly to its victim; whether the maker of the threat had made similar statements to the victim in the past; and whether the victim had reason to believe that the maker of the threat had a propensity to engage in violence."*[80]

A defendant's background can often be considered relevant towards the determination of a "true threat".[81]

The courts disagree on how "true threat" should be defined.[82] The majority of courts use the "objective test", which examines whether a reasonable person would regard the threat as true. Nevertheless, based on the *Supreme Court's* decision in *Virginia v. Black*, several courts use the "subjective test", which examines whether a reasonable speaker would foresee that the recipients of the communication would interpret it as threat.[83]

A "true threat" is a

[77] Op. cit., p. 385.

[78] See *RAV v. St. Paul.* (1992) 505 U.S. 377, 388, 22 June.

[79] *United States v. Jongewaard.* (2009) 567 F.3d 336, 340 (8th Cir.), 3 June.

[80] *United States v. Schweitzer.* (2017) No. 4: 17CR3094 (D. Neb.), 28 November.

[81] See *United States v. Parr.* (2008) 545 F.3d 491 (7th Cir.), 18 September.

[82] See, e.g. McCann, A.E. (2006) Are Courts Taking Internet Threats Seriously Enough? An Analysis of True Threats Transmitted Over the Internet, as Interpreted in United States v. Carmichael. *Pace Law Review*, 26, pp. 523, 527.

[83] *Virginia v. Black.* (2003) 538 U.S. 343, 360, 7 April (a "true threat" occurs where the *"speaker directs a threat to a person or group of persons with the intent of placing the victim in fear of bodily harm or death,"* without the need for the speaker to intend to carry out the threat).

> *"serious threat as distinguished from mere political argument, idle talk, or jest,"*
>
> *"declaration of intention, purpose, design, goal, or determination to inflict punishment, loss, or pain on another, or to injure another or his property by the commission of some unlawful act."*[84]

Also, a "true threat" is a

> *"serious statement expressing an intention to do an act which under the circumstances would cause apprehension in a reasonable person, as distinguished from idle or careless talk, exaggeration, or something said in a careless manner."*[85]

A threatening statement that is merely "hyperbole", or an exaggeration that aims to add a "heightened effect" to a certain viewpoint, without the intent to carry it out against a specific individual or property, is protected by the First Amendment and cannot be considered "true threat".[86] In *Commonwealth v. Knox*[87], for illustration, the court held that the "true threat" doctrine requires the speaker to have *"acted with an intent to terrorize or intimidate."*

In *United States v. Tinoco*[88], the defendant argued that his statements were not "true threats" as he

> *"didn't intend to place the victims in fear; (2) his Facebook posts didn't reach the victims; and (3) he frequently peppered his statements with the phrase 'figuratively speaking'."*

However, the court rejected the argument and held that, as the victim's testimony demonstrates, the threats were taken seriously (also, as per the defendant's own admission, according to which the people receiving his threats *"would feel threatened"*, and statements: *"I mean every word"* and *"You can quote me"*.)[89] Even if

[84] *United States v. Twitty.* (2019) Criminal Case No. 13-CR-00076-RBJ (D. Colo.), 4 January.

[85] *United States v. Parr.* (2008) 545 F.3d 491, 497 (7th Cir.), 18 September.

[86] *United States v. Kirsch.* (2015) 151 F. Supp. 3d 311, 313 (W.D.N.Y.), 16 December (*"Strong language that, if taken literally, may seem to communicate a threat, may not constitute a true threat"*).

[87] *Commonwealth v. Knox.* (2018) 190 A.3d 1146 (Pa.), 21 August.

[88] *United States v. Tinoco.* (2018) No. 17-2059 (10th Cir.), 28 March.

[89] Ibid.

> *"the alleged threat did not identify any specific person or group,"*

the defendant's communications can, in certain contexts, be interpreted as true threat.[90]

In *United States v. Killen*[91], the defendant posed as a young girl on a messaging-based mobile-phone application. The defendant sent to the victims images of a partially dressed girl and asked and received from the boys nude photos of themselves in return.[92] When the boys tried to end the contact with the defendant, the latter threatened the boys that, unless they will send him more nude photos, he will post the photos received on social media platforms, such as *Instagram*.[93] On appeal, the defendant challenged the sufficiency of the evidence.[94] However, taking into account the electronic evidence recovered from the defendant's electronic devices, and on the admission of the defendant to the extortionate conduct, the court found that there is

> *"sufficient evidence on these counts to permit a jury to find guilt beyond a reasonable doubt without testimony from the victims."*[95]

4.3. SENTENCING ASPECTS

The U.S.S.G., which contains non-binding rules that aim to create a uniform sentencing policy those convicted in the U.S. federal court system, has numerous enhancements that are applicable to these offenses. In *United States v. Sunmola*[96], for example, the defendant and his co-conspirators created profiles on dating websites, which included pictures of U.S. military men in uniforms as part of his online profile. After gaining the trust of women met online, the defendant and his co-conspirators asked for money and merchandise.[97] The defendant was charged with several offenses, including interstate extortion, in violation of 18 U.S.C. § 875(d). The defendant also sexually exploited the victims: he persuaded women to pose in a sexually suggestive positions, in front of a web camera. Without the victims' consent, the defendant recorded them, then posted the videos

[90] *United States v. Cox.* (1992) 957 F.2d 264, 266 (6th Cir.), 27 February.

[91] *United States v. Killen.* (2018) No. 15-15001 (11th Cir.), 29 March.

[92] Ibid.

[93] Ibid.

[94] Ibid.

[95] Ibid.

[96] *United States v. Sunmola.* (2018) 887 F.3d 830 (7th Cir.), 16 April.

[97] Ibid.

online and sent the relevant links to the victims and their relatives, with an extortion demand, containing the alarming warning that

> *"by the time he was finished with her she would want to kill herself."*[98]

The court in this case applied the following sentencing enhancements: four-level leadership,[99] two-level for acting on behalf of a government agency,[100] four-level substantial financial hardship,[101] a two-level vulnerable victim,[102] a 16-level for an intended loss of $2,054,972.66,[103] and a two-level due to the perpetration of the offense outside of the United States.[104] The judge also granted two upward departures, for psychological injury to a victim and for the gratuitous infliction of injury to a victim.[105]

The defendant appealed the sentencing enhancements; however, the court held that the district court did not erred in imposing the enhancements, as follows, respectively: the defendant had a *"high level of control and authority"* in the scheme; while the defendant argued that he used the false military status

> *"to impress his victims, not for the purpose of obtaining a benefit on behalf of the military or other government organization,"*

the court held that he misrepresented that he was acting on behalf of the military;[106] as per the findings in the *Pre-Sentencing Report (PSR)*, seven victims suffered substantial financial hardship, some of them submitted victim impact statements; while the victims were middle-aged women, rather than elderly, many of the women

[98] *United States v. Sunmola.* (2018) 887 F.3d 830 (7th Cir.), 16 April, at 835.

[99] U.S. Sentencing Commission. (2018) *Guidelines Manual*. Aggravating Role § 3B1.1(a). [online] Available from: https://guidelines.ussc.gov/gl/§3B1.1. [Accessed 4 June 2019].

[100] U.S. Sentencing Commission. (2018) *Guidelines Manual*. Offense Conduct § 2B1.1(b)(9)(A). [online]. Available from: https://guidelines.ussc.gov/gl/§2B1.1. [Accessed 4 June 2019].

[101] U.S. Sentencing Commission. (2018) *Guidelines Manual.* Offense Conduct § 2B1.1(b)(2)(B). [online]. Available from: https://guidelines.ussc.gov/gl/§2B1.1. [Accessed 4 June 2019] (the substantial financial hardship enhancement applies if the offense resulted in *"substantial financial hardship to five or more victims"*).

[102] U.S. Sentencing Commission. (2018) *Guidelines Manual.* Hate Crime Motivation or Vulnerable Victim § 3A1.1(b)(1). [online]. Available from: https://guidelines.ussc.gov/gl/§3A1.1. [Accessed 4 June 2019].

[103] U.S. Sentencing Commission. (2018) *Guidelines Manual.* Offense Conduct § 2B1.1(b)(1)(I). [online]. Available from: https://guidelines.ussc.gov/gl/§2B1.1. [Accessed 4 June 2019].

[104] Ibid.

[105] Op. cit., at 836.

[106] Op. cit., at 838.

> *"had been divorced, abandoned, widowed, or ignored by the men in their lives"*

and, through online dating, they were seeking companionship, position that made them

> *"particularly susceptible to falling into the vicious trap of a man who deceitfully made them believe they were in love,"*

therefore vulnerable to extortionate tactics;[107] based on

> *"direct interviews, phone interviews, mailed-in statements, or mailed-in supporting documentation with the victims describing what happened and the amount of money they lost,"*

the determination of the total loss was construed as correctly calculated by the court.[108]

Another example of enhancements application, *United States v. Haileselassie*, the defendant appealed his sentence, which had two upward enhancements under the U.S.S.G. for *"substantial disruption of governmental function and obstruction of justice"*.[109] The appeal court, however, citing the

> *"extensive criminal history, including multiple convictions for threats, false reports, harassment, assault, trespass, and mailing threatening communications,"*

affirmed the sentence.[110] Other upward U.S.S.G. enhancements applicable to these offenses include substantial disruption of governmental function and obstruction of justice,[111] violation of court protective orders, making of multiple threats, and intention to carry out the threats.[112]

[107] Op. cit., at 837.

[108] Op. cit., at 840.

[109] *United States v. Haileselassie.* (2019) No. 18-1343 (8th Cir.), 10 June.

[110] Ibid.

[111] Ibid.

[112] *Irizarry v. United States.* (2008) 553 U.S. 708, 128 S. Ct. 2198, 171 L. Ed. 2D 28, 12 June.

4.4. THE INSANITY DEFENSE

Cyber extortion and threats are specific intent crimes, allowing defendants to bring up defenses involving their mental or emotional conditions.[113] Importantly, however, insanity is a legal, not a medical aspect.[114]

Evidence of a defendant's mental problems at the time of the crime is brought up to establish the insanity defense. This defense, however,

> *"is not concerned with the mens rea element of the crime; rather, it operates to completely excuse the defendant whether or not guilt can be proven."*[115]

Different from "insanity", the diminished capacity defense, which regards a defendant's ability to come to the required criminal state of mind, is not considered an excuse:

> *"successful defendants simply are not guilty of the offense charged, although they are usually guilty of a lesser included offense."*[116]

As explained by the court in *United States v. Long,* a severe mental disease or defect (such as the schizotypal personality disorder) alone, will not be considered enough for the purposes of 18 U.S.C. § 17(a), which regards the affirmative defense of insanity:

> *"there must be sufficient evidence of a temporal and causal nexus between the symptoms of the disease and the commission of the acts themselves."*[117]

However, the defendants that have a mental disease or defect, can, upon receiving treatment, be rendered competent to stand the trial. In *United States v. Arega,* for instance, the defendant was charged with transmitting a threatening communication.[118] After a *"regimen of medications, including antipsychotics,"* the medical evaluation rendered the defendant as being lucid, no longer suffering

[113] *United States v. Sullivan.* (2016) No. 3: 13-cr-00064-HZ (D. Or.), 6 January.

[114] See *Kahler v. Kansas.* (2020) No. 18-6135 (U.S.), 23 March (*"The insanity defense sits at the juncture of medical views of mental illness and moral and legal theories of criminal culpability."*); The Free Dictionary. *Insanity Defense*. [online]. Available from: https://legal-dictionary.thefreedictionary.com/Insanity+Defence [Accessed 2 July 2019] (*"A defense asserted by an accused in a criminal prosecution to avoid liability for the commission of a crime because, at the time of the crime, the person did not appreciate the nature or quality or wrongfulness of the acts."*).

[115] *United States v. Twine.* (1988) 853 F.2d 676, 678 (9th Cir.), 1 August.

[116] Op. cit., at 678.

[117] *United States v. Long.* (2009) No. 07-31131 (5th Cir.), 5 March.

[118] *United States v. Arega.* (2018) No. 1: 17-cr-00225-TSC (D.C.), 17 January.

> *"from the irrational and delusional ideation that he had previously exhibited,"*

therefore competent to stand the trial.[119]

In *United States v. Christian*[120], the defendant, charged with two counts of transmitting, via e-mail, threats to injure the person of another, in violation of 18 U.S.C. § 875(c), in order to establish that he was incapable of forming the specific intent to threaten, raised the diminished capacity defense. The district court, however, precluded his expert witness from testifying.[121] *The Court of Appeals*, held that the district court acted abusively by not considering the expert's testimony, which could have helped the jury decide on the defendant's capacity

> *"to form the specific intent to threaten when he sent the emails at issue,"*

and vacated and remanded the conviction for a new trial.[122]

United States v. Ivers provides another example of mental competency examination: the defendant was charged with transmission of threats to assault and murder a law enforcement officer, in violation of 18 U.S.C. § 115(a)(1)(B) and 18 U.S.C. § 875(c).[123] During the initial competency hearing, the defendant, who claimed that

> *"federal authorities (he most commonly names the CIA and FBI) implanted a 'non organic foreign body/object' into his brain and had been using the implant to torture him,"*

was not found competent to stand the trial, as he was assessed to suffer *"from mental disease or defect,"* therefore not mentally competent

> *"to understand the nature and consequences of the proceedings against him or to assist properly in his defense."*[124]

[119] Ibid.

[120] *United States v. Christian.* (2014) 749 F.3d 806-8 (9th Cir.), 17 April.

[121] Op. cit., at 809.

[122] Op. cit., at 811–5.

[123] *United States v. Ivers.* (2018) No. 3: 16-cr-00347-AA (D. Or.), 21 February.

[124] Ibid.

After several months of hospitalization, the clinical psychologist assessed that the defendant can communicate in a "'very rational' manner" and can stand the trial.[125]

Mental diseases or defects can also be taken into consideration for reduced sentences. In *United States v. Humphries*, for illustration, the defendant experienced

> *"symptoms consistent with diagnosis of Post-Traumatic Stress Disorder (PTSD), Obsessive Compulsive Disorder (OCD) and adjustment disorder with mixed anxiety and depressed mood."*[126]

Taking the defendant's mental issues into consideration, the court granted a downward departure from the U.S.S.G. In contrast, in *United States v. Wyrick*, the defendant-appellant, contested as "substantively unreasonable" his 37-month sentence for the numerous telephone calls containing threats to injure the person of another he made, in violation of 18 U.S.C. § 875(c). The defendant-appellant cited his diagnosed mental condition of "Delusional Disorder, Persecutory and Erotomania Type" and his "true first offender" status, and requested a downward sentencing variance.[127] The appeal court found that a downward variance, based on the defendant's mental illness, was unwarranted, as the defendant's behavior

> *"was no less serious as a result and is no less likely to happen again."*[128]

The appeal court went on and, while it acknowledged the defendant's arguments, considered them *"unconvincing given the facts of the case"* and affirmed the sentence of the district court.[129]

5. CONCLUSION

This article presented a comprehensive analysis of the cyber extortion and threats phenomenon. The article extends the understanding of the phenomenon by providing a thorough understanding

[125] Ibid (the defendant was administered the Inventory of Legal Knowledge and the MacArthur Competence Assessment Tool-Criminal Adjudication).

[126] *United States v. Humphries.* (2013) No. 12 Cr. 347 (RWS) (S.D.N.Y.), 28 October.

[127] *United States v. Wyrick.* (2011) No. 10-3117 (10th Cir.), 24 March (people suffering from Delusional Disorder-Erotomania Type *"believe another person, usually someone of a higher social status, is in love with them"*).

[128] Ibid.

[129] Ibid.

of the attributes and of the most important litigation aspects, such as the legal elements of these offenses, how the U.S. legal system addresses them, and sentencing aspects.

The article evidenced that these communications, especially in their extreme forms, can have very serious consequences, such as placing the victims in an constant state of fear and stress, which can result in a major psychological harm or generalized trauma, disrupting the course of people's activities, and affecting public interests.

The phenomenon poses complex and many-faceted challenges regarding the criminalization, prosecution, and sentencing. For a more effective response to this phenomenon, it is necessary to better understand the initiation and escalation of these offenses, to form threat assessment professionals, and to promote law enforcement best practice guidelines. There is also a need for stronger and more coherent legal framework, including uniform interpretation of the legal elements of these offenses and the explicit incrimination of intentional infliction of emotional distress. Appropriate protection of personally identifying information, including through encryption and redaction, must also receive adequate consideration.

The development of effective computerized natural language analysis tools, employed to analyze the linguistic features of the phenomenon, can help better control the phenomenon, by filtering out of such communications, triggering account termination, and referring such instances to law enforcement, for a prompt reaction to imminent threats.

General educational programs that address related aspects, such as cyberviolence risks, personal data protection, preservation of digital evidence, appropriate reactions to cyber threats, and incident reporting, can also play a significant role in the control of the phenomenon.

Even though this article analyzed cases from just one jurisdiction, the findings can be of interest to a global audience. The findings of this article can be used to elaborate educational materials for law enforcement training programs and for law school clinics, to develop fact analysis and client advising skills.

LIST OF REFERENCES

[1] Barney, D. (2016) Elonis v. United States: Why the Supreme Court Punted on Free Speech. *Pepperdine Law Review*, 2016.

[2] Berman, M.N. (1998) The Evidentiary Theory of Blackmail: Taking Motives Seriously. *University of Chicago Law Review*, 65.

[3] Brusco, M.A. (2016) Read This Note or Else!: Conviction Under 18 U.S.C. § 875(c) for Recklessly Making a Threat. *Fordham Law Review*, 84.

[4] Bumb, M. L. (2017) Domestic Violence Law, Abusers' Intent, and Social Media: How Transaction-Bound Statutes Are the True Threats to Prosecuting Perpetrators of Gender--Based Violence. *Brooklyn Law Review*, 82 (2).

[5] Coenen, D.T. (2017) Freedom of Speech and the Criminal Law. *Boston University Law Review*, 97.

[6] Collins, E. (2018) Insane: James Holmes, Clark v. Arizona, and America's Insanity Defense. *Journal of Law and Health*, 31.

[7] *Commonwealth v. Knox.* (2018) 190 A.3d 1146 (Pa.), 21 August.

[8] Crump, D. (2010) What Does Intent Mean? *Hofstra Law Review*, 38.

[9] Cybercrime Convention Committee (T-CY). (2018) *Mapping Study on Cyberviolence*. [online] Strasbourg: Council of Europe.

[10] *Elonis v. United States.* (2015) 135 S. Ct. 2001, 575 U.S., 192 L. Ed. 2D 1, 1 June.

[11] European Institute for Gender Equality. (2017) *Cyber violence against women and girls*.

[12] European Union Agency for Law Enforcement Cooperation (Europol). (2017) *Internet Organised Crime Threat Assessment*. The Hague: Europol.

[13] Florida Statutes 836.05 Threats; extortion.

[14] *Fontana v. United States.* (2020) No. 14-20141 (E.D. Mich.), 17 April.

[15] Geha, G. (2016) Think Twice Before Posting Online: Criminalizing Threats Under 18 U.S.C. § 875(c) After Elonis. *John Marshall Law Review*, 50.

[16] Green, S.P. (2005) Theft by Coercion: Extortion, Blackmail, and Hard Bargaining. *Washburn Law Journal*, 44.

[17] Han, D.S. (2014) The Mechanics of First Amendment Audience Analysis. *William and Mary Law Review*, 55.

[18] Harawa, D.S. (2014) Social Media Thoughtcrimes. *Pace Law Review*, 35.

[19] *In the Matter of Search of a Residence in Oakland.* (2019) Case No. 4-19-70053 (N.D. Cal.), 10 January.

[20] *Irizarry v. United States.* (2008) 553 U.S. 708, 128 S. Ct. 2198, 171 L. Ed. 2D 28, 12 June.

[21] Kachulis, L. (2017) Insane in the Mens Rea: Why Insanity Defense Reform is Long Overdue. *Southern California Interdisciplinary Law Journal*, 26.

[22] *Kahler v. Kansas.* (2020) No. 18-6135 (U.S.), 23 March.

[23] McCann, A.E. (2006) Are Courts Taking Internet Threats Seriously Enough? An Analysis of True Threats Transmitted Over the Internet, as Interpreted in United States v. Carmichael. *Pace Law Review*, 26.

[24] Peterson, J. and Densley, J. (2017) Cyber Violence: What Do We Know and Where Do We Go From Here?. *Aggression and Violent Behavior*, 34.

[25] Pierce, M. (2015) Prosecuting Online Threats After Elonis. *Northwestern University Law Review*, 110.

[26] Quek, J.X. (2016) Elonis v. United States: The Next Twelve Years. *Berkeley Technology Law Journal*, 31.

[27] *RAV v. St. Paul.* (1992) 505 U.S. 377, 388, 22 June.

[28] Roark, M.M. (2015) Elonis v. United States: The Doctrine of True Threats: Protecting Our Ever-Shrinking First Amendment Rights in the New Era of Communication. *Pittsburgh Journal of Technology Law & Policy*, 15.

[29] Romney, J. (2012) Eliminating the Subjective Intent Requirement for True Threats in United States v. Bagdasarian. *Brigham Young University Law Review*, 2012.

[30] *Scheidler v. National Organization for Women.* (2003) 537 U.S. 393.

[31] Shavell, S. (1993) An Economic Analysis of Threats and Their Illegality: Blackmail, Extortion, and Robbery. *University of Pennsylvania Law Review,* 141.

[32] Spitzberg, B.H. and Gawron, J.M. (2016) Toward Online Linguistic Surveillance of Threatening Messages. *Journal of Digital Forensics, Security and Law*, 11.

[33] Strasser, M. (2011) Advocacy, True Threats, and the First Amendment. *Hastings Constitutional Law Quarterly*, 38.

[34] The Free Dictionary. *Insanity.*

[35] *United States v. Abrahams.* (2013) No. 8:13-mj-00422 (C.D. Cal.), 17 September.

[36] *United States v. Alkhabaz.* (1997) 104 F.3d 1492 (6th Cir.), 29 January.

[37] *United States v. Arega.* (2018) No. 1: 17-cr-00225-TSC (D.C.), 17 January.

[38] *United States v. Avenatti.* (2020) No.(S1) 19 Cr. 373 (PGG) (S.D.N.Y.), 14 January.

[39] *United States v. Bagdasarian.* (2011) 652 F.3d 1113 (9th Cir.), 19 July

[40] *United States v. Bishop.* (2018) Case 118MJ24LDA (D.R.I.), 23 January.

[41] *United States v. Cain.* (2018) No. 1: 16-cr-00103-JAW (D. Me.), 1 June.

[42] *United States v. Carrillo.* (2020) No. 1: 19-cr-01991 KWR (D.N.M.), 8 April.

[43] *United States v. Champ, United States v. Wood.* (2006) 459 F. Supp. 2d 451 (E.D. Va.), 29 September.

[44] *United States v. Chansler.* (2010) No. 3:10-cr-00100 (M. D. Fla.), 15 April.

[45] *United States v. Christian.* (2014) 749 F.3d 806-8 (9th Cir.), 17 April.

[46] *United States v. Christy.* (2019) No. 3: 18-CR-223 (M.D. Pa.), 14 February.

[47] *United States v. Coss.* (2012) 677 F.3d 278 (6th Cir.), 16 April.

[48] *United States v. Cox.* (1992) 957 F.2d 264, 266 (6th Cir.), 27 February.

[49] *United States v. Cruz.* (2017) No. 15-3139 (3d Cir.), 8 November.

[50] *United States v. Dillard.* (2011) 835 F. Supp. 2d 1120 (D. Kan.), 21 December.

[51] *United States v. Doggart.* (2020) 947 F.3d 879 (6th Cir.), 15 January.

[52] *United States v. Dutcher.* (2017) 851 F.3d 757 (7th Cir.), 22 March.

[53] *United States v. Fontana.* (2017) No. 16-2208 (6th Cir.), 15 August.

[54] *United States v. Fowler.* (2010) Case No. 8:10-cr-65-T-24 AEP (M.D. Fla.), 25 October.

[55] *United States v. Gillenwater.* (2014) 749 F.3d 1094 (9th Cir.), 11 April.

[56] *United States v. Gomez.* (2020) No. 18-12089 (11th Cir.), 14 February.

[57] *United States v. Gossett.* (2019) No. 1: 19-cr-00081 WJ (D.N.M.), 7 May.

[58] *United States v. Haileselassie.* (2019) No. 18-1343 (8th Cir.), 10 June.

[59] *United States v. Heineman.* (2014) 767 F.3d 970, 972 (10th Cir.), 15 September.

[60] *United States v. Humphries.* (2013) No. 12 Cr. 347 (RWS) (S.D.N.Y.), 28 October.

[61] *United States v. Ivanov*. (2001) 175 F. Supp. 2d 367 (D. Conn.), 6 December.

[62] *United States v. Ivers.* (2018) No. 3: 16-cr-00347-AA (D. Or.), 21 February.

[63] *United States v. Jongewaard.* (2009) 567 F.3d 336, 340 (8th Cir.), 3 June.

[64] *United States v. Jordan.* (2017) No. 16-CR-93-FPG-HKS-1 (W.D.N.Y.), 24 October.

[65] *United States v. Kadar.* (2017) Case No. 6:17-mj-1361 (M.D. Fla.), 4 April.

[66] *United States v. Killen.* (2018) No. 15-15001 (11th Cir.), 29 March.

[67] *United States v. Kirsch.* (2015) 151 F. Supp. 3d 311, 313 (W.D.N.Y.), 16 December.

[68] *United States v. Leach.* (2017) Case No. 2:17mj-44-1 (D. Vt.), 21 April.

[69] *United States v. Lisnyak.* (2015) Case No. 15-04179MJ-PCTDMF (D. Ariz.), 16 July.

[70] *United States v. Long.* (2009) No. 07-31131 (5th Cir.), 5 March.

[71] *United States v. McCrudden.* (2015) No. CR-11-061 (DRH) (E.D.N.Y.), 16 March.

[72] *United States v. Michael.* (2012) No. 2: 12-cr-1-WTL-CMM (S.D. Ind.), 9 October.

[73] *United States v. Parr.* (2008) 545 F.3d 491 (7th Cir.), 18 September.

[74] *United States v. Petrovic.* (2012) 701 F.3d 849 (8th Cir.), 13 December.

[75] *United States v. Schweitzer.* (2017) No. 4: 17CR3094 (D. Neb.), 28 November.

[76] *United States v. Smith.* (2017) 878 F.3d 498 (5th Cir.), 28 December.

[77] *United States v. Springer.* (2018) No. 17-15584, Non-Argument Calendar (11th Cir.), 26 October.

[78] *United States v. Sullivan.* (2016) No. 3: 13-cr-00064-HZ (D. Or.), 6 January.

[79] *United States v. Sunmola.* (2018) 887 F.3d 830 (7th Cir.), 16 April.

[80] *United States v. Swarbrick.* (2018) Case 3:18-MJ-1214 (M.D. Tenn.), 19 September.

[81] *United States v. Telfair.* (2020) No. 19-CR-270 (E.D.N.Y.), 3 February.

[82] *United States v. Tinoco.* (2018) No. 17-2059 (10th Cir.), 28 March.

[83] *United States v. Turrella.* (2012) No. 10-30051 (9th Cir.), 15 March.

[84] *United States v. Twine.* (1988) 853 F.2d 676, 678 (9th Cir.), 1 August.

[85] *United States v. Twitty.* (2019) Criminal Case No. 13-CR-00076-RBJ (D. Colo.), 4 January.

[86] *United States v. Vandevere.* (2019) No. 1: 19-cr-63-MOC (W.D.N.C.), 16 September.

[87] *United States v. Wheeler.* (2015) 776 F.3d 736, 743 (10th Cir.), 15 January.

[88] *United States v. Wheeler.* (2019) Criminal Case No. 12-cr-0138-WJM (D. Colo.), 9 July.

[89] *United States v. White.* (2010) Criminal Action No. 7:08-CR-00054 (W.D. Va.), 20 January.

[90] *United States v. White.* (2017) Criminal Action No. 7: 13CR00013 (W.D. Va.), 31 May.

[91] *United States v. Williams.* (2012) 693 F.3d 1067 (9th Cir.), 7 September.

[92] *United States v. Williams.* (2018) No. 17-2454 (8th Cir.), 26 October.

[93] *United States v. Wyrick.* (2011) No. 10-3117 (10th Cir.), 24 March.

[94] U.S. Department of Justice. (2010) *Prosecuting Computer Crimes*. [online] Washington: Office of Legal Education Executive Office for United States Attorneys.

[95] U.S. Departmentt of Justice. (2016) *The National Strategy for Child Exploitation Prevention and Interdiction*.

[96] U.S. Model Penal Code.

[97] Van Der Wilk, A. (2018) *Cyber violence and hate speech online against women*. PE 604.979. Brussels: European Parliament.

[98] *Virginia v. Black.* (2003) 538 U.S. 343, 360, 7 April.

[99] Volokh, E. (2016) The Freedom of Speech and Bad Purposes. *UCLA Law Review*, 63.

[100] *White v. United States.* (2019) No. 6: 17-cv-689-Orl-28GJK (M.D. Fla.), 14 February.

[101] Women and Gender Equality Canada. (2019) *New federal investment will help end cyberviolence*. [press release] 27 August. Available from: https://www.canada.ca/en/status-women/news/2019/08/new-federal-investment-will-help-end-cyberviolence.html [Accessed 3 December 2019]

DOI 10.5817/MUJLT2020-1-2

HIGHER SUSTAINABILITY OF MENTAL MODELS ACQUIRED FROM A DIGITAL GAME IN COMPARISON WITH A LIVE ACTION ROLE--PLAYING GAME AND A TRADITIONAL LECTURE[*]

by

MICHAELA SLUSSAREFF[**], VÍT ŠISLER[***]

This article analyses the effectivity of teaching EU law using various educational media. It specifically explores the differences between, and sustainability of, mental models constructed within three various educational environments: (1) a digital game played on PCs, (2) a non-digital role-playing game, and (3) a traditional lecture with discussions. We conducted a laboratory experiment, in which participants (253 high school students, M = 112, F = 141, mean age 16.5) studied EU laws, institutions, and politics in the three above-mentioned environments. We evaluated and compared mental models participants constructed through content analysis of the concept maps they drew immediately after the experiment and others made one month later. Within the analysis, we studied content, architecture, and changes in mental models over time. The resulting data offer unique insight into the process of mental models creation and sustainability thereof within game-based learning; particularly, when using a digital game. Digital game-based learners' concept maps differed in comparison with those of the educational role-playing and traditional lecture groups; the students tended to keep less altered mental models

[*] During writing this article, the authors were supported by the *Charles University* project *Progress Q15*. *Vít Šisler* was further supported by the *European Regional Development Fund--Project "Creativity and Adaptability as Conditions of the Success of Europe in an Interrelated World"* (No. CZ.02.1.01/0.0/0.0/16_019/0000734) and *Charles University* project PRIMUS/HUM/03. We would like to thank *Cyril Brom* for comments on the early version of this text.

[**] michaela.slussareff@ff.cuni.cz, Assistant Professor, Institute of Information Science and Librarianship, Faculty of Arts, Charles University, Czech Republic.

[***] vit.sisler@ff.cuni.cz, Assistant Professor, Institute of Information Science and Librarianship, Faculty of Arts, Charles University, Czech Republic .

in their long-term memory: even after the one month period. The results suggest that a digital game-based learning environment could be more successful in mental model retention and for efficacy of future recall; particularly, when dealing with complex phenomena like EU law.

KEY WORDS

Concept Maps, Digital Game-based Learning, Mental Models

1. INTRODUCTION

Teaching EU law, the role of European institutions and EU politics in a formal school system is a challenging task; particularly, at the high school level. These issues are complex and cannot be easily explained through the frontal lectures that still dominate higher education in the Czech Republic.[1] As *Baroncelli, Farneti and Vanhoonacker* argue, teaching EU law should

> *"move beyond traditional knowledge-based learning"* and utilize a *"learning to learn paradigm with emphasis on more pragmatic problem-solving and problem-based learning."*[2]

The rise of constructivist theories of learning has triggered a variety of new methods and learning environments for teaching EU law: including project-based learning and educational simulations.[3] More recently, this domain has also begun to benefit from using computer-based instruction and digital games.[4]

Based on some studies, digital games in particular are able to simulate tasks involving the same cognitive processes required for task performance in the real world.[5] They can also provide immediate feedback that might induce correction of misunderstood information or mental model re-

[1] Švaříček, R., Šeďová, K. and Šalamounová, Z. (2012) *Komunikace ve školní třídě.* Praha: Portál, pp. 161–170.

[2] Baroncelli, S., Farneti, R. and Vanhoonacker, S. (2014) Introduction – Teaching European Studies: Educational Challenges. In: Stefania Baroncelli, Roberto Farneti, Ioan Horga and Sophie Vanhoonacker (eds.). *Teaching and Learning the European Union: Traditional and Innovative Methods.* Dordrecht: Springer, p. 2.

[3] Jones, R. and Bursens, P. (2014) Assessing EU Simulations: Evidence from the Trans-Atlantic EuroSim. In: Stefania Baroncelli, Roberto Farneti, Ioan Horga and Sophie Vanhoonacker (eds.). *Teaching and Learning the European Union: Traditional and Innovative Methods.* Dordrecht: Springer.

[4] Ibid; Brom, C. et al. (2016) You like it, you learn it: affectivity and learning in competitive social role play gaming. *International Journal of Computer-Supported Collaborative Learning,* 11.

-construction.[6] Despite many studies supporting the educational value and efficiency of a digital game-based approach to learning[7], other reports[8] argue that there is no significant proof that digital games affect learning positively; i.e. as compared to traditional instruction or multimedia presentations. Nevertheless, most authors concur with regards to positive emotional and motivational responses in students interacting with games incorporated into educational programs.[9]

The process of information delivery within game-based educational treatment and frontal teaching differs on many levels: game elements as simulation, immediate feedback and emotional engagement seem to be essential ingredients of learning.

The aim of this study is to explore the process of mental models' construction within three different educational environments: (1) a digital game played on PCs, (2) a non-digital role-playing game, and (3) a traditional lecture with discussions. We conducted a laboratory experiment, in which a sample of 253 high-school students (M = 112, F = 141, mean age 16.5) studied EU laws, European institutions, and EU politics in the three above-mentioned environments. We subsequently evaluated

[5] Tobias, S. and Fletcher, D. (2011) Learning from Computer Games: A Research Review. In: Stefan De Wannemacker, Sylke Vandercruysse and Geraldine Clarebout (eds.). *Serious Games: The Challenge. Communications in Computer and Information Science*. Springer, Berlin, Heidelberg.

[6] Moreno, R. and Mayer, R. (2007) Interactive multimodal learning environments: Special issue on interactive learning environments: Contemporary issues and trends. *Educational Psychology Review.*

[7] Schneider, S. et al. (2018) Anthropomorphism in decorative pictures: benefit or harm for learning? *Journal of Educational Psychology,* 110 (2); Plass, J. and Kaplan, U. (2016) Emotional Design in Digital Media for Learning. In: Sharon Tettegah and Martin Gartmeier (eds.). *Emotions, Technology, Design, and Learning;* Sitzmann, T. (2011) A Meta-Analytic Examination of the Instructional Effectiveness of Computer-Based Simulation Games. *Personnel Psychology*, 64 (2).

[8] Münchow, H., Mengelkamp, C. and Bannert, M. (2017) The better you feel the better you learn: Do warm colours and rounded shapes enhance learning outcome in multimedia learning? *Education Research International*; Clark, D. B., Tanner-Smith, E. E. and Killingsworth, S. S. (2016) Digital Games, Design, and Learning: A Systematic Review and Meta-Analysis. *Review of Educational Research,* 86 (1); Wouters, P. et al. (2013) A Meta-Analysis of the Cognitive and Motivational Effects of Serious Games. *Journal of Educational Psychology,* Advance online publication; Adams, D. M. et al. (2012) Narrative games for learning: Testing the discovery and narrative hypotheses. *Journal of Educational Psychology*, 104 (1).

[9] Ryan, R. M. and Deci, E. L. (2000) Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions. *Contemporary Educational Psychology,* 25, p. 56; Brom, C., Šisler, V. and Slavík, R. (2010) Implementing digital game-based learning in schools: augmented learning environment of 'Europe 2045'. *Multimedia Systems,* 16 (1); Habgood, J. M. P. and Ainsworth, S. E. (2011) Motivating children to learn effectively: Exploring the value of intrinsic integration in educational games. *Journal of the Learning Sciences*, 20.

and compared mental models for EU laws and politics that students constructed in the different environments.

We built our study on the theory of mental models mostly popularized by *Johnson-Laird*, for whom the mental model:

> *"has the same structure as the situation that it represents. Like an architect's model, or a molecular biologist's model, the parts of the model and their structural relations correspond to those of what it represents. […] a mental model is also partial because it represents only certain aspects of the situation.*[10]*"*

Current research defines mental models as intrinsic representations of objects, ideas, or processes which individuals generate during cognitive functioning. The models contain presuppositions about the systems and causal rules and relations between their subsystems. People use these models to reason, describe, explain, predict phenomena, and/or generate expressed models in various formats (e.g. verbal description, diagrams, simulations, or concrete models) to communicate their ideas to others or to solve problems.[11]

Through the analysis of mental models we aimed to provide complex insight into the architecture of learning outcomes within game-based learning. The research question was designed as a casual/effect question seeking *"if and how game-based learning affects the construction and retention of mental models?"* We hypothesized that the game-based educational approach (groups 1 and 2 mentioned above) will have a positive effect on the creation and retention of mental models. Specifically, we expected mental models students created within a game-based learning session to be more extensive and persistent over a longer period of time. The second hypothesis was directed at the digital game-based intervention and postulated that audiovisual elements in digital game-based learning will play a supportive role in the retention of mental models over longer periods of time. Thus, we expected the digital game-based group (group 1 mentioned above) to have more sustainable mental models.

[10] Johnson-Laird, P. (2005) The history of mental models. In: *The Cambridge Handbook of Thinking and Reasoning,* p. 181.

[11] Buckley, B. C. and Boulter, C. J. (2000) Investigating the role of representations and expressed models in building mental models. In: John Gilbert and Carolyn Boulter (eds.). *Developing models in science education.* Netherlands: Kluwer Academic Publishers, pp. 120–123.

The study was conducted as part of a larger research project examining the connection between positive affects triggered by a game and its related learning outcomes.[12] This larger research was based on the experimental design outlined above, but it used extended methods for measuring knowledge gains through pen and paper knowledge tests, as well other methods of knowledge evaluation based on quantitative assessment. The outcomes clearly showed that both game-based approaches led to comparatively higher and – in the one-month observation period – more sustainable knowledge gains. The present study offers new, previously unpublished data based on a qualitative approach while studying participating students' mental models.

We evaluated the mental models using content analysis of concept maps drawn by the participating students: both immediately after the educational intervention and one month later. Through a comparison of those two concept maps we were able to explore structural changes over time. The data indicates that we can follow structural differences in mental models acquired within a digital game-based educational session compared to a non-digital role-playing game and also a traditional lecture with discussions. Students using the digital game showed a remarkably wider tendency to keep their acquired mental model over time. More precisely, when students were asked to create a concept map one month later, those from the digital game group created a map that was 60 % similar to the concept map created right after the workshop (4.4 repeated concepts from 7.2). On the contrary, students taking part in the traditional lecture or the non-digital role-play session tended to rebuild their concept map to a large degree: in their delayed, post-test concept maps they kept less than 50 % of their previous map and more than half of the concepts they added were new (three repeated concepts out of 6.2 in the non-digital role--playing group and 2.9 repeated concepts out of 5.9 in the traditional lecture group).

This article presents not only the results of, but also introduces a possible use for simplified content analysis as a method for evaluating mental model acquisition within different educational environments. As far as we know, content analysis applied within concept map drawing is a method that is not currently applied in research on digital game-based learning.

[12] Brom, C. et al. (2016) You like it, you learn it: affectivity and learning in competitive social role play gaming. *International Journal of Computer-Supported Collaborative Learning,* 11.

Importantly in this regard, our study shows its promising possibilities in this field.

2. THEORETICAL BACKGROUND

2.1. KNOWLEDGE ACQUISITION WITHIN THE CONSTRUCTIVIST APPROACH

In order to understand the world, all humans construct internal representations or mental models that they constantly revise based on new knowledge, ideas, concepts and experiences.[13] *Nersessian* claims that humans – thanks to their linguistic abilities – are able to create these models from a mere description, e.g. an oral description within a traditional lecture or from a lecture book.[14] Constructivists, on the other hand, suggest that theoretical instruction might not be sufficient in this process.[15] They propose experience – or problem-based methods of learning, since the latter provide multiple dimensions of knowledge representation and thus foster multiple interconnections across knowledge components. Additionally, presentation of contradictory understandings and interpretations may help in this process[16]; thus, case studies, debates, individual and group summarizing, and team teaching are appropriate instructional activities for creating efficient mental models. Digital game-based learning processes are very close (similar) to the constructivist point of view.[17]

Mental Models: Overview. The most influential account of the concept of mental models is that of *Johnson-Laird*, who refers to a mental model specifically as a model having the same structure as the situation it represents. In his point of view, mental models are partial because they represent only certain aspects of a situation.[18] Other authors define mental models as intrinsic representations of objects, ideas, or processes, which

[13] Greca, I. M. and Moreira, M. A. (2000) Mental models, conceptual models, and modelling. *International Journal of Science Education*, 22.

[14] Nersessian, N. J. (2002) The cognitive basis of model-based reasoning in science. In: Peter Carruthers, Stephen Stich and Michael Siegal (eds.). *The Cognitive Basis of Science.* Cambridge, UK: Cambridge University Press.

[15] Novak, J. D. and Gowin, B. D. (1984) *Learning how to learn.* Cambridge, UK: Cambridge University Press, p. 161.

[16] Kanuka, H. and Anderson, T. (1999) Using Constructivism in Technology-Mediated Learning: Constructing Order out of the Chaos in the Literature. *Radical Pedagogy*, p. 6.

[17] Li, M. and Tsai, C. (2013) Game-Based Learning in Science Education: A Review of Relevant Research. *Journal of Science Education & Technology*, 22 (6); Rosario, R. M. and Widmeyer, G. R. (2009) An Exploratory Review of Design Principles in Constructivist Gaming Learning Environments. *Journal of Information Systems Education*, 20 (3).

[18] Johnson-Laird, P. (2005) The history of mental models. In: *The Cambridge Handbook of Thinking and Reasoning*, p. 203.

individuals generate during cognitive functioning.[19] The models contain presuppositions about a system and causal rules and relations between its subsystems. People use these models to reason, describe, predict phenomena, and/or generate expressed models in various formats (e.g. verbal description, diagrams, simulations, or concrete models) to communicate their ideas to others; or to solve problems.[20] Mental models are stored in people's long-term memory[21] and are retrieved and mobilized immediately to deal with encountered problems[22]. While doing so, people can construct completely new models in order to accommodate a novel situation.[23] The process of mental simulation means that the models can be manipulated mentally or "run in the mind's eye" to make predictions about outcomes of causal states in the world.[24]

Mental Models: Assessment. To evaluate mental models, *Mayer* proposes written questioning focusing on (near or far) knowledge transfer and mental models' "runnability".[25] Another technique in the assessment of learning processes and mental models themselves is concept mapping.[26] Concept mapping is a tool used to visualize the organization and relationships between various concepts, thoughts and/or theories; it was developed by *Novak* in 1972[27] and later described by *Stewart et al.*[28] Although concept maps are well accepted as a viable assessment tool in qualitative

[19] Buckley, B. C. and Boulter, C. J. (2000) Investigating the role of representations and expressed models in building mental models. In: John Gilbert and Carolyn Boulter (eds.). *Developing models in science education.* Netherlands: Kluwer Academic Publishers, p. 120.

[20] Buckley, B. C. and Boulter, C. J. (2000) Investigating the role of representations and expressed models in building mental models. In: John Gilbert and Carolyn Boulter (eds.). *Developing models in science education.* Netherlands: Kluwer Academic Publishers; Greca, I. M. and Moreira, M. A. (2000) Mental models, conceptual models, and modelling. *International Journal of Science Education*, 22.

[21] Coll, R. K. and Treagust, D. F. (2003) Learners' mental models of metallic bonding: A cross--age study. *Science Education*, 87.

[22] Vosniadou, S. and Brewer, W. (1992) Mental models of the Earth: A study of conceptual change in childhood. *Cognitive Psychology*, 24, p. 543.

[23] Johnson-Laird, P. (1983) *Mental models.* Cambridge: MA: MIT Press, pp. 444–448.

[24] Vosniadou, S. and Brewer, W. (1992) Mental models of the Earth: A study of conceptual change in childhood. *Cognitive Psychology*, 24, p. 537

[25] Mayer, R. E. Dyck, J. and Cook, L. K. (1984) Techniques that help readers build mental models from scientific text: Definitions pretraining and signaling. *Journal of Educational Psychology*, 78 (6), p. 1091.

[26] Besterfield-Sacre, M. et al. (2004) Scoring concept maps: An integrated rubric for assessing. *Journal of Engineering Education*, 93 (2).

[27] Novak, J. D. and Cañas, A. J. (2008) *The theory underlying concept maps and how to construct and use them.* Pensacola: Florida Institute for Human and Machine Cognition.

[28] Stewart, J., Van Kirk, J. and Rowell, R. (1979) Concept maps: A tool for use in biology teaching. *American Biology Teacher*, 41 (3).

educational research, there is no general agreement on a scoring technique.[29] A number of researchers have attempted to develop accurate methods for assessing concept maps. The most traditional one was developed by *Mintzes et al.*, who evaluated concept maps through the inner connections between their sub-concepts, i.e. they evaluated the validity of the connections and determined the latter's super/subordinate nature.[30] Another approach was proposed by *Bayram*, who focused more on the whole structure of a map.[31] He proposed a point system based on the map's hierarchical levels, correct propositions, and branches. One point was given for each hierarchical level; each relationship between concepts established by a correct connection. *Ruiz-Primo et al.* combined *Novak's* and *Bayram's* approaches and related each map to a criterion map created by an expert.[32] The evaluation afterwards consists of measuring the degree of similarity to the expert map (*expert map comparison*). This method is mostly used in pedagogical research and the evaluation of educational goals.

Theories of Mental Models and Digital Games. A number of experiments have investigated the mental processes of literature readers and confirmed the hypothesis that readers spontaneously construct mental models to represent and reason about situations depicted in the text.[33] Readers mostly imagined situations by "being in the place of an observer".[34] There remain questions about what kind of experience can be created by a game (digital or non-digital) and what differences it brings to mental modelling processes and their outcomes. Digital games, considered a medium for the representation of information, offer novel ways to represent complex models and themes; they create new environments for perceiving new kinds of information and experiences. Similar to mental models, game

[29] Yun Soo, L., Yongkyu, J. and Minsoo, K. (2015) Validity and Responsiveness of Concept Map Assessment Scores in Physical Education. *Physical Educator*, 72 (2); Besterfield-Sacre, M. et al. (2004) Scoring concept maps: An integrated rubric for assessing. *Journal of Engineering Education*, 93 (2).

[30] Mintzes, J. J., Wandersee, J. H. and Novak, J. D. (2001) Assessing understanding in biology. *Journal of Biological Education*, 35 (3).

[31] Bayram, S. (1995) *The effectiveness of concept and software mapping for representing student data and process schema in science.* Thesis. University of Pittsburgh.

[32] Ruiz-Primo, M. A. et al. (2001) On the validity of cognitive interpretations of scores from alternative concept-mapping techniques. *Educational Assessment*, 7 (2), p. 11.

[33] Johnson-Laird, P. (1983) *Mental models.* Cambridge: MA: MIT Press, pp. 396–479; Zwann, R. A and Radvansky, G. A. (1998) Situation models in language comprehension and memory. *Psychological Bulletin*, 123, pp. 396–400.

[34] Nersessian, N. J. (2008) Mental modeling in conceptual change. In: Stella Vosniadou (ed.). *International handbook of research in conceptual change.* New York: Routledge, p. 24.

mechanics define all possible functions and relationships in a system. They also influence a game's playability. In this regard, *Boyan* postulates that to master the in-game challenges, a player must create a mental model of the intrinsic obstacles in the game world: a model that is similar or identical to the true computer game model.[35] Well-designed educational games constantly test players' prior mental models and embody the process of cognitive disequilibrium and resolution; they foil expectations (create cognitive disequilibrium) without exceeding the player's capacity to succeed. Interacting with a game typically requires a constant cycle of hypothesis formulation, testing, and revision.[36] Traditional lectures influence the creation and conceptual change of mental models through theoretical description, explanation, questioning, and discussion. Games, on the contrary, immerse their users directly in the topic and let them create, recreate and test mental models through (inter)action.

Similarly, the theory of multimedia learning proposes that multimedia platforms play an important role in knowledge acquisition and mental modelling.[37] The the process of transferring knowledge to long-term memory and its further reconstruction are still not clear. However, new memory models and the theory of multimedia learning provide a so-called embedded processes model. This model argues that working memory is not a separate cognitive system but is the activated part of long-term memory.[38] Activation is therefore supported by focusing one's attention (voluntary and involuntary) which, particularly in multimedia learning, is strengthened by using positive, or strongly connected, images.[39] Our study's research question and hypotheses are built on this theoretical background.

[35] Boyan, A. and Sherry, J. L. (2011) The Challenge in Creating Games for Education: Aligning Mental Models with Game Models Child Development Perspectives. *The Society for Research in Child Development*, 5 (2), p. 5.

[36] Van Eck, R. (2006) Digital Game-Based Learning: It's Not Just Digital Natives Who Are Restless. *Educause Review*, 41 (2).

[37] Mayer, R. E. and Johnson, C. I. (2010) Adding instructional features that promote learning in a game-like environment. *Educational computing research*, 42 (3).

[38] Schweppe, J. and Rummer, R. (2014) Attention, Working Memory, and Long-Term Memory in Multimedia Learning: An Integrated Perspective Based on Process Models of Working Memory. *Educational Psychology Review*, 26.

[39] Schneider, S. et al. (2018) Anthropomorphism in decorative pictures: benefit or harm for learning? *Journal of Educational Psychology,* 110 (2); Plass, J. and Kaplan, U. (2016) Emotional Design in Digital Media for Learning. In: Sharon Tettegah and Martin Gartmeier (eds.). *Emotions, Technology, Design, and Learning.*

2.2. PRESENT STUDY

Building on the current findings mentioned earlier[40] and the theory of mental models mainly popularized by *Johnson-Laird*[41], we decided to test their theoretical postulates. Our research question asks if and how does game-based learning affect the construction and retention of mental models.

We were mostly interested in real schooling possibilities, so we closely copied a typical, formal schooling environment and used teaching approaches accessible to today's teachers. We compared three different educational environments while adopting a controlled experiment design with one experimental and two control groups: (1) a digital game (the experimental group) containing strong connected visuals and an interactive simulation model; (2) a non-digital role-playing game copying the digital game but without PCs and lacking the multimedia visual element; and (3) a traditional lecture with discussions.

We hypothesized (our first hypothesis) that the game-based educational approach (groups 1 and 2 mentioned above) will have a positive effect on the creation and retention of students' mental models. Specifically, we expected the mental models that students created within a game-based learning session to be more extensive and persistent over a longer period of time. In other words, after one month, both game-based groups will lose a smaller part of their mental model. Afterwards, we expected (our second hypothesis) that the audiovisual elements so typical for digital game-based learning will play a supportive role in the retention of mental models. Thus, we anticipated that the digital game-based group (group 1 mentioned above) would have more sustainable mental models, i.e. after one month a significantly larger part of their mental model would remain unchanged.

This study used a mix of qualitative and quantitative approaches. Therefore, we present their development and our use of a simplified content analysis applied to the interpretation of concept maps. This approach can be considered a method for evaluating mental model acquisition within different educational environments. In the discussion we describe its limitations and potential for future research.

[40] Ibid.

[41] Johnson-Laird, P. (2005) The history of mental models. In: *The Cambridge Handbook of Thinking and Reasoning*, pp. 185–187.

3. METHODS

3.1. RESEARCH INSTRUMENT: EUROPE 2045

We used a modified version of the educational simulation *Europe 2045*[42] as a research instrument. The game has three educational goals: (1) to improve students' high-level skills, i.e. to increase their ability to discuss, negotiate, work in teams, and make group decisions; (2) to familiarize students with facts (such as the geographies of European countries, EU institutions and policies, typologies of political inclinations); and (3) help students acquire mental models of large-scale processes and socio-political notions (such as a model of "energy dependence" or "liberalism").

Europe 2045 was released in 2008 and was successfully integrated into the formal schooling system.[43] Up to now, the game has been used in dozens of Czech high schools and played by more than 4,000 students. *Europe 2045* was modified for the purposes of this experimental research.

The modified game was limited to eight players and combined the principles of multi-player online videogames and social role-playing games. One part of the game is played in a multi-user virtual environment (on a PC) and the second part in a classroom where role-playing game activities take place. A teacher is always present and takes on the role of discussion moderator.

In the beginning, each user chooses a project in the game to play out (e.g. Social Europe – Social Democracy, Liberal Europe – Liberalism, etc.). The project is a vision of how the EU should look in the future. Therefore, players need to achieve structural changes to bring the EU closer to their project goal. The project is always related to one EU member state that students are chosen to represent; they define that country's domestic policy. Students also take on the role of an EU representative and have an opportunity to present drafts for policy changes to EU governing bodies. Discussions about these changes take place in the classroom and can be conceived as a simulation of official EU negotiations within institutions: such as the *European Parliament*, the *Council of Europe*, and the *Foreign Affairs Council*. The winners of the game are the students who pushed through

[42] Šisler, V. and Brom, C. (2008) Designing an Educational Game: Case Study of 'Europe 2045'. *Transactions of Edutainment I*, 5080.

[43] Brom, C., Šisler, V. and Slavík, R. (2010) Implementing digital game-based learning in schools: augmented learning environment of 'Europe 2045'. *Multimedia Systems*, 16 (1).

or refused as many policy changes as possible in order to re-create the EU according to their project's vision. Players can also support votes for their policies by creating informal pacts with other state leaders. The game features both collaborative and competitive aspects at the same time. Throughout the game, students face global situations represented by the game scenario. The game was played during a one-day workshop and game-play lasted about four hours.

3.2. RESEARCH DESIGN

The present study was part of a larger experiment examining the connection between positive affects triggered by a game and learning outcomes therefrom.[44] This study was based on set of pen and paper knowledge tests that were distributed at the same time as the task for drawing mentioned concept maps.

The timetable and all workshop activities were strictly defined, so we could assure comparability of research variables in all the groups. The same amount of time was dedicated to learning activities, frontal teaching sessions, pauses, similar vocabulary and communication styles, etc. To avoid environmental issues that might threaten the study's reliability, we chose a laboratory design – the experiment did not take place at students' ordinary schools but rather in classrooms at *Charles University* and teachers were hired specifically for the experiment. To minimize possible bias caused by specific teacher personalities, we worked with a group of eight teachers: all males younger than 35 years of age, with a similar clothing style, short hair, and similar speech and teaching styles. These teachers rotated through different classrooms and taught in all three types of research groups. Within the experiment, we organized 14 workshop days (six hours); always for one high school class (15–16 participants).

Distribution of students into subgroups was not random. In order to have a comparable sample, participants were asked to fill out a pre--questionnaire assessing their knowledge of EU affairs after a short introduction to the project. Students with similar results were grouped and then assigned randomly to the experimental conditions. Thus, each subgroup had the same proportion of students with each level

[44] Brom, C. et al. (2016) You like it, you learn it: affectivity and learning in competitive social role play gaming. *International Journal of Computer-Supported Collaborative Learning*, 11.

of knowledge. Gender was also taken into account; each group had similar gender representation. Students participated in only one selected treatment: digital game, non-digital game, or traditional lecture with discussions.

Digital game-based treatment. Students played the modified PC version of the game *Europe 2045*. The rounds of the game always had a similar design: four players selected by a computer were to propose a draft for a policy change; they had eight minutes to study the materials related to the game (mainly the online encyclopedia). The rest of the students could control their state or read materials about policies associated with their own projects or about policies proposed by the other four players. Afterwards, they were invited to turn away from the computer screens, and each student assigned to propose a policy change had exactly 1.5 minutes to introduce the policy and present its benefits. After that, there was an open discussion moderated by the teacher (2–3 minutes). When all four proposals were presented, there were five minutes of overall negotiations where the teacher challenged students to leave their seats and discuss ideas with other players individually. In the end, students voted separately on their own computers. The teacher presented the results at the beginning of the next round along with the players' current rankings in the game. The students played six rounds; always with eight students taking part.

Non-digital role-playing game. Students played the game *Europe 2045* as a social role-playing game without PCs. This set-up copied the activities of the experimental game group but computer use was avoided. The voting system was simulated directly in the classroom using a voting urn. The in-game textual materials (encyclopedia texts) were printed out and distributed to the players. The schedule and the content were exactly the same as in the experimental game group except that players did not have the opportunity to control their state. Six to eight students took part.

Traditional lecture with discussions. Students did not play any game, but in the workshop the same content as used in the two previous groups was shared with students through non-game-based learning techniques: a traditional lecture and discussions about EU policies and projects. Since these students did not vote on policy drafts and did not interact with a European state model, the whole workshop for the traditional lecture control group was shorter. The game's introductory simulated scenario was replaced by an unrelated 40-minute-long frontal lecture on the EU and by a 20-minute-long, pen-and-paper mini-rebus about EU law. The content of those additional activities was not related to the experimental research topic and was not tested via concept maps. Six to ten students took part.

3.3. RESEARCH APPARATUS

Students' mental models were examined through concept maps that students drew right after the learning sessions (maps #1) and one month later (maps #2). There was one more map created before the educational workshop (maps #0), but those were not analyzed. They served only as a training tool to assure the same level of understanding and experience with concept maps among all students.

For the evaluation, only participants who attended the educational workshop and the one month delayed testing sessions (so we could compare both maps #1 and #2) were chosen. Concept maps from 253 subjects were evaluated; 84 from the experimental digital game group, 99 from the control traditional lecture group and 70 from the control non--digital role-playing game group.

As mentioned above, at the very beginning of the educational workshop, students were asked to read a three- to four-sentence summary of eight political projects (each was a specific political project, e.g. liberal, conservative, environmental, multicultural, etc.) and choose three projects that interested them. After that, they were assigned one project. For their concept map, students got an empty sheet with an ellipse in the middle and the following instructions: *"Write in the empty ellipse the name of the political philosophy you were reading about today. In the surrounding area write the key concepts related to this philosophy."* Before map creation, the teacher presented the following instructions: *"For my mental map, I chose anarchism. Actually, I just recently saw a documentary on anarchism, so I know a lot about it... What am I thinking of now?"* … writes "Anarchism"' into the ellipse. *"On which side of the political spectrum?"* … writes "radical left" and connects it directly to "Anarchism". *"As it is on the left side of the political spectrum, it tries to enforce…"* … writes "social justice" and connects it directly to "radical left". *"Everyone has probably heard of…"* … writes "Sex Pistols" and connects it directly to "Anarchism". *"I think its origin is…"* … writes "France" and connects it directly to "Anarchism", etc.

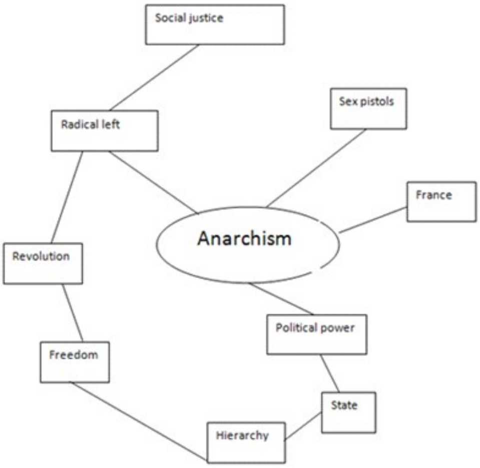

Diagram 1: Concept map drawn by teacher as an instructional example

Within the evaluation, we applied the traditional quantitative measures of content analysis: keyword frequencies and spatial measurements for maps (branching, subcategorizing).[45] Two evaluators independently analyzed each entry word in map #1 and followed its development in map #2. The base value for the content analysis was a "sub-concept", a fragment of a concept map related to one specific theme (so it could contain more than one entry). For example, in the exemplary concept map described above (see Diagram 1) eight entries would have been counted: (1) political power + state; (2) hierarchy; (3) France; (4) Sex Pistols; (5) freedom; (6) revolution; (7) radical left; and (8) social justice.

Content analysis of maps #1. We utilized two categories for evaluating sub--concepts in maps #1: (1) relevant, (2) irrelevant (unrelated to the theme). Thus, the first step in the content analysis consisted merely of evaluating and quantifying the incorporated sub-concepts.

Content analysis of maps #2. In the evaluation of maps #2, we made comparisons with maps #1 (those made by similar students). Therefore, we used six categories for the sub-concepts: (1) forgotten (present in map #1 but not in map #2); (2) remained unchanged; (3) changed to "upgraded" form (the sub-concept in map #2 was in a more apposite position or more appropriate and/or developed phrase than in map #1); (4) changed to a "downgraded" form (a less apposite position or less appropriate and/or

[45] Neuendorf, K. (2002) *The Content Analysis Guidebook.* Thousand Oaks, CA: Sage Publications, pp. 212–214.

developed phrase than in map #1); (5) new (present in maps #2 but not present in maps #1); (6) irrelevant.

We considered entries or groups of entries that developed or concretized the entries from map #1 to be upgraded sub-concepts in maps #2. For example "P.-J. Proudhon" drawn as an additional branch to "France" would be considered an upgraded sub-concept (see Diagram 1). The student had developed a hierarchy branching into the upper class. Additionally, "punk rock movement" written in map #2 instead of "Sex Pistols" in map #1 would be considered an upgraded sub-concept, because it puts forward a general concept that concretizes social forces that helped disseminate anarchist ideas in the 1970s.

The downgraded sub-concepts lacked a rich branching or were more reductive in comparison with their corresponding values in map #1. For instance, were "social justice" missing in map #2 that would be considered a downgraded sub-concept. "No-government" written instead of "political power" and/or "state" would be considered a downgraded sub-concept as well. In such cases, the student used a simplified concept that did not represent the issue's complexity.

Indeed, the comparison between individual maps #1 and maps #2 was crucial for the analysis. Additional qualitative analysis was also used to explain differences in greater detail, i.e. the character of the content was evaluated; trends in the maps' content were described.

4. RESULTS

Two raters evaluated each map independently. To ensure evaluation reliability, their outcomes were compared to each other using an internal consistency test, *Cronbach's* alpha (α). This test can show possible statistical variability in evaluations. All values were higher than 0.7, thus statistically consistent. The average α for all results was α = 0.931. So for the final evaluation we used the mean values from both raters. To analyze the differences in the group means in the three conditions we used the one--way ANOVA test with a statistical significance $p < .05$. When the ANOVA showed a significant difference, we applied a Tukey HSD range test to identify which means (group conditions) resulted from others and by how much. The rest of the data was commented in discussions.

Group		Maps #1 entries	Irrelevant entries
Digital game	M	8.45	0.33
	SD	2.87	0.71
Traditional lecture	M	7.19	0.56
	SD	2.67	1.23
Non-digital game	M	7.46	0.65
	SD	2.56	1.19

Table 1: Maps #1 descriptive statistics

Further analysis of the maps #1 (see Table 1) reveals the influence of the educational approach on the extensiveness of the concept maps and on the amount of relevant sub-concepts included. Maps #1 created by students who played the digital game included more entries (the concept maps were bigger and more branched) than those created by students who followed the role-play based game or the traditional lecture with in-class discussions. There was a statistically significant effect, with small effect size from type of educational activity on the extensiveness of students' mental models at the $p < .05$ level for the three conditions, $F(2, 250) = 5.218$, $p = .006$, $\eta 2 = .040$. Post hoc comparisons using the Tukey HSD test indicated that the mean score for the amount of concept map entries in the digital game treatment ($M = 8.45$, $SD = 2.87$) was significantly higher than for the non--digital role-playing game and traditional lecture treatments. The non--digital role-playing game mean score was 7.46 ($SD = 2.56$) and the traditional lecture mean score was 7.20 ($SD = 2.67$) for sub-concepts. The amount of irrelevant entries in the concept maps #1 was comparable across all three groups $F(2, 250) = 1.837$, $p = 0.161$, $\eta 2 = .014$.

After one month, all students lost a roughly constant amount of knowledge (missing entries in concept maps #2), thus the difference in the map size remained: the mean score for the digital game treatment was 7.21 ($SD = 2.79$), for the non-digital role-playing game 6.18 ($SD = 2.35$), and for the traditional lecture 5.90 ($SD = 2.92$).

Group		Maps #2 entries	New	Repeated	Repeated – upgraded	Repeated – downgraded	Irrelevant
Digital Game	M	7.21	2.79	4.42	0.45	0.07	0.17
	SD	2.79	1.79	2.09	0.66	0.26	0.45
Traditional lecture	M	5.90	3.03	2.88	0.07	0.05	0.51
	SD	2.92	2.11	1.96	0.29	0.24	0.90
Non-digital game	M	6.18	3.15	3.03	0.06	0.13	0.59
	SD	2.35	1.77	1.91	0.29	0.36	0.99

Table 2: Maps #2 descriptive statistics

Content analysis of the maps #2 (see Table 2) revealed a significantly higher amount of repeated concepts (concepts that stayed in unchanged form compared to maps #1) with large effect size in the digital game group. There was a statistically significant effect (caused by the type of educational activity) on the number of repeated concepts in the maps referring to the stability of students' mental models; F(2, 250) = 15.565, p = .00, η2 = 111. Post hoc comparisons using the Tukey HSD test indicated that the mean score for the digital game treatment (M = 4.42, SD = 2.09) was significantly higher than for the non-digital role-playing game treatment (M = 3.03, SD = 1.91) and the traditional lecture treatment (M = 2.88, SD = 1.96).

The digital game group seemed to build on knowledge gained during the educational workshop and did not create a new concept map – let us say mental model – when asked to present their knowledge. In comparison, maps #2 in the traditional lecture group and the non-digital role-playing group contained more new entries than those repeated from maps #1.

There was always a low proportion of irrelevant, upgraded or downgraded sub-concepts. So we did not use advanced statistical measurements.

5. DISCUSSION

Content analysis of students' concept maps revealed structural differences in mental models for students learning with the digital game compared to students learning with the non-digital role-playing game and traditional schooling methods. Those interacting with the digital game were obviously willing to put more sub-concepts into their concept maps – they drew larger and more branched maps. Although all three groups lost approximately the same amount of knowledge during the one-month period prior to the delayed testing, the large size of maps from the digital game-based group lasted. This might be caused by better involvement in learning supported by higher affective engagement with the digital game-based learning platform; i.e. as some previous research proposes.[46]

On the other hand, a mere number of sub-concepts integrated into a map does not directly mean better quality of the maps; and thus of mental models. As we have mentioned above, this study was part of a larger experimental study using the same research design as described above (for more details see Section 3.3.).[47] Unlike the present study, knowledge gains in the larger experimental study were assessed based on different, mostly quantitative measures. The outcomes of the larger experimental study showed that both game-based approaches led to comparatively higher and more sustainable knowledge gains: as observed in the one-month, post-experiment period.[48]

In the context of these outcomes, we can assume that the significantly higher extensiveness of the concept maps created by the digital game-based group was not a characteristic of knowledge quality but rather a reflection on media used. The quantity of concepts in the digital game-based group was boosted mostly by the fact that students also imported unimportant details about discussed policies and agendas: content that is an inherent part of the graphical user interface in the digital game. Players were repeatedly exposed to this content; thus, it seems that those details stayed imprinted in their memories.

When analyzing the concept maps one month later, we could observe a decline of retention over time. All groups copied a similar forgetting curve; all three groups lost approximately the same amount of concepts: the digital game group lost 14.65 %, the non-digital role-playing game group lost 17.23 %, and the traditional lecture group 17.97 %.

Otherwise, the key outcome was that students who learned with the digital game tended rather to use the model they gained through

[46] Wouters, P. et al. (2013) A Meta-Analysis of the Cognitive and Motivational Effects of Serious Games. *Journal of Educational Psychology.* Advance online publication; Um, E. et al. (2012) Emotional Design in Multimedia Learning. *Journal of Educational Psychology*, 104 (2).

[47] Brom, C. et al. (2016) You like it, you learn it: affectivity and learning in competitive social role play gaming. *International Journal of Computer-Supported Collaborative Learning*, 11.

[48] Ibid.

the workshop: their maps #1 (after the educational workshop) and #2 (one month later) contained a high amount of similar entries (61.22 %). By contrast, students from the other two groups produced second concept maps considerably different from their first ones. The non-digital role-playing game group used on average 50.98 % new concepts (49.02 % similar ones) and the traditional lecture group 51.24 % new concepts (48.76 % similar ones). It seems that their mental models are not as stable and do not last over time. Rather, one month later, students created a new model "on demand" when asked to do so. With regard to that point, our content analysis does not predicate on the quality of the students' knowledge, but rather the structure thereof. The fact that students use similar keywords, concepts and connections indicates that their mental model is more integrated and stable within their long-term memory.

As discussed above, the comparison with the expert maps proposes that the digital as well as the non-digital role-playing game leads to comparable quality of mental models. But content analysis shows that the media used within the game-based learning approach influences the way users work with acquired knowledge over the long-term. Such an outcome supports theories where multimedia platforms play an important role in knowledge acquisition and mental modelling.[49] It seems that digital games that include additional audiovisual cues help create a long-lasting mental model that is easily recalled even after one month. Such an outcome confirms theories of strengthened focus of attention when using in-game positive or strongly connected pictures.[50]

Within this framework, our research provides preliminary evidence suggesting possible significant impact of multimedia learning on the process of mental model construction. Additional multimedia material seems to help students integrate greater amounts of information and construct viable mental models in their long-term memory: ones that are easily accessible over time. Furthermore, content analysis of concept maps seems to be a helpful tool for developing an understanding of mental

[49] Mayer, R. E. and Johnson, C. I. (2010) Adding instructional features that promote learning in a game-like environment. *Educational computing research*, 42 (3).

[50] Schneider, S. et al. (2018) Anthropomorphism in decorative pictures: benefit or harm for learning? *Journal of Educational Psychology*, 110 (2); Plass, J. and Kaplan, U. (2016) Emotional Design in Digital Media for Learning. In: Sharon Tettegah and Martin Gartmeier (eds.). *Emotions, Technology, Design, and Learning.*

model development. Current digital game-based research provides mixed results.

This study contributes to the research community mainly by providing new insight for mental modelling; especially, for persons interested in multimedia learning and cognitive theories of learning within digital game-based learning. The results are particularly viable for formal education on EU law, institutions and politics at the high school level.

LIST OF REFERENCES

[1] Adams, D. M. et al. (2012) Narrative games for learning: Testing the discovery and narrative hypotheses. *Journal of Educational Psychology*, 104 (1), pp. 235–249.

[2] Baroncelli, S., Farneti, R. and Vanhoonacker, S. (2014) Introduction – Teaching European Studies: Educational Challenges. In: Stefania Baroncelli, Roberto Farneti, Ioan Horga and Sophie Vanhoonacker (eds.). *Teaching and Learning the European Union: Traditional and Innovative Methods.* Dordrecht: Springer, pp. 157–185.

[3] Bayram, S. (1995) *The effectiveness of concept and software mapping for representing student data and process schema in science.* Thesis. University of Pittsburgh.

[4] Besterfield-Sacre, M. et al. (2004) Scoring concept maps: An integrated rubric for assessing. *Journal of Engineering Education*, 93 (2), pp. 105–115.

[5] Boyan, A. and Sherry, J. L. (2011) The Challenge in Creating Games for Education: Aligning Mental Models with Game Models Child Development Perspectives. *The Society for Research in Child Development*, 5 (2), pp. 82–87.

[6] Brom, C., Šisler, V. and Slavík, R. (2010) Implementing digital game-based learning in schools: augmented learning environment of 'Europe 2045'. *Multimedia Systems*, 16 (1), pp. 23–41.

[7] Brom, C. et al. (2016) You like it, you learn it: affectivity and learning in competitive social role play gaming. *International Journal of Computer-Supported Collaborative Learning*, 11, pp. 313–348.

[8] Buckley, B. C. and Boulter, C. J. (2000) Investigating the role of representations and expressed models in building mental models. In: John Gilbert and Carolyn Boulter (eds.). *Developing models in science education.* Netherlands: Kluwer Academic Publishers, pp. 119–135.

[9] Clark, D. B., Tanner-Smith, E. E. and Killingsworth, S. S. (2016) Digital Games, Design, and Learning: A Systematic Review and Meta-Analysis. *Review of Educational Research*, 86 (1), pp. 79–122.

[10] Coll, R. K. and Treagust, D. F. (2003) Learners' mental models of metallic bonding: A cross-age study. *Science Education*, 87, pp. 685–707.

[11] Greca, I. M. and Moreira, M. A. (2000) Mental models, conceptual models, and modelling. *International Journal of Science Education*, 22, pp. 1–11.

[12] Habgood, J. M. P. and Ainsworth, S. E. (2011) Motivating children to learn effectively: Exploring the value of intrinsic integration in educational games. *Journal of the Learning Sciences*, 20, pp. 169–206.

[13] Johnson-Laird, P. (1983) *Mental models.* Cambridge: Cambridge University Press.

[14] Johnson-Laird, P. (2005) The history of mental models. In: *The Cambridge Handbook of Thinking and Reasoning*, pp. 179–212.

[15] Jones, R. and Bursens, P. (2014) Assessing EU Simulations: Evidence from the Trans--Atlantic EuroSim. In: Stefania Baroncelli, Roberto Farneti, Ioan Horga and Sophie Vanhoonacker (eds.). *Teaching and Learning the European Union: Traditional and Innovative Methods.* Dordrecht: Springer, pp. 157–185.

[16] Kanuka, H. and Anderson, T. (1999) Using Constructivism in Technology-Mediated Learning: Constructing Order out of the Chaos in the Literature. *Radical Pedagogy.*

[17] Li, M. and Tsai, C. (2013) Game-Based Learning in Science Education: A Review of Relevant Research. *Journal of Science Education & Technology*, 22 (6), pp. 877–898.

[18] Mayer, R. E., Dyck, J. and Cook, L. K. (1984) Techniques that help readers build mental models from scientific text: Definitions pretraining and signaling. *Journal of Educational Psychology*, 78 (6), pp. 1089–1106.

[19] Mayer, R. E. and Johnson, C. I. (2010) Adding instructional features that promote learning in a game-like environment. *Educational computing research*, 42 (3), pp. 241–265.

[20] Mintzes, J. J., Wandersee, J. H. and Novak, J. D. (2001) Assessing understanding in biology. *Journal of Biological Education*, 35 (3), pp. 118–124.

[21] Moreno, R. and Mayer, R. (2007) Interactive multimodal learning environments: Special issue on interactive learning environments: Contemporary issues and trends. *Educational Psychology Review*, pp. 309–326.

[22] Münchow, H., Mengelkamp, C. and Bannert, M. (2017) The better you feel the better you learn: Do warm colours and rounded shapes enhance learning outcome in multimedia learning? *Education Research International.*

[23] Nersessian, N. J. (2002) The cognitive basis of model-based reasoning in science. In: Peter Carruthers, Stephen Stich and Michael Siegal (eds.). *The Cognitive Basis of Science.* Cambridge, UK: Cambridge University Press, pp. 133–153.

[24] Nersessian, N. J. (2008) Mental modeling in conceptual change. In: Stella Vosniadou (ed.). *International handbook of research in conceptual change.* New York: Routledge, pp. 391–416.

[25] Neuendorf, K. (2002) *The Content Analysis Guidebook.* Thousand Oaks, CA: Sage Publications.

[26] Novak, J. D. and Cañas, A. J. (2008) *The theory underlying concept maps and how to construct and use them.* Pensacola: Florida Institute for Human and Machine Cognition.

[27] Novak, J. D. and Gowin, B. D. (1984) *Learning how to learn*. Cambridge, UK: Cambridge University Press, pp. 133–143.

[28] Plass, J. and Kaplan, U. (2016) Emotional Design in Digital Media for Learning. In: Sharon Tettegah and Martin Gartmeier (eds.). *Emotions, Technology, Design, and Learning*, pp. 131–162.

[29] Rosario, R. M. and Widmeyer, G. R. (2009) An Exploratory Review of Design Principles in Constructivist Gaming Learning Environments. *Journal of Information Systems Education*, 20 (3), pp. 289–300.

[30] Ruiz-Primo, M. A. et al. (2001) On the validity of cognitive interpretations of scores from alternative concept-mapping techniques. *Educational Assessment*, 7 (2), pp. 99–141.

[31] Ryan, R. M. and Deci, E. L. (2000) Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions. *Contemporary Educational Psychology*, 25, pp. 54–67.

[32] Schneider, S. et al. (2018) Anthropomorphism in decorative pictures: benefit or harm for learning? *Journal of Educational Psychology*, 110 (2), pp. 218–232.

[33] Schweppe, J. and Rummer, R. (2014) Attention, Working Memory, and Long-Term Memory in Multimedia Learning: An Integrated Perspective Based on Process Models of Working Memory. *Educational Psychology Review*, 26, pp. 285–306.

[34] Sitzmann, T. (2011) A Meta-Analytic Examination of the Instructional Effectiveness of Computer-Based Simulation Games. *Personnel Psychology*, 64 (2), pp. 489–528.

[35] Stewart, J., Van Kirk, J. and Rowell, R. (1979) Concept maps: A tool for use in biology teaching. *American Biology Teacher*, 41 (3), pp. 171–175.

[36] Šisler, V. and Brom, C. (2008) Designing an Educational Game: Case Study of 'Europe 2045'. *Transactions of Edutainment I*, 5080, pp. 1–16.

[37] Švaříček, R., Šeďová, K. and Šalamounová, Z. (2012) *Komunikace ve školní třídě.* Praha: Portál.

[38] Tobias, S. and Fletcher, D. (2011) Learning from Computer Games: A Research Review. In: Stefan De Wannemacker, Sylke Vandercruysse and Geraldine Clarebout (eds.). *Serious Games: The Challenge. Communications in Computer and Information Science*, Springer, Berlin, Heidelberg, pp. 6–17.

[39] Um, E. et al. (2012) Emotional Design in Multimedia Learning. *Journal of Educational Psychology*, 104 (2), pp. 485–498.

[40] Van Eck, R. (2006) Digital Game-Based Learning: It's Not Just Digital Natives Who Are Restless. *Educause Review*, 41 (2), pp. 16–30.

[41] Vosniadou, S. and Brewer, W. (1992) Mental models of the Earth: A study of conceptual change in childhood. *Cognitive Psychology*, 24, pp. 535–585.

[42] Wouters, P. et al. (2013) A Meta-Analysis of the Cognitive and Motivational Effects of Serious Games. *Journal of Educational Psychology.* Advance online publication, pp. 249–265.

[43] Yun Soo, L., Yongkyu, J. and Minsoo, K. (2015) Validity and Responsiveness of Concept Map Assessment Scores in Physical Education. *Physical Educator*, 72 (2), pp. 206–223.

[44] Zwann, R. A and Radvansky, G. A. (1998) Situation models in language comprehension and memory. *Psychological Bulletin*, 123, pp. 162–185.

DOI 10.5817/MUJLT2020-1-3

THE COMPLEXITY OF CRIMINAL LIABILITY OF AI SYSTEMS[*]

by

NORA OSMANI[**]

Technology is advancing at a rapid pace. As we anticipate a rapid increase in artificial intelligence (AI), we may soon find ourselves dealing with fully autonomous technology with the capacity to cause harm and injuries. What then? Who is going to be held accountable if AI systems harm us?

Currently there is no answer to this question and the existing regulatory framework falls short in addressing the accountability regime of autonomous systems. This paper analyses criminal liability of AI systems, evaluated under the existing rules of criminal law. It highlights the social and legal implications of the current criminal liability regime as it is applied to the complex nature of industrial robots. Finally, the paper explores whether corporate liability is a viable option and what legal standards are possible for imposing criminal liability on the companies who deploy AI systems.

The paper reveals that traditional criminal law and legal theory are not well positioned to answer the questions at hand, as there are many practical problems that require further evaluation. I have demonstrated that with the development of AI, more questions will surface and legal frameworks will inevitably need to adapt. The conclusions of this paper could be the basis for further research.

KEY WORDS

Artificial Intelligence, Autonomous Systems, Criminal Law, Criminal Liability

[*] This article was supported by ERDF *"CyberSecurity, CyberCrime and Critical Information Infrastructure Center of Excellence"* (No. CZ.02.1.01 / 0.0 / 0.0 / 16_019 / 0000822). The author would like to thank *Professor Radim Polcak* for his guidance and constructive comments while preparing this article for publication.

[**] osmani.nora@hotmail.com, PhD Candidate, Faculty of Law, Ss. Cyril and Methodius University, Skopje, Republic of North Macedonia; visiting researcher at Masaryk University, Brno, The Czech Republic.

1. INTRODUCTION

Robotics and AI are moving towards a Cambrian explosion,[1] given the explosive and rapid developments in the field. A lot of countries have recognized the enormous importance of the AI industry[2] and are now actively competing for the global AI market.[3] In terms of revolution, machine learning created the ability for AI entities to accumulate experience and learn from it.[4] During an experiment, researchers from the *Georgia Tech Institute* fielded two autonomous aircraft (auto-piloted airplanes), which shared and communicated information to each other using data communication software and Wi-Fi systems; thus no human control was involved whatsoever.[5]

The self-development ability of AI systems presents society with machines that have their own needs and goals, referred to in the literature as *Artificial Super Intelligence (ASI)*.[6] These thinking machines[7] can act directly upon their environment,[8] thus raising questions about liability for

[1] Pratt, GA. (2015) Is a Cambrian Explosion Coming for Robotics?. *Journal of Economic Perspectives*, 29 (3), p. 55.

[2] Countries such as: Germany, Switzerland, Canada, Hong Kong, Singapore, South Korea, France, United Arab Emirates, Japan, Russia, and Israel aspire to participate in the global AI market and are actively supporting the development of the AI industry through their tech--hubs. For more information, see: Deep Knowledge Analytics. (2018) *Artificial Intelligence Industry in the UK*. [online] London: DKA. Available from: https://www.dka.global/ai-in-uk-report [Accessed 12 May 2019].

[3] China and the US remain the leaders of the AI race, but they are actively competing to outperform each other and to become leaders in the global IT market. Chinese President *Xi Jinping* has committed $150 billion in government funding in order to make China the undisputed global leader in the AI race by 2030. Ibid.

[4] Machine learning is described as an inductive method of learning in which the AI system analyses various given data and identifies patterns for future use without being explicitly programmed for that purpose. In this sense, the computer's behaviour is not predictable by either the operator–owner or the original programmers. See, e.g., Vojislav, K. (2001) *Learning and Soft Computing: Support Vector Machines, Neutral Networks and Fuzzy Logic Models*. Cambridge: The MIT Press; Karnow, C.E.A. (2013) The Application of Traditional Tort Theory to Embodied Machine Intelligence. In: Ryan Calo, Michael Froomkin, Ian Kerr (eds.). *Robot Law*. Cheltenham: Edward Elgar Publishing Ltd, pp. 51–77.

[5] Toon, J. (2017) *Swarms of Autonomous Aerial Vehicles Test New Dogfighting Skills*. [online] Atlanta: GeorgiaTech. Available from: http://www.rh.gatech.edu/news/590743/swarms-autonomous-aerial-vehicles-test-new-dogfighting-skills [Accessed 15 May 2019].

[6] Radutniy, O.E. (2017) Criminal Liability of the Artificial Intelligence. *Problems of Legality*, (138), p. 136.

[7] Hallevy, G. (2010) 'I, Robot – I, Criminal' – When Science Fiction Becomes Reality: Legal Liability of AI Robots Committing Criminal Offenses. *Syracuse Science and Technology Law Reporter*, 22 (Spring), p. 1.

[8] In his research, *Calo* defines robots as machines with three qualities: *"(1) a robot can sense its environment, (2) a robot has the capacity to process the information it senses, and (3) a robot is organized to act directly upon its environment"*. See: Calo, R. (2016) *Robots in American Law. University of Washington School of Law Research Paper No. 2016-042*. Available from: https://ssrn.com/abstract=2737598 [Accessed 22 June 2019].

their actions. While they deliver great social benefits, can society's interaction with robots also cause harm?

In an increasingly automated world, these threats are becoming real and many people have spoken out about their fears. At a tech conference that took place on 6 November, 2017 in Lisbon, Portugal, the physicist *Dr. Stephen Hawking* warned us about the dangers of AI, stating that AI can be the worst case of human intelligence.[9] The entrepreneur *Elon Musk* has also expressed his concerns. He calls for establishment of a regulatory authority that would monitor development of AI, citing it as the most likely cause of World War III.[10]

The fact that the *US Air Force (USAF)* already uses some semi- and fully autonomous technology and expects to increase these systems' autonomy in the future,[11] gives credence to these fears. According to a study conducted by researchers from *Oxford* and *Yale Universities*, AI systems will outperform humans in many activities in the next ten years.[12]

In our coexistence with intelligent agents, one can naturally ask: *Who should be sued in court if a robot (that is, only fully autonomous robots, that operate without human control) makes a mistake, thereby killing, or causing serious injuries?* These questions have been puzzling academics and researchers. Even though this problem has been addressed before,[13] only recently it has attracted enough attention for a prompt examination. Due to the absence of direct legal regulation of AI, the questions at hand still remain unclear. The uncertainty largely stems from the complex nature

[9] See, for example: Murphy, M. (2017) *Stephen Hawking: AI Could Be Best – or Worst – Thing in Human History*. [online] New York City: MarketWatch. Available from: https://www.marketwatch.com/story/stephen-hawking-ai-could-be-best-or-worst-thing-in-human-history-2017-11-06 [Accessed 29 October 2018].

[10] See, for example: Osborne, S. (2017) Elon Musk Calls for Urgent Laws on Robot as They Will Soon Be Risk to Public. *Express*, 28 November. [online] Available from: https://www.express.co.uk/news/science/885344/elon-musk-artificial-intelligence-robotics-regulation [Accessed 29 October 2018].

[11] Palmer, A. (2010) Autonomous UAS: a partial solution to America's future airpower needs. [pre-print] Submitted to: *Air University in partial fulfillment of the graduation requirements*. Available from: https://apps.dtic.mil/dtic/tr/fulltext/u2/1018416.pdf [Accessed 29 November 2018].

[12] Grace, K. et al. (2018) Viewpoint: When Will AI Exceed Human Performance? Evidence from AI Experts. *Journal of Artificial Intelligence Research*, 62, pp. 729–754.

[13] See, for example: Willick, M. (1983) Artificial Intelligence: Some Legal Approaches and Implications. *AI Magazine*, 4 (2), p. 5. Available from: https://aaai.org/ojs/index.php/aimagazine/article/view/392 [Accessed 29 November 2018]; Karnow, C.E.A. (1996) Liability for Distributed Artificial Intelligences. *Berkeley Technology Law Journal*, 11 (1), pp. 147–204. Available from: https://lawcat.berkeley.edu/record/1115611?ln=en [Accessed 29 November 2018].

of industrial robots and the multiple parties involved in the process of their manufacture.

The aim of this research is to outline a comprehensive analysis of significant liability models that address the responsibility for hazards caused by autonomous systems. This paper does not intend to offer a detailed answer for the models presented, considering that such an analysis goes beyond a research paper. Therefore, theories and explanations intend to serve the reader as guideposts to further exploration.

To limit the scope of the study, the paper primarily reflects a criminal approach to liability, and the focus is mostly in the assessment of fault rather than in the allocation of cost. Thus, a tort law approach to providing compensation for damage or physical injuries caused by AI systems is not an object of analysis in this article.

The paper consists of three main parts. The first part examines direct liability of AI systems. The matter is approached by considering that, in the near future, robots might become sophisticated machines having human-like abilities. The paper examines whether AI agents could be granted legal personhood and whether they can be held criminally liable for their actions. The second part examines whether responsibility can be allocated to different agents in the production chain, i.e. imposing strict liability on operators of the AI agents, such as programmers, designers, owners, and other parties involved in the process of manufacturing. Finally, corporate criminal liability is considered as a plausible method to address the wrongdoings of autonomous systems.

The article argues that current criminal law and the current legal system are not well positioned to balance a concern for physical safety with incentivizing innovation of AI and industrial robots. The doctrine of direct liability of AI systems is problematic from a normative perspective. In the absence of a regulatory framework governing the legal status of AI systems, the question of whether AI systems could become legal persons remains only theoretical. The concept of AI as a tool and strict liability of manufacturers is also problematic, as the plaintiff may find it very difficult to prove that the AI system was defective in the moment it left the manufacturer or its developer. On the other hand, there are no clear grounds on which to allocate liability of producers based on negligence. With regard to AI systems as self-learning entities, it is hard to predict their behaviours and define the cause-effect pattern; therefore, the operators of AI systems may not be in a favourable position to foresee risks and provide due diligence. Given the fact that AI represents a great power in the hands of giant tech companies, it may fairly be said that corporate liability should gain more attention from researchers, academics, and policymakers. However, there is a need for an international regulatory response that would set down basic rules that respond to the factual problem.

2. DIRECT CRIMINAL LIABILITY OF AI SYSTEMS

Are machines legal authors of their actions? The first question is whether or not we can recognize AI agents as legally responsible for their behaviours in terms of traditional criminal law theories.

In criminal law, to impose criminal liability for intentional offences, two main criteria must be met.[14] One is the factual element (*actus reus*), which contains the criminal conduct, and the other one is the mental element (*mens rea*), which consists of the general intent of the offender and embodies the idea of culpability.[15] *Mens rea,* in this respect, means a desire or a will to cause a certain consequence as a result of the conduct of a person.[16] It reflect the offender's state of mind. What about robot crime? Can we treat autonomous intelligent machines' crimes under the existing criminal law principles?

As *Calo* points out,

> *"humans are, or are not, like robots, is a critical distinction that informs the legal issue before the court".*[17]

In this respect, the relevant question is: *Are AI systems capable of meeting the requirements of both factual and mental elements?* Although both elements should be present to establish criminal liability,[18] the greatest challenge remains the establishment of the *mens rea* element. How do we demonstrate the intentions of a non-human? This is particularly difficult due to AI systems' lack of consciousness.

[14] Hallevy, G. (2013) *When Robots Kill: Artificial Intelligence under Criminal Law*. Boston: Northeastern University Press, p. 85.

[15] Ibid.

[16] Gaur, K.D. (2003) Principles of Criminal Liability. In: K.D. Gaur (ed.). *Criminal Law and Criminology*. New Delhi: Deep and Deep Publications, p. 24.

[17] Calo, R. (2016) Op. cit., p. 25.

[18] Hallevy, G. (2013) Op. cit., p. 85.

Generally, self-consciousness represents a person's ability to think and make moral judgments, for instance judge good and evil. Thus, from an ethical and legal perspective, holding AI systems criminally accountable for their actions proves to be inappropriate, because they are not aware of the consequences of their actions. Such offenders are considered absent of adequate culpability (*nullum crimen sine culpa*).[19] However, from a technical perspective, researchers believe that robots already have a rudimentary consciousness, referring to robots' abilities to accumulate knowledge and make judgments accordingly,[20] and may soon become human-like entities, or even exceed human intelligence.[21] In light of that, *Hallevy* suggests that a new subject be added to criminal law, in addition to humans and corporations, to which he refers as *machina sapiens criminalis*.[22]

2.1. LEGAL PERSONHOOD: CAN AI SYSTEMS BE SUBJECTS OF LAW?

Many researchers are looking for regulatory means to accommodate the status of intelligent agents in the legal system and in society. Perhaps encouraged by the case of two chimpanzees (*Hercules* and *Leo*) who were granted the status of "legal persons" by the *Manhattan Supreme Court* in 2015,[23] researchers have started to look at the possibility of granting "personhood" to AI systems. As one might expect, scholars share differing perspectives. It primarily depends on whether they accept the robot as a legal subject, i.e. *"metaphors or similes that support a particular verdict"*[24] or see it just as an object, i.e. *"artifacts in the world that have legal disputes."*[25]

[19] Hallevy, G. (2015) *Liability for Crimes Involving Artificial Intelligence Systems*. Springer International Publishing, p. 33.

[20] See, Retto, J. (2017) *Sophia, First Citizen Robot of the World*. [online] Available from: https://www.researchgate.net/publication/321319964_SOPHIA_FIRST_CITIZEN_ROBOT_OF_THE_WORLD [Accessed 29 November 2018] .

[21] Radutniy, O.E. (2017) Op. cit., p. 136.

[22] Hallevy, G. (2013) Op. cit., p. 21 (arguing that given the human-like actions of autonomous systems, the current criminal law is adequate to address AI technology issues. *Hallevy* continues his argument by stating that as long as technology is about to advance into creating what he calls "machina sapiens" – an AI system that imitates the human mind – current criminal law would be even more adequate to address criminal liability issues of AI entities, since the human mind is already the subject of the current criminal law).

[23] Bekoff, M. (2015) *Judge Recognizes Two Chimpanzees as Legal Persons: A First Two Chimpanzees, Hercules and Leo, Are Determined to Be Persons in NY Court*. [online] Available from: www.psychologytoday.com/us/blog/animal-emotions/201504/judge-recognizes-two-chimpanzees-legal-persons-first [Accessed 29 November 2018].

[24] Calo, R. (2016) Op. cit., p. 44.

[25] Ibid.

Some legal scholars argue that robots are objects created by people and, as such, they are perceived as items or property, which by default cannot possess any legal rights.[26] They are merely regarded as tools in the hands of their producers or owners. This perspective reflects the views of the American writer *Isaac Asimov*, who distinguishes robots as property in the disposal of their human creators.[27]

In contrast, others note that AI systems are significantly different from other objects due to their active intervention in human relations. *Cerka et al.*, for example, point out that AI systems interact with other subjects of law, thus it is imperative to recognize them as legal entities in order to be able to clearly define subjects' rights, interests, and their obligations.[28] Such rights may prove difficult to enforce and thus call for establishment of legal provisions that accommodate the relationship between individuals and AI systems. An interesting case, for instance, was represented by a mock trial at the *International Bar Association* conference in San Francisco on 16 September 2013, where attorney *Dr. Martine Rothblatt* addressed the legality of a corporation unplugging/shutting down an intelligent computer, arguing that the computer had the right to maintain an existence.[29] In the absence of legislation, the court could not rule whether the AI system had the right not to be destroyed.

At the international level, robotic rights have already gained importance. In the autumn of 2017, Saudi Arabia granted citizenship to a humanoid robot named *Sophia*.[30] *Sophia*, a robot that mimicked human expressions and

[26] See, for example: Radutniy, O.E. (2017) Op. cit., p. 136.

[27] *Asimov* explores the "three law of robotics", which are as follows: *"(1) a robot may not injure a human being or, through inaction, allow a human being to come to harm; (2) a robot must obey orders given it by human beings except where such orders would conflict with the First Law; and (3) a robot must protect its own existence as long as such protection does not conflict with the First or Second Law"*. See: Houvast, F. Timmerman, R. and Zwaan, Y. (2018) Exploring the Legal Rights & Obligations of Robots: A Legal Book Review of I, Robot by Isaac Asimov reviewed in *Law Literature Project, Utrecht University*, pp. 1–8.

[28] Having regard that AI systems cannot express their will as humans do, the authors suggest that by using legal analogy, AI entities should be viewed as artificial subjects of law, similar to the corporate personality. See: Čerka, P., Grigienė, J. and Sirbikytė, G. (2017) Is It Possible to Grant Legal Personality to Artificial Intelligence Software Systems?. *Computer Law and Security Review*, 33 (5), pp. 685–699.

[29] Rothblatt, M. and Angelica, A.D. (2003) *Bio-Cyber-Ethics: Should We Stop a Company from Unplugging an Intelligent Computer?*. [blog entry] 28 September. Available from: http://www.kurzweilai.net/biocyberethics-should-we-stop-a-company-from-unplugging-an-intelligent-computer [Accessed 24 October 2018].

[30] Wootson, C. (2017) *Saudi Arabia, Which Denies Women Equal Rights, Makes a Robot a Citizen*. [online] Available from: https://www.ndtv.com/world-news/saudi-arabia-which-denies-women-equal-rights-makes-a-robot-a-citizen-1768666 [Accessed 20 January 2019].

could learn human behaviours by interacting with people, became the first robot in the world to received citizenship.

The leading country in robotics, Japan, also seems to have settled the question of robot rights. On 7 November 2010, a therapeutic robot named *Paro*, received its own koseki, a special residency permit, which in Japanese society conflates legal rights such as family, nationality, and citizenship.[31]

In its turn, the *European Parliament* adopted a resolution entitled *Civil Law on Robotics*. This resolution envisages granting robots a specific legal status as electronic persons, responsible for any damage resulting from their autonomous decisions.[32] The assumption is that such a legal status would allocate liability for the damages caused by *"the most sophisticated autonomous robots"*, whose decisions are made independently, without human intervention.[33]

The *European Union's* oversight on granting autonomous systems legal personhood could be a starting point for allocating rights and responsibilities to AI systems; however, this insight is not accepted by all scholars. In March 2018, *Nathalie Nevejans*, a lecturer in law at the *University of Artois*, addressed this issue with an open letter to the *European Commission*, objecting to the legal status of robots.[34] She claims that a legal status for robots would collide with human rights, such as: the right to dignity, the right to its integrity, the right to remuneration, or the right to citizenship.[35]

It is fair to suggest that at some point in the evolution of AI, robots might become capable of generating their own goals and intentions, thus they may qualify as subjects of current criminal liability law. The next question is: How does the court punish an AI robot? Can they experience blame?

These issues remain without a clear answer. The traditional criminal justice system is designed by humans for humans, making punishment

[31] Robertson, J. (2014) Human Rights vs. Robot Rights: Forecasts from Japan. *Critical Asian Studies*, 46 (4), pp. 571–598.

[32] Civil Law Rules on Robotics, European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)), 16 February. Available from: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2017-0051&language=EN&ring=A8-2017-0005 [Accessed 03 January 2019].

[33] Paragraph 59(f) of the Resolution.

[34] Robotics Open Letter. (2017) *Open Letter to the European Commission Artificial Intelligence and Robotics*. [online] Available from: http://www.robotics-openletter.eu/ [Accessed 20 January 2019].

[35] Ibid.

seem out of place in the discussion of robot field. Criminal law seeks justice by punishing offenders. Its key purpose is to establish security and order in society. In this respect, the role of criminal law is to correct wrongdoers, and to reintegrate them into society. Clearly, this may not be the case with robots, as they are different from humans in many aspects. Many human attributes could not apply to robots, such as: fear, pain, freedom of movement, etc. In this respect, robot imprisonment would be pointless. Therefore, the question of robot "personhood" remains an open debate with inconclusive results.

3. STRICT LIABILITY: AI AS A TOOL

In legal research, many scholars share the opinion that the legal responsibility for the actions of AI systems falls on the individual who has produced or owns the robot. For instance, *Asaro* explains that robots qualify as built systems where the schemes are chosen by designers, so the designers and programmers of the learning methods would be responsible for the machine's actions.[36] *Hallevy* expands on this idea. He introduces the *Perpetration-by-Another Liability Model*.[37] According to this model, AI entities are considered innocent agents – machines with no human attributes – and therefore an AI system could not be regarded as a perpetrator of an offence. Pursuant to this model, the real perpetrator is the programmer of the robot, who designs a software with certain instructions leading the robot to commit certain offences. In this scenario, although the conduct (*actus reus*) falls upon the AI, the intent (*mens rea*) is determined by the programmer's mental state.[38] The user of AI can also be considered as the perpetrator-by-another. *Hallevy* explains that AI is completely dependent on its user (end-user) who uses it with the intent to commit offences.[39]

It is important to note that this model suggests that AI is merely a tool (equivalent to a hammer) in the hands of the programmer or the user. It

[36] Asaro, P.M. (2006) What Should We Want From a Robot Ethic? *International Review of Information Ethics*, 6 (12), pp. 2–15. Available from: http://cybersophe.com/writing/Asaro IRIE.pdf [Accessed 20 January 2019].

[37] Hallevy, G. (2010) Op. cit., pp. 9–12.

[38] Ibid.

[39] Ibid.

lacks the *mens rea* element, hence the fault cannot be attributed to the AI itself.[40]

This perspective imposes non-fault liability and is similar to product liability regulated by the *Directive 85/374/EEC*.[41] According to this Directive, strict liability is imposed as a result of a manufacturing defect.[42] If the defective product causes an injury, producers are held strictly liable for that injury.[43]

Relying on the abovementioned analysis, AI systems are regarded as tools in the hands of the sellers, distributors, and users, and liability is imposed, not because of their wrong acts, but due to their specific relationship with the AI systems. The behaviour of an AI system is directly linked with the natural person on whose behalf it acts, therefore that person is held accountable for any injury caused by the AI system, regardless of whether such conduct was intentional or planned. This view reflects the concept of vicarious liability, according to which someone is held liable for the wrongs of others, such as, for example, employers who are vicariously liable for the wrongdoings of their employees.[44] Summarizing the idea of robot-as-tools based on the concept of vicarious liability, AI systems are regarded as agents acting on behalf of several individuals that could be considered as perpetrators, such as: the producer, the programmer, the designer, the seller, the distributor, the user of the robot, etc.

Yet, by comparing the parent-child relationship, *Sparrow* implies that product liability could not apply to programmers and robots, as it would be analogous to

[40] Freitas, P.M., Andrade, F. and Novais, P. (2014) Criminal Liability of Autonomous Agents: From the Unthinkable to the Plausible. In: Pompeu Casanovas, Ugo Pagallo, Monica Palmirani and Giovanni Sartor (eds.). *AI Approaches to the Complexity of Legal Systems*. Berlin: Springer, p. 150.

[41] Council Directive 85/374/EEC of 25 July 1985 on the Approximation of the Laws, Regulations and Administrative Provisions of the Member States Concerning Liability for Defective Products. *Official Journal of the European Union* (L 210), 25 July. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31985L0374 [Accessed 23 January 2019].

[42] Article 1 states: *"The producer shall be liable for damage caused by a defect in his product"*. Ibid.

[43] Ibid.

[44] For an overview of vicarious liability, see: Lederman, E. (2000) Models for Imposing Corporate Criminal Liability: From Adaptation and Imitation Toward Aggregation and the Search For Self-Identity. *Buffalo Criminal Law Review*, 4 (1), pp. 641–708.

> *"holding parents responsible for the actions of their children once they have left their care"*.[45]

Perhaps this reasoning should be given importance in the liability chain, due to AI systems' ability to make independent decisions and change behaviour through machine learning, making it very difficult to determine the cause-effect link between AI and the responsible participant. In this respect, strict liability might be a too heavy a burden on the producers or owners of the robot. Besides that, substantially different ways to resolve liability issues lead to potential legal errors.[46] Courts are likely to adopt different solutions, leading to widespread disagreement in the general public and among manufacturers trying to assess their potential liability in the national market.[47] Furthermore, an excessive blameworthiness could obstruct the progress of technology development and all its benefits would be lost.[48]

The practical solution lies in devising mechanisms of accountability that promote innovation and development of advanced autonomous artificial agents that benefit society, while effectively managing the risks and their harmful actions. In addressing the need to incentivise safety without ruining robot supply in the market, *Calo* argues in favour of providing protection to manufacturers and distributers of open robotics, similar to the immunity of gun manufacturers.[49]

3.1. NEGLIGENCE-BASED LIABILITY

Negligence imposes liability only if the defendant is at fault.[50] To simplify, liability in negligence in a criminal context arises if there is a reasonable

[45] Sparrow, R. (2007) Killer Robots. *Journal of Applied Philosophy*, 24 (1), p. 62.

[46] Geistfeld, M.A. (2017) A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation. *California Law Review*, 105, p. 1611.

[47] Ibid.

[48] Čerka et al. (2017) Op. cit., p. 689; See also: Gless, S. Silverman, E. and Weigend, T. (2016) If Robots Cause Harm, Who Is to Blame? Self-Driving Cars and Criminal Liability. *New Criminal Law Review*, 19 (3), p. 430.; see also Hubbard, P. (2014) 'Sophisticated Robots': Balancing Liability, Regulation, and Innovation. *Florida Law Review*, 66 (5), pp. 1803–1872 (explaining that *"All technology presents the challenge of balancing its costs against its benefits. First, the expanded potential liability of innovators could negatively affect their decision to develop, for example, an Unmanned Aircraft System (UAS). Second, the increased liability could also reduce the demand for a robotic vehicle like a UAS because purchasers and users would need to worry about potential greater liability for personal injury"*).

[49] Calo, R. (2011) Open Robotics. *Maryland Law Review*, 70 (3), pp. 101–142. Available from: http://ssrn.com/abstract=1706293 [Accessed 25 January 2019].

[50] Kelley, R. et al. (2010) Liability in Robotics: An International Perspective on Robots as Animals. *Advanced Robotics*, 24 (13), pp. 1861–1871.

duty of care. A negligent action is something a rational individual would not do. For example, texting on the phone while driving qualifies as negligence.

Negligence is the failure to use reasonable care to prevent harm to oneself or to others. A person can be negligent by acting or by failing to act. A person is negligent if he or she does something that a reasonably careful person would not do in the same situation or fails to do something that a reasonably careful person would do in the same situation.[51]

It seems logical that a person who has suffered a harm by an AI system files a suit against the agent that failed to provide due care, i.e. to do something that is morally and legally required. Other researchers share the same opinion. *Roff*, for instance, points out that the responsibility and liability lie with the software programmers. She discusses that the burden of legal responsibility falls upon programmers or the manufacturers, who, having the status of the creators of the machine, are legally responsible for providing warnings and taking necessary measures to avoid any risk.[52] In accordance with this view, *Hallevy* argues that the programmer or the user of the robot is liable when he or she has failed to foresee the offence committed by the robot and failed to prevent it.[53] In *Hallevy's* research, this is called the *Natural-Probable-Consequence liability model*.[54] According to this model, there is a link between the AI system's offence and manufacturer's or user's action. Even though the manufacturer or the user had no intent to commit an offence, if there is evidence that they should have taken corrective measures to prevent the happening, they are held accountable.[55] This model is based on the duty of reasonable programmers and manufacturers to foresee potential wrongdoings of the robots, i.e. to ensure that their products have no design flaws and to avoid obstacles by warning consumers of hidden dangers.

Criminal liability based on negligence relies on the assumption that none of the aforementioned individuals intended to cause harm to another

[51] Judicial Council of California. (2017) *California Civil Jury Instruction 2017 Edition ("CACI") No.401*. [online] Available from: https://www.justia.com/trials-litigation/docs/caci/400/401/ [Accessed 20 December 2018].

[52] Roff, H.M. (2013) Killing in War: Responsibility, Liability and Lethal Autonomous Robots. In: Fritz Allhoff, Nicholas Evans and Adam Henschke (eds.). *Routledge Handbook of Ethics and War: Just War Theory in the 21st Century*. Routledge Press, p. 356.

[53] Hallevy, G. (2010) Op. cit., pp. 15, 16.

[54] Ibid, p. 9.

[55] Ibid, pp. 14, 15.

human being, thus the liability arises due to lack of reasonable care, i.e. a rational person should have acted to avoid damage. This resembles the relationship between owners and domesticated animals.[56] *Kelley at al.* note that

> *"robot owners should be held liable for negligence with respect to their robots, much like dog owners are held liable for negligence with respect to their dogs".*[57]

In this sense, manufacturers, sellers, or distributors are criminally liable when they have failed to warn about a foreseeable risk or they have failed to give adequate instructions to avoid harm.

However, it is very difficult to impose liability based on negligence. Most importantly, it is not clear how to determine the standards of care. Let us imagine that instructions to avoid a risk in a given situation are provided in due time. The next question is: Was that warning or instruction reasonable? Currently there are no international legal norms determining safety requirements of AI systems upon which plaintiffs can rely in a certain situation. The acquisition of autonomy and the self-learning capacity of AI systems makes it difficult to predict their behaviours and to determine possible risks and threats, therefore it is not an easy task for victims who have the burden of proof to allocate the "fault". For example, if someone is injured by an autonomous robot that is designed to learn and to interact with the environment, it may be hard to identify what went wrong and what caused the accident. Additionally, due to the large number of individuals involved in the process of manufacturing, it is unclear which agent among multiple component suppliers of hardware and software has the duty to avoid risks.

3.1.1. FORESEEABILITY

To impose criminal liability based on negligence, it is important to determine whether the manufacturer could anticipate the potential malfunctions of the AI system. Prediction theory is central to negligence.[58] Negligence arises when a reasonably prudent person "ought to have

[56] Kelley, R. et al. (2010) Op. cit., p. 1864 (explaining: *"We justify this negligence analysis by analogizing robots to domesticated animals, whose owners are as a general rule subject to negligence liability because such animals are generally predictable"*).

[57] Ibid.

[58] Karnow, C.E.A. (2013) Op. cit., p. 9.

known" that his actions would cause harm.[59] In traditional product liability, the manufacturer is responsible for the product if he could foresee potential problems or harms it may cause. The verb "to foresee" means "to have prescience of; to know in advance".[60]

Foreseeability

> *"is not to be measured by what is more probable than not, but includes whatever is likely enough in the setting of modern life that a reasonably thoughtful [person] would take account of it in guiding practical conduct."*[61]

Early robotic machines, such as automated elevators, have been subject to liability claims based on the duty of the manufacturer to provide reasonable care, i.e. to undertake safety measures to prevent risk or harm. Plaintiffs have sued for injuries caused by lack of due care in the maintenance of these machines.[62] However, there are no easy guidelines to determine whether the risk or physical harm is "foreseeable" for sophisticated and autonomous robots.

To effectively address responsibility and blame, as noted by *Owen*, we must first determine the individual's ability to understand that the action might cause harm and that opting for another action would be a safer alternative, in accordance to individual's obligations to the community.[63] The responsibility of manufacturers, distributors, and users of AI systems thus depend upon their capacity to understand the behaviour patterns of AI systems, the causal possibilities of AI systems' actions, and expected results. When it comes to intelligent robots and their ability to learn from environmental data, designers and users may not have a feasible way to predict their behaviour, simply because machine learning techniques

[59] Ibid, p. 10.

[60] Webster's Unabridged Dictionary. (2001) 2nd ed.

[61] *Constance B. v. State of California.* (1986) 178 Cal. App. 3d 200,206. Available from: https://law.justia.com/cases/california/court-of-appeal/3d/178/200.html [Accessed 20 December 2018].

[62] See, e.g. *Estabrook v. J.C. Penney Co.* (1970) 464 P.2d 325 (In Banc.). Available from: https://www.courtlistener.com/opinion/1247130/estabrook-v-jc-penney-company/ [Accessed 20 December 2018] (The plaintiff sued for injuries incurred while he was playing on an escalator); *Brown v. Sears, Roebuck & Co.* (1987) 514 So. 2d 439. Available from: https://law.justia.com/cases/louisiana/supreme-court/1987/87-c-0726-0-1.html [Accessed 20 December 2018] (A twenty-two month old child caught his finger in the space between the moving treads and the left side panel of the elevator. The court ruled in favor of the plaintiff).

[63] Owen, D. (2009) Figuring Foreseeability. *Wake Forest Law Review*, 44, pp. 1277–1307.

allow AI systems to modify their functions and learn after they are deployed.[64]

The second factor in determining responsibility is evaluation of the actor's decision;[65] whether it was the right decision that would have prevented the risk. This is often left to the judges to decide. As stated earlier, foreseeability is an abstract and vague concept, and in many cases cannot be proven in court. Some argue that judges use the doctrine of foreseeability as a means to weed out cases they deem unworthy;[66] that is, the judges use "foreseeability" as a means of deciding whether the action was right or wrong, upon which they impose or deny negligence liability. This can lead to different judgments for similar cases.[67]

Having said that, concepts like "foreseeability" and "reasonable care" cannot be used as key elements to impose criminal liability on manufacturers and sellers, as they may simply not have the level of skill required to foresee the manner in which the harm will occur. Consequently, standards of reasonable care may be vague. In addition, any attempt to impose responsibility on such a basis could lead to infinite liability for creators of AI systems that could obstruct the economy and innovation of AI.

4. AI LIABILITY GAP: A LOOK INTO CORPORATE CRIMINAL LIABILITY

So far, we have seen that imposing criminal liability for the harmful and erratic behaviours of robots often leads us to a vicious circle due to the fact that it is often very difficult to attribute responsibility to specific individuals. When addressing the AI accountability gap, there are always two parties in the centre of the debate: those who develop AI, i.e. big

[64] Asaro, P.M. (2016) The Liability Problem for Autonomous Artificial Agents. In: Bipin Indurkhya and Georgi Stojanov (eds.). *AAAI Symposium on Ethical and Moral Considerations in Non-Human Agents*, Stanford, 21–23 March. USA: Association for the Advancement of Artificial Intelligence, pp. 190–194. Available from: https://www.aaai.org/ocs/index.php/SSS/SSS16/paper/view/12699 [Accessed 29 December 2018].

[65] Ibid.

[66] See, e.g. Cardi, W.J. (2005) Purging Foreseeability: The New Vision of Duty and Judicial Power in the Proposed Restatement (Third) of Torts. *Vanderbilt Law Review*, 58 (3), p. 739. Available from: https://wakespace.lib.wfu.edu/handle/10339/58895 [Accessed 15 October 2018] (explaining *"In many courts the foreseeability lens seems to expand, contract or change focus at the will of the judge"*); See also: Owen, D. (2009) Op. cit., p. 1278 (arguing *"while foreseeability may be the fundamental moral glue of tort, it provides so little decisional guidance that scholars often revile it for being vague, vacuous, and indeterminate"*).

[67] Cardi, WJ. (2005) Op. cit., p. 740.

companies; and those who are directly impacted from such development, i.e. society.[68] Anticipating an exponential growth of technology, it seems that this gap is going to accelerate in the future. Importantly, this paper examines whether accountability should be imposed over institutions, i.e. corporations, rather than individuals.

The need for corporate liability cannot be understood without an understanding of the great dominance and influence of the private sector. There are two key factors that ensure corporations' great digital power and dominance: data collection and money.

With the advent of globalisation, multinational corporations[69] wield tremendous financial power. As noted by *Pasquale*, these dominant players control money and information.[70] Today a great amount of digital power is concentrated in the hands of just a few people. This is a threat both to democracy and to functioning markets.[71] At the core of their reputation,[72] search,[73] and finance[74] lies our data, which too often is stored and processed under secrecy.[75] The big tech companies, in particular the "Frightful 5"[76] (*Google*, *Facebook*, *Amazon*, *Apple*, and *Microsoft*) control and collect the data and information of billions of people,[77] which is often used to shape consumers' behaviour and maximize profit.[78] Indeed, as *Bryson and Theodorou* point out,

[68] See: Whittaker, M. et al. (2018) *AI Now Report*. [online] New York City: AI Now Institute. Available from: https://ainowinstitute.org/AI_Now_2018_Report.pdf [Accessed 19 December 2018].

[69] The term "multinational corporation" is defined as *"an economic entity, which owns (in whole or in part), controls and manages income generating assets in more than one country"*. For the detailed review, see: Muchlinski, P.T. (2007) *Multinational Enterprises and the Law*. Oxford: Oxford University Press, p. 12.

[70] Pasquale, F. (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, Massachusetts: Harvard University Press, pp. 4–6.

[71] Nemitz, P. (2018) Constitutional Democracy and Technology in the Age of Artificial Intelligence. [in press] Submitted to: *Philosophical Transactions of the Royal Society A*. Available from: https://ssrn.com/abstract=3234336 [Accessed 07 January 2019].

[72] Pasquale, F. (2015) Op. cit., p. 4.

[73] Ibid.

[74] Ibid.

[75] Ibid.

[76] See: Manjoo, F. (2016) Tech's 'Frightful 5' Will Dominate Digital Life for Foreseeable Future. *N.Y. Times*, 20 January. [online] Available from: https://www.nytimes.com/2016/01/21/technology/techs-frightful-5-will-dominate-digital-life-for-foreseeable-future.html [Accessed 10 January 2019].

[77] Chadwick, P. (2018) To Regulate AI We Need New Laws, Not Just a Code of Ethics. *The Guardian*, 28 October. [online] Available from: https://www.theguardian.com/commentisfree/2018/oct/28/regulate-ai-new-laws-code-of-ethics-technology-power [Accessed 20 January 2019].

[78] Nemitz, P. (2018) Op. cit.

> *"with great power (or even just money) does come great responsibility".*[79]

Consequently, the big question is: Should corporations be held accountable for criminal actions arising from the tools they deploy in the market?

The "deep pockets" of the corporations might give us the answer to this question. Organisational blameworthiness, in this regard, derives from the profit-driven expansion of mega corporations' commercial activities. It seems legitimate and necessary to allocate the threats by recurring accountability to those who collect the fruits of AI deployment. Otherwise, the struggle to impose liability for the harmful actions of AI systems would provide room for big corporations to expand their businesses, while potential harmful acts of intelligent machines would remain a constant threat to society.

As noted by a report published in 2018, the accountability gap in AI is favourable for the companies that create and deploy these technologies, at the expense of society's interest.[80] Hence, a limited and unregulated corporation liability may encourage corporations to take greater risks – socially harmful risks – in order to maximize their profit. *Anderson and Luchsinger* share the same concerns:

> *"Most AI tools are and will be in the hands of companies striving for power. Values and ethics are often not baked into digital systems making people's decision for them. These systems are globally networked and not easy to regulate or rein in".*[81]

The big tech lobby campaigns against the law[82] give credence to these concerns. It demonstrates their efforts to avoid responsibility at all cost. The internet giants are the only corporations in history that have managed

[79] Bryson, J. and Theodorou, A. (2019) How Society Can Maintain Human-Centric Artificial Intelligence. In: Marja Toivonen and Eveliina Saari (eds.). *Human Centered Digitalization and Services*. Singapore: Springer, pp. 305–323. Available from: http://www.cs.bath.ac.uk/~jjb/ftp/BrysonTheodorou19.pdf [Accessed 20 January 2019].

[80] Whittaker et al. (2018) Op. cit.

[81] Anderson, J. Rainie, L. and Luchsinger, A. (2018) *Artificial Intelligence and the Future of Humans*. [online] Washington, DC: Pew Research Center. Available from: http://www.pewinternet.org/2018/12/10/artificial-intelligence-and-the-future-of-humans/ [Accessed 23 January 2019].

[82] For the latest big tech lobby campaigns against new law, see: Meyer, D. (2017) *Inside the EPrivacy Regulation's Furious Lobbying War*. [online] Kansas City: IAAP. Available from: https://iapp.org/news/a/inside-the-eprivacy-regulations-furious-lobbying-war/ [Accessed 23 January 2019]; Fang, L. (2018) *Google and Facebook Are Quietly Fighting California's Privacy Rights Initiative, Emails Reveal*. [online] First Look Media. Available from: https://theintercept.com/2018/06/26/google-and-facebook-are-quietly-fighting-californias-privacy-rights-initiative-emails-reveal/ [Accessed 23 January 2019].

to maximize their profit at the top of the stock exchange, and at the same time maintain their output largely unregulated.[83] Therefore, to shape their practice in the common good, there is an urgent need for sector-specific regulation. Without a regulation that goes beyond ethical standards, principles like justice and accountability will remain conflict concepts between mega-companies and the common good of the general public. Ethical codes, without enforceable mechanisms, have little or no effect regarding AI's social implications and liability problems. It seems that some of these companies have realized the complexity of the problem and have come to the same conclusion. A representative of *Microsoft*, for instance, calls for establishment of a new field of law governing *"a growing pool of businesses involved"*.[84]

Following the great impact corporations have in the development of AI, coupled with the difficulty to assign individual criminal liability and moral responsibility for crimes committed by intelligent robots, the discussion about holding corporations, rather than individuals, responsible is both timely and topical. The nature of the debate should now move on from "whether" legal entities should have criminal liability, to "how" to properly address and regulate their responsibility in the field of AI.

4.1. CONSIDERING CORPORATE CRIMINAL LIABILITY

As an initial matter, corporate liability is not a new concept. The advances in communication technologies and the rise of consumer activism in the mid-twentieth century brought a public debate regarding the impact of large multinational enterprises towards society.[85] The rise of social responsibility movement caused a shift from the state-centred concerns of corporate regulations (focusing on problems such as taxation and corruption) towards people-centred approaches, mainly focusing on health and safety issues.[86]

Given the great impact corporations have had on the economy, particularly railroads, the need to impose criminal liability to large

[83] Nemitz, P. (2018) Op. cit.

[84] Bass, D. (2018) *Microsoft Says AI Advances Will Require New Laws, Regulations*. [online] New York City: Bloomberg L.P. Available from: https://www.bloomberg.com/news/articles/2018-01-18/microsoft-says-ai-advances-will-require-new-laws-regulations [Accessed 21 January 2019].

[85] Zerk, J.A. (2006) *Multinationals and Corporate Social Responsibility: Limitations and Opportunities in International Law*. New York: Cambridge University Press, p. 21.

[86] Ibid, p. 23.

corporations was acknowledged by courts in the late nineteenth century. The courts began to apply criminal sanctions to corporations for actions committed by individuals.[87] In the years to come, the traditional principle of *societas delinquere non potest*[88] gradually faded away. As a result, most national jurisdictions recognise corporations as legal persons, and have put in place domestic legislation that regulate the imposition of criminal liability of corporations.[89] From a legal standpoint, then, corporate liability could fill the gap of accountability issues regarding autonomous systems.

There are several theories widely adopted to impose criminal liability of corporations.[90] Generally, corporate liability is imposed indirectly, through the acts of their agents, such as, for instance, vicarious liability and *respondeat superior*.[91] This represents a nominalist approach under which corporation's liability is induced from the individual liability of its representatives.[92] In these cases, a plaintiff would need to prove that there is an agent or group of agents upon whose erratic conducts the company's liability can be established. The liability of a company, therefore, does not represent an independent wrongdoing, but arises due to its legal relationship with these individuals.[93] The search for the rogue actor and individual blameworthiness brings to light complications inherent in assessing fault. As previously stated,[94] in response to the argument that an intelligent machine's acts are unpredictable, it remains a challenge as far as establishing individual intent. Consequently, it would be a difficult task for the courts to establish blame and seek justice. That would lead to absolute impunity.

[87] Dragatsi, H. (2011) *Criminal Liability of Canadian Corporations for International Crimes*. Canada: Thomson Reuters, p. 147.

[88] Literally means "corporations cannot commit crimes" and postulates that legal entities do not bear moral and criminal responsibility. See: Stoitchkova, D. (2010) *Towards Corporate Liability in International Criminal Law*. Utrecht: Utrecht University, p. 7.

[89] Ibid.

[90] For an overview of corporate criminal liability doctrines, see: Suhariyanto, B. (2018) Corporate Criminal Liability Under the Reactive Corporate Fault to Achieve Good Corporate Governance in Indonesia. In: A. Raharjo and T. Sudrajat (eds.). *The 1st International Conference on Law, Governance and Social Justice*, Purwokerto, 25–26 September. Les Ulis: EDP Sciences. Available from: https://www.shs-conferences.org/articles/shsconf/pdf/2018/15/shsconf_icolgas2018_07009.pdf [Accessed 20 January 2019].

[91] See: Lederman, E. (2000) Op. cit., p. 651.

[92] Colvin, E. (1995) Corporate Personality and Criminal Liability. *Criminal Law Forum*, 6 (1), p. 2.

[93] Ibid.

[94] See section 2 of this paper.

A new concept of corporate liability, undergirded by a realistic view of corporations, suggests that corporations have individual personalities and intentions, which does not derive from the actions of its agents.[95] The realistic view on corporate criminal liability could provide normative support for law reformers. American literature in the past decade proposed a new model of criminal liability of legal bodies, which is also based on self--identity doctrine and reflects the idea of modern corporations.[96] According to this approach, liability of corporations is primary. The corporate fault is structured by considering a multitude of factors, directly questioning corporation's conduct, i.e. what it ought to have known and what it ought do have done in order to prevent harm.[97]

In support of the individual identity of corporations approach, it can be argued that a theoretical shift from derivative models, and a new concept of strict corporate liability based on the independent identity of the legal body could alleviate issues at hand. Considering the emerging concept of corporations,[98] and the unprecedented power in their hands, a focus towards organisational blameworthiness could be a powerful tool in allocating responsibility for the risks associated with intelligent machines. The exponential development of technology and AI calls for regulatory framework to address situations not anticipated before. Policymakers acknowledge that legal entities, who have managed to attain, to a large extent, trouble free, should be subject to criminal proceedings.[99]

In the absence of a particular legislation, it is imperative to look for legal alternatives. For instance, corporate criminal liability could be developed

[95] See, e.g. Colvin, E. (1995) Op. cit. (*"Corporations can act and be at fault in ways that are different from the ways in which their members can act and be at fault"*.); Lawrence, F. (2000) In Defense of Corporate Criminal Liability. *Harvard Journal of Law & Public Policy*, 23 (3), p. 833 (discussing that corporations *"have independent identities in the community, based upon attributes-identifiable personae and a capacity to express moral judgments-that substantively distinguish them from their owners, managers and employees"*.); Bucy, P.H. (1991) Corporate Ethos: A Standard for Imposing Corporate Criminal Liability. *Minnesota Law Review*, 75, p. 1182 (proposing a corporate ethos doctrine based on the idea of separate corporate intent).

[96] Lederman, E. (2000) Op. cit., p. 678.

[97] Ibid.

[98] The complex form of modern organisations, their decentralised units, etc. often prevent identifying personal liability of individual agents; therefore, the idea that the corporations have an individual personality that does not derive from its representatives has gained momentum in recent decades. See: Sperino, S. (2010) A Modern Theory of Direct Corporate Liability for Title VII. *Faculty Articles and Other Publications Paper 230*. Available from: https://scholarship.law.uc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&https redir=1&article=1233&context=fac_pubs [Accessed 21 January 2019].

[99] Lederman, E. (2000) Op. cit., p. 644.

through a correlate stream of public welfare doctrine for strict-liability offences.[100] This theory serves two purposes: First, it represents a doctrine that was designed as a necessity to promote social order at a time when the industrial revolution brought many new threats to society.[101] The public welfare rules were intended to control particular industries and activities that affected public health, safety or welfare.[102] Similarly, the digital revolution has brought so many threats unknown to humans before. Taking into consideration the great socio-economic impact of mega-corporations, the welfare offence doctrine could pave the way for charging corporations with criminal offences for the harmful acts of AI. Second, this doctrine omits the criteria of blameworthiness; a penalty can be imposed regardless of the actor's intent, so the plaintiff does not have to prove that the defendant acted purposely.[103] Intent or blameworthiness is replaced by the assumption of the risk that the actor bears when engaging in a certain activity.[104]

Assumption is particularly important, as it may resolve many core problems facing the liability regime of autonomous systems. A particular death caused by an intelligent robot, for instance, should alarm AI developers with respect to the risks associated with the tools they deploy in the market. Their failure to adopt necessary precautionary and corrective measures should be subject to criminal liability, provided that they should have known or at least should have assumed that their conduct may seriously threaten the community's safety. Responsibility, hence, arises as a burden to an entity,

> *"otherwise innocent, but standing in responsible relation to a public danger".*[105]

Examples given by *Meyer* illustrate my suggestion:

A defendant charged with criminal possession of an unregistered firearm may be convicted even if he mistakenly thought the firearm was

[100] Strict liability offences are those where liability can be imposed without a *mens rea* of an actor. See section 2 of this paper.

[101] Carpenter, C.L. (2003) On Statutory Rape, Strict Liability, and the Public Welfare Offense Model. *American University Law review*, 53 (2), pp. 313–391.

[102] See: *Morissette v. United States.* (1952) 342 U.S. 246. Available from: https://supreme.justia.com/cases/federal/us/342/246/ [Accessed 28 January 2019].

[103] Reitz, M.J. (2013) *Strict Liability and Public Welfare Offenses*. [online] Midland: Mackinac Center. Available from: https://www.mackinac.org/19579 [Accessed 21 January 2019].

[104] Carpenter, C.L. (2003) Op. cit., p. 320.

[105] *Morissette v. United States.* (1952) Op. cit.

registered as required; An immigrant alien may be criminally convicted for unlawfully re-entering the United States even if she believed that she had proper government approval to return.[106]

In 1994, for instance, the *Supreme Court* in *Staples v. United States*[107] imposed strict liability to a defendant possessing an unregistered "firearm" that had been modified into an automatic weapon.[108] Although the defendant claimed he was unaware of the factual situation and was ignorant of any automatic capability of the firearm, the Court ruled that

> *"as long as a defendant knows that he is dealing with a dangerous device of a character that places him in responsible relation to a public danger, he should be alerted to the probability of strict regulation".*[109]

Is a public welfare offence doctrine the solution then? One could argue that it depends on whether you consider that a serious injury or a death caused by an intelligent robot is not only a harmful event for society, but also a probable consequence of a blameworthy negligence, which ought to be identified and repressed.

4.2. QUESTIONS AND DOUBTS

Commenting on corporate criminal responsibility, *Chengeta* has observed that corporate responsibility may bring jurisdictional and cost challenges to victims.[110] Victims would be faced with the burden of bringing cases against corporations registered in foreign countries, thereby encountering enormous financial costs.[111]

Additionally, it is beyond dispute that an excessive burden of criminal liability on corporations would impede innovation. Making corporations fully liable means that they should not invest in advancing AI. Does society really want this? Perhaps to some extent the general public needs to adapt to technological advancement. That is to say, probably there should be some

[106] Meyer, J.A. (2007) Authentically Innocent: Juries and Federal Regulatory Crimes. *Hastings Law Journal*, 59 (1), p. 138.

[107] *Staples v. United States.* (1994) 511 U.S. 600. Available from: https://supreme.justia.com/cases/federal/us/511/600/ [Accessed 28 January 2019].

[108] Ibid. at 602–04 ("Automatic" refers to a weapon that fires repeatedly with a single pull of the trigger).

[109] Ibid.

[110] Chengeta, T. (2016) Accountability Gap: Autonomous Weapon Systems and Modes of Responsibility in International Law. *Denver Journal of International Law and Policy*, 45 (1), p. 4.

[111] Ibid.

safety issues that should be socially tolerated, especially when it comes to robots dedicated to social benefits. Some authors[112] postulate that we should look for an intermediate solution, by adjusting legal rules and by accepting a margin of tolerance of certain errors in the designing and programming of robots.[113]

Tolerance for robot malfunctions, though, should not play a central role in debates concerning the existence of corporate criminal liability. A variety of potential, harmful consequences will also occur if there is no one to be blamed for the dangers associated with the use of autonomous systems. Therefore, the challenge of balancing technological development and its benefits in relation to its potential threats remains a future challenge.

5. CONCLUSION

The successful development of the robot market has posed challenging liability issues that need to be addressed by regulators and policymakers. There is no one-size-fits-all solution. In the absence of an international regulatory framework, finding the person that should be held criminally liable for the mishaps of fully autonomous systems is not an easy task, especially due to the complex and sophisticated nature of the machines. The more autonomous the system, the greater the challenge to establish effective rules governing liability for harmful actions.

While some authors suggest that current criminal law is a plausible possibility to cope with AI,[114] this paper shows that liability questions[115] of AI systems push traditional criminal law to its limit. Old definitions are not suitable to the modern era.

In terms of thinking of robots as subject to the law, one could argue that it is not a straightforward solution, due to the uncertainty of many questions facing robot ethics. While giving civic status to AI systems would regulate the industry to some extent, many other problems, such as intention and culpability of AI systems, remain to be addressed.

Similarly, product liability is facing challenging questions that stem from the increasingly sophisticated nature of robots and the many individuals involved in the production and maintenance of AI systems. It cannot be

[112] Gless, S., Silverman, E. and Weigend, T. (2016) Op. cit., p. 17.

[113] Ibid.

[114] Hallevy, G. (2013) Op. cit., p. 29.

[115] Questions of risk, fault and punishment remain to be addressed.

conclusively established because methods to impose product liability are not clear.

We argue that there is a need for a shift from an individual-centred liability model to an organisation-centred liability model. We suggest that corporate criminal liability is the best solution whenever the responsibility of individual agents cannot be conclusively established. However, in the absence of a particular law in the AI field, this proposition is also fit for discussion.

The existing conflict clearly shows that AI systems and issues related to their criminal liability will remain a topic of discussion among academic for many years to come.

LIST OF REFERENCES

[1] Anderson, J. Rainie, L. and Luchsinger, A. (2018) *Artificial Intelligence and the Future of Humans*. [online] Washington DC: Pew Research Center. Available from: http://www.pewinternet.org/2018/12/10/artificial-intelligence-and-the-future-of-humans/ [Accessed 23 January 2019].

[2] Asaro, P.M. (2006) What Should We Want From a Robot Ethic?. *International Review of Information Ethics*, 6 (12), pp. 2–15. Available from: http://cybersophe.com/writing/Asaro IRIE.pdf [Accessed 20 January 2019].

[3] Asaro, P.M. (2016) The Liability Problem for Autonomous Artificial Agents. In: Bipin Indurkhya and Georgi Stojanov (eds.). *AAAI Symposium on Ethical and Moral Considerations in Non-Human Agents*, Stanford, 21–23 March. USA: Association for the Advancement of Artificial Intelligence, pp. 190–194. Available from: https://www.aaai.org/ocs/index.php/SSS/SSS16/paper/view/12699 [Accessed 29 December 2018].

[4] Bass, D. (2018) *Microsoft Says AI Advances Will Require New Laws, Regulations*. [online] New York City: Bloomberg L.P. Available from: https://www.bloomberg.com/news/articles/2018-01-18/microsoft-says-ai-advances-will-require-new-laws-regulations [Accessed 21 January 2019].

[5] Bekoff, M. (2015) *Judge Recognizes Two Chimpanzees as Legal Persons: A First Two Chimpanzees, Hercules and Leo, Are Determined to Be Persons in NY Court.* [online] Available from: https://www.psychologytoday.com/us/blog/animal-emotions/201504/judge-recognizes-two-chimpanzees-legal-persons-first [Accessed 02 December 2018].

[6] *Brown v. Sears, Roebuck & Co.* (1987) 514 So. 2d 439. Available from: https://law.justia.com/cases/louisiana/supreme-court/1987/87-c-0726-0-1.html [Accessed 20 December 2018].

[7] Bryson, J. and Theodorou, A. (2019) How Society Can Maintain Human-Centric Artificial Intelligence. In: Marja Toivonen and Eveliina Saari (eds.). *Human Centered Digitalization and Services*. Singapore: Springer, pp. 305–323. Available from: http://www.cs.bath.ac.uk/~jjb/ftp/BrysonTheodorou19.pdf [Accessed 20 January 2019].

[8] Bucy, P.H. (1991) Corporate Ethos: A Standard for Imposing Corporate Criminal Liability. *Minnesota Law Review*, 75.

[9] Calo, R. (2011) Open Robotics. *Maryland Law Review*, 70 (3). Available from: http://ssrn.com/abstract=1706293 [Accessed 25 January 2019].

[10] Calo, R. (2016) Robots in American Law. *University of Washington School of Law Research Paper No. 2016-042*. Available from: https://ssrn.com/abstract=2737598 [Accessed 22 June 2019].

[11] Cardi, W.J. (2005) Purging Foreseeability: The New Vision of Duty and Judicial Power in the Proposed Restatement (Third) of Torts W. *Vanderbilt Law Review*, 58 (3). Available from: https://wakespace.lib.wfu.edu/handle/10339/58895 [Accessed 15 October 2018].

[12] Carpenter, C.L. (2003) On Statutory Rape, Strict Liability, and the Public Welfare Offense Model. *American University Law review*, 53 (2), pp. 313–391.

[13] Čerka, P., Grigienė, J. and Sirbikytė, G. (2017) Is It Possible to Grant Legal Personality to Artificial Intelligence Software Systems?. *Computer Law and Security Review*, 33 (5), pp. 685–699.

[14] Chadwick, P. (2018) To Regulate AI We Need New Laws, Not Just a Code of Ethics. *The Guardian*, 28 October. [online] Available from: https://www.theguardian.com/commentisfree/2018/oct/28/regulate-ai-new-laws-code-of-ethics-technology-power [Accessed 20 January 2019].

[15] Chengeta, T. (2016) Accountability Gap: Autonomous Weapon Systems and Modes of Responsibility in International Law. *Denver Journal of International Law and Policy*, 45 (1).

[16] Civil Law Rules on Robotics, European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)), 16 February. Available from: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2017-0051&language=EN&ring=A8-2017-0005 [Accessed 03 January 2019].

[17] Colvin, E. (1995) Corporate Personality and Criminal Liability. *Criminal Law Forum*, 6 (1).

[18] *Constance B. v. State of California.* (1986) 178 Cal. App. 3d 200, 206. Available from: https://law.justia.com/cases/california/court-of-appeal/3d/178/200.html [Accessed 20 December 2018].

[19] Council Directive 85/374/EEC of 25 July 1985 on the Approximation of the Laws, Regulations and Administrative Provisions of the Member States Concerning Liability for Defective Products. *Official Journal of the European Union* (L 210), 25 July. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31985L0374 [Accessed 23 January 2019].

[20] Deep Knowledge Analytics. (2018) *Artificial Intelligence Industry in the UK*. [online] London: DKA. Available from: https://www.dka.global/ai-in-uk-report [Accessed 12 May 2019].

[21] Dragatsi, H. (2011) *Criminal Liability of Canadian Corporations for International Crimes*. Canada: Thomson Reuters.

[22] *Estabrook v. J.C. Penney Co*. (1970) 464 P.2d 325 (In Banc.). Available from: https://www.courtlistener.com/opinion/1247130/estabrook-v-jc-penney-company/ [Accessed 20 December 2018].

[23] Fang, L. (2018) *Google and Facebook Are Quietly Fighting California's Privacy Rights Initiative, Emails Reveal*. [online] First Look Media. Available from: https://theintercept.com/2018/06/26/google-and-facebook-are-quietly-fighting-californias-privacy-rights-initiative-emails-reveal/ [Accessed 23 January 2019].

[24] Freitas, P.M., Andrade, F. and Novais, P. (2014) Criminal Liability of Autonomous Agents: From the Unthinkable to the Plausible. In: Pompeu Casanovas, Ugo Pagallo, Monica Palmirani and Giovanni Sartor (eds.). *AI Approaches to the Complexity of Legal Systems*. Berlin: Springer.

[25] Gaur, K.D. (2003) Principles of Criminal Liability. In: K.D. Gaur (ed.). *Criminal Law and Criminology*. New Delhi: Deep and Deep Publications.

[26] Geistfeld, M.A. (2017) A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation. *California Law Review*, 105.

[27] Gless, S. Silverman, E. and Weigend, T. (2016) If Robots Cause Harm, Who Is to Blame? Self-Driving Cars and Criminal Liability. *New Criminal Law Review*, 19 (3).

[28] Grace, K. et al. (2018) Viewpoint: When Will AI Exceed Human Performance? Evidence from AI Experts. *Journal of Artificial Intelligence Research*, 62, pp. 729–754.

[29] Hallevy, G. (2010) ‘I, Robot – I, Criminal’ – When Science Fiction Becomes Reality: Legal Liability of AI Robots Committing Criminal Offenses. *Syracuse Science and Technology Law Reporter*, 22 (spring).

[30] Hallevy, G. (2013) *When Robots Kill: Artificial Intelligence under Criminal Law*. Boston: Northeastern University Press.

[31] Hallevy, G. (2015) *Liability for Crimes Involving Artificial Intelligence Systems*. Springer International Publishing.

[32] Houvast, F. Timmerman, R. and Zwaan, Y. (2018) Exploring the Legal Rights & Obligations of Robots: A Legal Book Review of I, Robot by Isaac Asimov reviewed in *Law & Literature Project, Utrecht University*.

[33] Hubbard, P. (2014) 'Sophisticated Robots’: Balancing Liability, Regulation, and Innovation. *Florida Law Review*, 66 (5), pp. 1803–1872.

[34] Judicial Council of California. (2017) *California Civil Jury Instruction 2017 Edition (“CACI”) No. 401*. [online] Available from: https://www.justia.com/trials-litigation/docs/caci/400/401/ [Accessed 20 December 2018].

[35] Karnow, C.E.A. (1996) Liability for Distributed Artificial Intelligences. *Berkeley Technology Law Journal*, 11 (1), pp. 147–204. Available from: http://scholarship.law.berkeley.edu/btlj/vol11/iss1/3 [Accessed 29 November 2018].

[36] Karnow, C.E.A. (2013) The Application of Traditional Tort Theory to Embodied Machine Intelligence. In: Ryan Calo, Michael Froomkin, Ian Kerr (eds.). *Robot Law*. Cheltenham: Edward Elgar Publishing Ltd, pp. 51–77.

[37] Kelley, R. et al. (2010) Liability in Robotics: An International Perspective on Robots as Animals. *Advanced Robotics*, 24 (13), pp. 1861–1871.

[38] Lawrence, F. (2000) In Defense of Corporate Criminal Liability. *Harvard Journal of Law & Public Policy*, 23 (3).

[39] Lederman, E. (2000) Models for Imposing Corporate Criminal Liability: From Adaptation and Imitation Toward Aggregation and the Search for Self-Identity. *Buffalo Criminal Law Review*, 4 (1), pp. 641–708.

[40] Manjoo, F. (2016) Tech’s ‘Frightful 5’ Will Dominate Digital Life for Foreseeable Future. *N.Y. Times*, 20 January. [online] Available from: https://www.nytimes.com/2016/01/21/technology/techs-frightful-5-will-dominate-digital-life-for-foreseeable-future.html [Accessed 10 January 2019].

[41] Meyer, D. (2017) *Inside the EPrivacy Regulation's Furious Lobbying War*. [online] Kansas City: IAAP. Available from: https://iapp.org/news/a/inside-the-eprivacy-regulations-urious-lobbying-war/ [Accessed 23 January 2019].

[42] Meyer, J.A. (2007) Authentically Innocent: Juries and Federal Regulatory Crimes. *Hastings Law Journal*, 59 (1).

[43] *Morissette v. United States*. (1952) 342 U.S. 246. Available from: https://supreme.justia.com/cases/federal/us/342/246/ [Accessed 28 January 2019].

[44] Muchlinski, P.T. (2007) *Multinational Enterprises and the Law*. Oxford: Oxford University Press.

[45] Murphy, M. (2017) Stephen Hawking: AI Could Be Best – or Worst – Thing in Human History. [online] New York City: MarketWatch. Available from: https://www.marketwatch.com/story/stephen-hawking-ai-could-be-best-or-worst-thing-in-human-history-2017-11-06 [Accessed 29 October 2018].

[46] Nemitz, P. (2018) Constitutional Democracy and Technology in the Age of Artificial Intelligence. [in press] Submitted to: *Philosophical Transactions of the Royal Society A*. Available from: https://ssrn.com/abstract=3234336 [Accessed 07 January 2019].

[47] Osborne, S. (2017) Elon Musk Calls for Urgent Laws on Robot as They Will Soon Be Risk to Public. *Express*, 28 November. [online] Available from: https://www.express.co.uk/news/science/885344/elon-musk-artificial-intelligence-robotics-regulation [Accessed 29 October 2018].

[48] Owen, D. (2009) Figuring Foreseeability. *Wake Forest Law Review*, 44, pp. 1277–1307.

[49] Palmer, A. (2010) Autonomous UAS: a partial solution to America's future airpower needs. [pre-print] Submitted to: *Air University in partial fulfillment of the graduation requirements*. Available from: https://apps.dtic.mil/dtic/tr/fulltext/u2/1018416.pdf [Accessed 29 November 2018].

[50] Pasquale, F. (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, Massachusetts: Harvard University Press.

[51] Pratt, G.A. (2015) Is a Cambrian Explosion Coming for Robotics?. *Journal of Economic Perspectives*, 29 (3).

[52] Radutniy, O.E. (2017) Criminal Liability of the Artificial Intelligence. *Problems of Legality*, 138.

[53] Reitz, M.J. (2013) *Strict Liability and Public Welfare Offenses*. [online] Midland: Mackinac Center. Available from: https://www.mackinac.org/19579 [Accessed 21 January 2019].

[54] Retto, J. (2017) *Sophia, First Citizen Robot of the World*. [online] Available from: https://www.researchgate.net/publication/321319964_SOPHIA_FIRST_CITIZEN_ROBOT_OF_THE_WORLD [Accessed 29 November 2018] .

[55] Robertson, J. (2014) Human Rights vs. Robot Rights: Forecasts from Japan. *Critical Asian Studies*, 46 (4), pp. 571–598.

[56] Robotics Open Letter. (2017) *Open Letter to the European Commission Artificial Intelligence and Robotics*. [online] Available from: http://www.robotics-openletter.eu/ [Accessed 20 January 2019].

[57] Roff, H.M. (2013) Killing in War: Responsibility, Liability and Lethal Autonomous Robots. In: Fritz Allhoff, Nicholas Evans and Adam Henschke (eds.). *Routledge Handbook of Ethics and War: Just War Theory in the 21st Century*. Routledge Press.

[58] Rothblatt, M. and Angelica, A.D. (2003) *Bio-Cyber-Ethics: Should We Stop a Company from Unplugging an Intelligent Computer?*. [blog entry] 28 September. Available from: http://www.kurzweilai.net/biocyberethics-should-we-stop-a-company-from-unplugging-an-intelligent-computer [Accessed 24 October 2018].

[59] Sparrow, R. (2007) Killer Robots. *Journal of Applied Philosophy*, 24 (1).

[60] Sperino, S. (2010) A Modern Theory of Direct Corporate Liability for Title VII. *Faculty Articles and Other Publications Paper 230*. Available from: https://scholarship.law.uc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1233&context=fac_pubs [Accessed 21 January 2019].

[61] *Staples v. United States*. (1994) 511 U.S. 600. Available from: https://supreme.justia.com/cases/federal/us/511/600/ [Accessed 28 January 2019].

[62] Stoitchkova, D. (2010) *Towards Corporate Liability in International Criminal Law*. Utrecht: Utrecht University.

[63] Suhariyanto, B. (2018) Corporate Criminal Liability Under the Reactive Corporate Fault to Achieve Good Corporate Governance in Indonesia. In: A. Raharjo and T. Sudrajat (eds.). *The 1st International Conference on Law, Governance and Social Justice, Purwokerto*, 25–26 September. Les Ulis: EDP Sciences. Available from: https://www.shs-conferences.org/articles/shsconf/pdf/2018/15/shsconf_icolgas2018_07009.pdf [Accessed 20 January 2019].

[64] Toon, J. (2017) *Swarms of Autonomous Aerial Vehicles Test New Dogfighting Skills*. [online] Atlanta: GeorgiaTech. Available from: http://www.rh.gatech.edu/news/590743/swarms-autonomous-aerial-vehicles-test-new-dogfighting-skills [Accessed 15 May 2019].

[65] Vojislav, K. (2001) *Learning and Soft Computing: Support Vector Machines, Neutral Networks and Fuzzy Logic Models*. Cambridge: The MIT Press.

[66] Whittaker, M. et al. (2018) *AI Now Report*. [online] New York City: AI Now Institute. Available from: https://ainowinstitute.org/AI_Now_2018_Report.pdf [Accessed 19 December 2018].

[67] Willick, M. (1983) Artificial Intelligence: Some Legal Approaches and Implications. *AI Magazine*, 4 (2). Available from: https://aaai.org/ojs/index.php/aimagazine/article/view/392 [Accessed 29 November 2018].

[68] Wootson, C. (2017) *Saudi Arabia, Which Denies Women Equal Rights, Makes a Robot a Citizen*. [online] Available from: https://www.ndtv.com/world-news/saudi-arabia-which-denies-women-equal-rights-makes-a-robot-a-citizen-1768666 [Accessed 20 January 2019].

[69] Zerk, J.A. (2006) *Multinationals and Corporate Social Responsibility: Limitations and Opportunities in International Law*. New York: Cambridge University Press.

DOI 10.5817/MUJLT2020-1-4

LAW APPLICABLE TO CLOUD COMPUTING CONTRACTS CONCLUDED WITH CONSUMERS UNDER REGULATION 593/2008, ACCORDING TO THE CJEU CASE LAW[*]

by

KRZYSZTOF ŻOK[**]

The undoubted popularity of cloud computing stems in particular from the fact that the provider can simultaneously offer access to his or her computing resources to an almost unlimited number of users located in different countries. Although this feature brings significant benefits to the provider, it also raises serious questions regarding the law governing the contract. The concerns become especially relevant in the case of contracts concluded between a consumer and a professional due to the limits of the choice of law and the special rules protecting consumers.

The article analyses the law applicable to cloud computing contracts concluded with consumers. The considerations focus on the special provisions regarding consumer protection. Contrary to some comments, the article claims that the current legal framework is sufficient to determine the applicable law, although this task is not without doubts.

KEY WORDS

Applicable Law, Cloud Computing, Contract Law, International Private Law

1. THE UBIQUITY OF CLOUD COMPUTING

Cloud computing has become commonly used in many areas of everyday life. Despite its popularity, this IT solution has yet not been defined in legal

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

[**] krzysztof.zok@amu.edu.pl; Faculty of Law and Administration, Adam Mickiewicz University in Poznań, Poland.

acts recognized at the European or international level. However, the gap can be filled by the recommendations of the *National Institute of Standards and Technology*, an agency of the *US Department of Commerce*.[1] The recommendations define the term "cloud computing" as

> *"a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*[2]

It is worth noting that "ubiquity" begins the list of characteristics of cloud computing. Although the term is not further explained, the recommendations justify the assumption that it refers to the ability to access the cloud at any time and place by an almost unlimited number of users. More importantly, mentioning ubiquity as the first feature of that IT solution is not entirely accidental. From the user's perspective, this characteristic translates into convenient access to provider's computing resources. It should also be noted that the fee paid by the user firstly covers the cost of establishing the cloud infrastructure. Then, the rest of the fee generates the provider's income. Moreover, the cost of establishing the infrastructure is relatively fixed. Therefore, when more and more users are paying for the cloud, the part of the fee constituting the provider's income is growing at a faster pace. This stems from the fact that the relatively fixed costs related to the infrastructure are shared among an increasing number of users. Consequently, the ubiquity of the clouds also offers significant benefits for the provider, enabling them to achieve economies of scale. It should also be emphasized that the rapidly growing online communication creates a demand for cloud computing. Nevertheless, establishing a robust infrastructure is often expensive. As the result, people interested in using the clouds usually have to rely on third parties, i.e. cloud service providers. The ubiquity of cloud computing is thus arguably one of the main reasons for the popularity of this IT solution.

[1] Mell, P. and Grance, T. (2011) *The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology.* [online] Gaithersburg: National Institute of Standards and Technology. Available from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf [Accessed 13 January 2020].

[2] Ibid.

From the legal point of view, the feature allows the provider to easily enter into contracts with users from various countries. The provider can thereby reduce the period in which the cloud is not working at its full potential. However, the ubiquity of cloud computing also exposes the provider to the risk of simultaneously applying multiple legal systems to essentially the same contract.[3] Therefore, the provider also faces the risk of not being able to dynamically comply with the requirements of different legal systems. As a result, the question of the law applicable to cloud computing contracts may often arise, especially in the context of consumer contracts due to the special rules of consumer protection and the mass nature of these agreements. The uncertainty as to the law governing the contract is not insignificant given the broad use of cloud computing.

According to some scholars, the issue does not present serious problems because the existing legal framework sufficiently determines the law governing cloud computing contracts.[4] However, this stance is not unanimously shared. Some scholars claim that determining the law applicable to cloud computing contracts is often difficult.[5] Others argue that the current legal analysis is not keeping pace with the rapid development of the discussed IT solution.[6] This may, in turn, translate into difficulties in determining the law applicable to these agreements. It is also claimed that the framework of international private law is no longer adequate for cloud computing contracts.[7] However, it should be noted that the above comments are often general.

In my opinion, these reservations are not fully convincing. The paper argues that the existing legal framework suffices to determine the law applicable to cloud computing contracts concluded with consumers.

[3] Castro, C., Reed, Ch. and de Queiroz, R. (2013) On the Applicability of the Common European Sales Law to Some Models of Cloud Computing Services. *European Journal of Law and Technology*, 4 (3). Available from: http://ejlt.org/article/view/186/409 [Accessed 13 January 2020].

[4] Haibach, G. (2015) Cloud computing and European Union private international law. *Journal of Private International Law*, 11 (2), p. 262.

[5] De Filippi, P. and McCarthy, S. (2012) Cloud Computing: Centralization and Data Sovereignty. *European Journal of Law and Technology*, 3 (2). Available from: http://ejlt.org/article/view/101 [Accessed 13 January 2020]; De Filippi, P. and Belli, L. (2012) Law of the Cloud v Law of the Land: Challenges and Opportunities for Innovation. *European Journal of Law and Technology*, 3 (2). Available from: http://ejlt.org/article/view/156 [Accessed 13 January 2020].

[6] Andrews, C.D. and Newman, J.M. (2013) Personal Jurisdiction and Choice of Law in the Cloud. *Maryland Law Review*, 73, p. 315.

[7] Celestine, C.M. (2013) "Cloudy" Skies, Bright Futures? In Defense of a Private Regulatory Scheme for Policing Cloud Computing. *Journal of Law, Technology & Policy*, 1, p. 152.

However, this task is not without doubts. The difficulties concern in particular the question of determining if the provider demonstrated the intention to enter into a contract with the consumer domiciled in a specific country. Therefore, the paper focuses on the special provisions regarding the law applicable to consumer contracts. It examines the choice of law and the general provisions concerning the law which governs the contract only to the extent that is necessary for the above analysis.

2. DETERMINING THE APPLICABLE LAW

2.1. THE CHOICE OF LAW AND ITS LIMITS

The provider usually offers standard terms, especially if the contract is concluded with the consumer.[8] The provider thus reduces the risks associated with the simultaneous performance of different obligations. The global nature of clouds, however, undermines this strategy. At first sight, the risk can easily be avoided by choosing the law applicable to the agreement, particularly the law of the country where the provider is established. Indeed, empirical studies confirm that cloud computing contracts often specify the law which governs them.[9] Nevertheless, the choice of law does not dispel all doubts. The applicable law provided for in the contract may adversely affect the user's situation. In particular, it may weaken the protection enjoyed by the consumer under his or her domestic law. Moreover, the user may not be familiar with the law specified in the contract.

Therefore, it should be emphasized that European law protects consumers not only through substantive law, but also through international private law. The protection also applies if a choice of law has been made. According to Article 3(1) of Regulation 593/2008, the choice must be made expressly or clearly demonstrated by the terms of the contract

[8] Bradshaw, S., Millard, Ch. and Walden, I. (2011) Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. *International Journal of Information Technology and Law*, 19 (3), pp. 188–189; Irion, K. (2015) Your Digital Home is No Longer Your Castle: How Cloud Computing Transforms the (Legal) Relationship Between Individuals and Their Personal Records. *International Journal of Law and Information Technology*, 23, p. 358.

[9] Bradshaw, S., Millard, Ch. and Walden, I. (2011) Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. *International Journal of Information Technology and Law*, 19 (3), pp. 198–199; Haibach, G. (2015) Cloud computing and European Union private international law. *Journal of Private International Law*, 11 (2), p. 259.

or the circumstances of the case.[10] The analysis of this provision lies beyond the scope of the current considerations as it would exceed volume limits of this paper. However, it should be noted that failure to meet the requirements set in Article 3(1) of Regulation 593/2008 precludes the application of the chosen law to the contract. Furthermore, the choice of law may be considered unenforceable under Directive 93/13.[11] There is, of course, no abstract answer to the question whether the choice of law for a particular cloud computing contract is legally binding.[12] Nevertheless, such situations cannot be completely ignored. Consequently, if the parties do not make a legally binding choice of law, the law governing the contract is determined by Article 6(1) of Regulation 593/2008 which contains a special rule for consumer contracts. Only if this provision cannot also be applied, the applicable law is determined on the basis of the general rules in Article 4 of the Regulation. The conclusion also covers a situation in which the choice of law is void.

Moreover, even if the choice of law is effective, according to Article 6(2) of Regulation 593/2008, the applicable law specified in the contract cannot deprive the consumer of the protection afforded to him or her by the provisions which cannot be derogate from by agreement by virtue of the law which would have been applicable based on Article 6(1) of the Regulation. The provider may, therefore, be often unable to fully subject the contract to the law which they considers the most appropriate. It can even be expected that at least some of the obligations will be determined by the law applicable under Article 6(1) of Regulation 593/2008.[13] Consequently, it is claimed that many contractual provisions drawn by the providers established in the USA may not be legally binding

[10] Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I). *Official Journal of the European Union* (2008/177-L/6), 4 July. Available from: http://data.europa.eu/eli/reg/2008/593/oj [Accessed 13 January 2020].

[11] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts. *Official Journal of the European Communities* (1993/95-L-29), 21 April. Available from: http://data.europa.eu/eli/dir/1993/13/oj [Accessed 13 January 2020].

[12] Wauters, E., Lievens, E. and Valcke, P. (2014) Towards a Better Protection of Social Media Users: a Legal Perspective on the Terms of Use of Social Networking Sites. *International Journal of Law and Information Technology*, 22, p. 278.

[13] Castro, C., Reed, Ch. and de Queiroz, R. (2013) On the Applicability of the Common European Sales Law to some Models of Cloud Computing Services. *European Journal of Law and Technology*, 4 (3). Available from: http://ejlt.org/article/view/186/409 [Accessed 13 January 2020]; Irion, K. (2015) Your Digital Home is No Longer Your Castle: How Cloud Computing Transforms the (Legal) Relationship Between Individuals and Their Personal Records. *International Journal of Law and Information Technology*, 23, pp. 367–368.

for consumers domiciled in the *European Union*.[14] This conclusion is also supported by the recent judgments in which the *Court of Justice of the European Union* decided that the lack of information about the law applicable under Article 6(2) of Regulation 593/2008, which causes consumer's error about the provisions which cannot be derogated from by agreement, may be an unfair term within the meaning of Article 3 of Directive 93/13.[15]

From this perspective, it can be argued that the choice of law is more relevant for small-to-medium entrepreneurs than for consumers, who enjoy the protection under European law.[16] The above considerations also clearly illustrate the importance of determining the law applicable to cloud computing contracts based on Article 6(1) of Regulation 593/2008. The law specified in this provision may often set the minimum standards of consumer protection or even govern the contract.

2.2. THE LAW OF THE COUNTRY WHERE THE CONSUMER IS DOMICILED

Pursuant to Article 6(1) of Regulation 593/2008, if the parties do not choose the applicable law, the contract concluded between a consumer and a professional is governed by the law of the country where the consumer has his or her habitual residence, given that other requirements set in this provision are met. In contrast to the general rules, Article 6(1) of the Regulation does not refer to the classification of the contracts. The difference is, however, irrelevant since under Articles 4(1)(b) and 4(2) thereof the contract would be governed by the law of country of the provider's domicile regardless of its qualification.

Besides, as pointed in Recitals 7 and 24 of Regulation 593/2008, Article 6(1) thereof is closely linked to Article 15(1)(c) of Regulation

[14] McGillivray, K. (2016) A Right Too Far? Requiring Cloud Service Providers to Deliver Adequate Data Security to Consumers. *International Journal of Law and Information Technology*, 25, p. 7; Rustad, M.L. and Onufario, M.V. (2012) Reconceptualizing Consumer Terms of Use for a Globalized Knowledge Economy. *University of Pennsylvania Journal of Business Law*, 14 (4), p. 1116.

[15] See judgment of 28 July 2016, *Verein für Konsumenteninformation v. Amazon EU Sàrl*, C-191/15, EU:C:2016:612; judgment of 3 October 2019, *Verein für Konsumenteninformation v. TVP Treuhand- und Verwaltungsgesellschaft für Publikumsfonds mbH & Co KG*, EU:C:2019:827.

[16] Bradshaw, S., Millard, Ch. and Walden, I. (2011) Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. *International Journal of Information Technology and Law*, 19 (3), p. 198.

44/2001[17] which was replaced by Article 17(1)(c) of Regulation 1215/2012.[18] The above provisions undoubtedly aim to improve consumer protection, especially in the case of contracts concluded over the Internet.[19] Therefore, they take precedence over the general rules. As a result, the *Court of Justice of the European Union* repeatedly stressed that Article 15(1)(c) of Regulation 44/2001, as an exception, should be interpreted strictly.[20] Although this stance only refers to the provision of Regulation 44/2001, it remains valid in the context of Article 6(1) of Regulation 593/2008 and Article 17(1)(c) of Regulation 1215/2012 due to the link described above.

From this point of view, the correct interpretation of Article 6(1) of Regulation 593/2008 is crucial. The application of this provision depends on two requirements. Firstly, the professional must pursue his or her commercial or professional activities in the country where the consumer is domiciled. Alternatively, the professional has to direct the activities to that country. Secondly, the contract should fall within the scope of the professional's activities. The latter requirement does not raise important legal questions related to cloud computing contracts. Doubts may, however, concern the fulfilment of the first requirement which consists of two alternative conditions.

3. PURSUING THE PROFESSIONAL'S ACTIVITIES

According to Article 6(1)(a) of Regulation 593/2008, the contract is governed by the law of the country where the consumer is domiciled if the professional pursues his or her commercial or professional activities in that country. The wording of this provision is clear. However, the question arises about the significance of Article 6(1)(a) of Regulation

[17] Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. *Official Journal of the European Union* (2001/12-L/1), 16 January. Available from: http://data.europa.eu /eli/reg/2001/44/oj [Accessed 13 January 2020].

[18] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast). *Official Journal of the European Union* (2012/351-L/1), 20 December. Available from: http://data.europa.eu/eli/reg/2012/1215/2015-02-26 [Accessed 13 January 2020].

[19] For such an interpretation of Article 15(1)(c) of Regulation 44/2001, see e.g. *Ilsinger* (2009) C-180/06, EU:C:2009:303, paragraph 50, 14 May; *Mühlleitner* (2012) C-190/11, EU:C:2012:542, paragraph 29, 6 September; *Emrek* (2013) C-218/12, EU:C:2013:666, paragraph 24, 17 October.

[20] *Mühlleitner* (2012) C-190/11, EU:C:2012:542, paragraph 27, 6 September; *Česká spořitelna* (2013), C-419/11, EU:C:2013:165, paragraph 26, 14 March; *Kolassa* (2015), C-375/13, EU:C: 2015:37, paragraph 28, 28 January; *Schrems* (2018), C-498/16, EU:C:2018:37, paragraph 45, 25 January.

593/2008 for cloud computing contracts. Empirical studies indicate that providers often choose a law of a particular state in the USA.[21] As a result, it can be argued that Article 6(1)(a) of Regulation 593/2008 rarely applies to cloud computing contracts concluded with consumers domiciled in the European Union, since the providers generally do not pursue their activities in the Member States.

Indeed, the above provision seems to be of lesser significance in comparison to Article 6(1)(b) of Regulation 593/2008. Because of the ubiquity, the pursuit of the activities in a certain country is not essential for the conclusion and performance of cloud computing contracts concluded with the consumer domiciled in that country. Nevertheless, in my opinion, Article 6(1)(a) of Regulation 593/2008 is not entirely without significance in the case of cloud computing contracts. Several major companies on the cloud market have their local offices in selected countries of the *European Union*. For example, *Microsoft* offices operate in all Member State,[22] *Google* offices – in 13 Member States,[23] *Spotify* offices – in 11 Member States[24] and *Dropbox* offices – in 4 Member States.[25] Therefore, at least some providers pursue their activities in the country of the consumer's domicile. Consequently, Article 6(1)(a) of Regulation 593/2008 may apply to cloud computing contracts. This, however, does not change the fact that not all consumers are covered by the above provision, since the providers do not always operate in the country where the consumer has his or her habitual residence.

[21] Castro, C., Reed, Ch. and de Queiroz, R. (2013) On the Applicability of the Common European Sales Law to some Models of Cloud Computing Services. *European Journal of Law and Technology*, 4 (3). Available from: http://ejlt.org/article/view/186/409 [Accessed 13 January 2020]; Haibach, G. (2015) Cloud computing and European Union private international law. *Journal of Private International Law*, 11 (2), pp. 255, 263 and 266; Irion, K. (2015) Your Digital Home is No Longer Your Castle: How Cloud Computing Transforms the (Legal) Relationship Between Individuals and Their Personal Records. *International Journal of Law and Information Technology*, 23, pp. 367–368. For empirical studies, see Bradshaw, S., Millard, Ch. and Walden, I. (2011) Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. *International Journal of Information Technology and Law*, 19 (3), pp. 198–199.

[22] Microsoft. (2020) *Microsoft Office Locations Around the World*. [online] Available from: https://www.microsoft.com/en-us/worldwide.aspx [Accessed 13 January 2020].

[23] Google. (2019) *Our Offices*. [online] Google. Available from: https://about.google/locations/?region=europe [Accessed 13 January 2020].

[24] Spotify. (2020) *About Us*. [online] Available from: https://www.spotify.com/about-us/contact [Accessed 13 January 2020].

[25] Dropbox. (2019) *Join Us Around the World*. [online] Available from: https://www.dropbox.com/jobs/locations [Accessed 13 January 2020].

4. DIRECTING THE PROFESSIONAL'S ACTIVITIES

4.1. THE SIGNIFICANCE OF THE PROFESSIONAL'S INTENTION

In accordance with Article 6(1)(b) of Regulation 593/2008, the law of the country in which the consumer is domiciled governs the contract if the professional, by any means, directs his or her activities to that country. The provision is particularly important for cloud computing contracts, since the provider does not have to establish an office in a Member State to allow the consumer to access the cloud. The ubiquity of that IT solution facilitates offering computing resources to consumers having their habitual residence in countries other than the one in which the provider pursues his or her activities. As a result, it is claimed that Article 6(1)(b) of Regulation 593/2008 often determines the law applicable to the discussed contracts.[26] Without questioning this conclusion, in my opinion, it is necessary to provide a more in-depth analysis of the applicability of Article 6(1)(b) of Regulation 593/2008 to cloud computing contracts.

The above provision refers to the concept of directed activities. However, Regulation 593/2008 does not explain how to verify whether the activities are "directed" to the country where the consumer is domiciled. The Regulation only specifies that the activities should be of a commercial or professional nature. Consequently, the key element determining the scope of Article 6(1)(b) of Regulation 593/2008 remains unclear. This uncertainty may easily translate into practical concerns. In particular, it could be argued that the provision applies to any situation in which the information of contractual significance (offer, invitation to treat, advertisement, etc.) is placed in a way accessible to the consumer. The indication that the activities can be directed "by any means" seems to additionally support the broad understanding of Article 6(1)(b) of Regulation 593/2008. Similarly, the purpose of the provision, i.e. the improvement of consumer protection, only strengthens this argument.

However, such a broad interpretation would subject almost all contracts concluded over the Internet to Article 6(1)(b) of Regulation 593/2008. This

[26] Bradshaw, S., Millard, Ch. and Walden, I. (2011) Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. *International Journal of Information Technology and Law*, 19 (3), p. 198; Castro, C., Reed, Ch. and de Queiroz, R. (2013) On the Applicability of the Common European Sales Law to some Models of Cloud Computing Services. *European Journal of Law and Technology*, 4 (3). Available from: http://ejlt.org/article/view/186/409 [Accessed 13 January 2020].

would certainly be the case in cloud computing contracts, since providers often present contractual information on their websites. More importantly, the provision would apply even if the professional does not intend to conclude contracts with consumers domiciled in a specific country. Such an interpretation could often be detrimental to professionals who would not be able to predict the law applicable to the contract.

Nevertheless, the lack of explanation of the concept of directed activities is not without reason. Instead of defining the term, Recital 24 of Regulation 593/2008 refers in this regard to Article 15(1)(c) of Regulation 44/2001 which was replaced by Article 17(1)(c) of Regulation 1215/2012. Regulation 593/2008 thereby aims to maintain harmony with the provisions on jurisdiction. Yet, even the reference to the provisions of Regulations 44/2001 and 1215/2012 does not dispel all doubts. None of the Regulations explains how to verify whether the professional directs his or her activities to the country where the consumer is domiciled. The gap is, however, filled by the interpretation of Article 15(1)(c) of Regulation 44/2001 by the *Court of Justice of the European Union*.[27] According to the judgment, the concept of directed activities only covers situations in which the professional intended to conclude the contract in the country where the consumer has his or her habitual residence. The stance is based on the comparison of Article 13(3) of *Brussels Convention*[28] and its successor, i.e. Article 15(1)(c) of Regulation 44/2001.[29]

Although this position is well-founded, it inevitably leads to the question of how to determine the intention of the professional. The issue may raise serious practical concerns since analysing people's motivation is often associated with difficulties. In particular, the intention of the professional can usually be verified only on the basis of inference, i.e. by considering the circumstances surrounding the conclusion of the contract. Therefore, it is worth noting that the *Court of Justice of the European Union* provided a list of factors which can be used to determine whether the professional intended to enter into contracts with consumers domiciled in a specific country. The factors can be divided into

[27] *Hotel Alpenhof* (2010), C-585/08 and C-144/09, EU:C:2010:740, paragraphs 65–69 and 74–76, 7 December.

[28] *Brussels Convention on jurisdiction and the enforcement of judgments in civil and commercial matters*, 1968, (1972/L 299/32). Available from: https://curia.europa.eu/common/recdoc/convention/en/c-textes/brux.htm [Accessed 13 January 2020].

[29] *Hotel Alpenhof* (2010), C-585/08 and C-144/09, EU:C:2010:740, paragraph 57, 7 December.

positive and negative. The former can further be divided into explicit (i.e. confirming that the professional intended to conclude contracts with consumers domiciled in a certain country) and implicit (i.e. only suggesting such an intention). A relatively large number of factors may not only offer valuable guidelines, but also force parties or the court to weigh potentially conflicting hints.[30] Consequently, it should be considered if the factors support the application of Article 6(1)(b) of Regulation 593/2008 to cloud computing contracts.

4.2. EXPLICIT POSITIVE FACTORS

According to the *Court of Justice of the European Union*, Article 6(1)(b) of Regulation 593/2008 applies if the professional clearly indicates that they offers goods or services in a specific country.[31] This comment is useful for cloud computing contracts because sometimes providers explicitly name the countries where they offer access to the cloud. For instance, *Spotify* and *Microsoft* created such a list.[32] Nevertheless, identifying the above factor may not always be an easy task. The providers often do not state that they want to enter into contracts with consumers domiciled in a certain country. For instance, *Google* refers to broadly understood *"[c]ustomer [who] has a billing address in the EU,"* thereby not indicating the country by name.[33] However, sometimes the terms of service may indirectly point to a specific country or a group of countries. For example, the *Dropbox Terms of Service* refer to the *European Union* several times, mostly in the context of consumer protection (i.e. the right of withdrawal, the prorogation of jurisdiction and the applicable law).[34] A similar provision is also stipulated in the *Facebook Terms of Service*.[35]

Therefore, the question arises whether such information clearly indicates that the provider envisaged doing business with consumers who have their

[30] Bogdan, M. (2011) Website Accessibility as Basis for Jurisdiction under the Brussels I Regulation. *Masaryk University Journal of Law and Technology*, 5 (1), p. 8.

[31] *Hotel Alpenhof* (2010), C-585/08 and C-144/09, EU:C:2010:740, paragraph 81, 7 December.

[32] Microsoft. (2019) *Microsoft Cloud Agreements by Region and Language*. [online] Available from: https://docs.microsoft.com/en-us/partner-center/agreements [Accessed 13 January 2020]; Spotify. (2019) *Spotify Terms and Conditions of Use*. [online] Available from: https://www.spotify.com/legal/end-user-agreement/ [Accessed 13 January 2020].

[33] Google. (2019) *Google Cloud Platform Terms of Service*. [online] Available from: https://cloud.google.com/terms/ [Accessed 13 January 2020].

[34] Dropbox. (2019) *Dropbox Terms of Service*. [online] Dropbox. Available from: https://www.dropbox.com/terms?view_en#terms [Accessed 13 January 2020].

[35] Facebook. (2019) *Terms of Service*. [online] Facebook. Available from: https://www.facebook.com/legal/terms [Accessed 13 January 2020].

habitual residence in a specific country. In my opinion, the answer requires careful consideration not only of the quantity, but also of the quality of the information given by the provider. In particular, the intention to conclude the contract with the consumer domiciled in a Member State may manifest by referring to the matters of consumer protection, e.g. the provisions which cannot be derogated by agreement, the right of withdrawal or the rights available in the event of the provider's non-performance. From this perspective, it can be argued that the above information sufficiently demonstrates the intention required under Article 6(1)(b) of Regulation 593/2008. Yet, even if the information cannot be regarded as a clear declaration of intention to do business in a specific country, it may still be classified as a positive indirect factor. Consequently, the information is not devoid of significance. In combination with other factors, it may justify the application of Article 6(1)(b) of Regulation 593/2008.

It should also be noted that the provider may explicitly limit directing his or her activities only to a specific country or a group of countries. Currently, this model is not widely adopted by the providers operating mainly on the public cloud market. However, granting access to the cloud only to selected users is typical for private clouds.[36] Therefore, it can be assumed that Article 6(1)(b) of Regulation 593/2008 generally does not apply to contracts concerning private clouds, although the conclusion should be drawn after case-by-case analysis.[37]

Furthermore, the contract is governed by the law of the country where the consumer has his or her habitual residence if the professional invests in referencing services to attract the consumers domiciled in a particular country.[38] It can be expected that this requirement is usually met for large companies offering access to the cloud. For example, displaying the provider's website as the first search result with an indication that the result is an advertisement may confirm the use of the above service.

[36] Mell, P. and Grance, T. (2011) *The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology*. [online] Gaithersburg: National Institute of Standards and Technology. Available from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf [Accessed 13 January 2020].

[37] Haibach, G. (2015) Cloud computing and European Union private international law. *Journal of Private International Law*, 11 (2), p. 263.

[38] *Hotel Alpenhof* (2010), C-585/08 and C-144/09, EU:C:2010:740, paragraph 81, 7 December.

4.3. IMPLICIT POSITIVE FACTORS

The intention to enter into contracts with consumers domiciled in a certain country can be indirectly demonstrated by undertaking activities which by their nature are international.[39] At first glance, the factor appears to be particularly useful for cloud computing contracts. The ubiquity of cloud computing almost implies the international nature of these agreements. The general description seems to further support the application of this factor to cloud computing contracts. Consequently, it is claimed that the factor is often present in the case of these agreements due to their global nature.[40]

In my opinion, however, it should be emphasized that the provider may not take advantage of the potential of clouds to undertake international activities. The provider may simply choose to do business only with consumers who have their habitual residence in the country of the provider's establishment. Therefore, the use of cloud computing as such does not demonstrate the intention required under Article 6(1)(b) of Regulation 593/2008. Rather, it is necessary to consider the type of activities undertaken by the provider, not the IT solution used to perform these activities. It is worth noting that the *Court of Justice of the European Union* pointed to certain tourist activities, not to the website or the Internet, as an example of activities of international nature.[41] Therefore, the cloud storage may manifest the intention if the provider declares that the files are accessible in any Member State or may not demonstrate that intention if the provider states that the files are accessible only in the country of his or her establishment.

Moreover, the contract may be governed by the law of the country where the consumer is domiciled if the professional mentions phone number with the international code or uses a top-level domain name specific to the country other than the one in which they is established (e.g. the professional uses domain with ".de" suffix, although they operates in Sweden).[42] This also includes neutral top-level domain names (e.g. ".com" or ".eu").

[39] *Hotel Alpenhof* (2010), C-585/08 and C-144/09, EU:C:2010:740, paragraph 83, 7 December.

[40] Haibach, G. (2015) Cloud computing and European Union private international law. *Journal of Private International Law*, 11 (2), p. 263.

[41] *Hotel Alpenhof* (2010), C-585/08 and C-144/09, EU:C:2010:740, paragraph 83, 7 December.

[42] Ibid. Similarly with the reference to phone number, see *Emrek* (2013), C-218/12, EU:C:2013: 666, paragraph 30, 17 October.

The reference to a phone number may not offer valuable insight for cloud computing contracts because the providers do not always specify such a number. Instead, they may allow the users to enter the chat, which can be seen as a substitute for phone calls,[43] send an e-mail, or post a message on *Twitter* or community forum.[44] These means of communication as such do not provide information about the intention to do business in a specific country. In particular, the intention required under Article 6(1)(b) of Regulation 593/2008 cannot be determined solely based on the e-mail or geographical address of the professional or his or her intermediary.[45] However, the indication of the means of communication can be analysed together with other circumstances. For example, offering a chat in Spanish by the provider established in Ireland may indicate that they intended to enter into contracts with consumers domiciled in Spain.

On the other hand, the top-level domain name can be a source of information as to whether the provider envisaged doing business in a Member State. This stems from the fact that providers often use multiple top-level domain names to attract consumers from various countries. For example, *Facebook* controls many top-level domain names which are prefixed by a language indicator and suffixed by a general name ".com".[46] Similarly, the last part of *Microsoft* top-level domain names consists of a language indicator.[47] Therefore, the activities of such providers can be regarded as directed to consumers having their habitual residence in the country covered by the language indicator. This conclusion is further supported if the website available under such domain name contains information in a corresponding language.

The professional's intention necessary to trigger the application of Article 6(1)(b) of Regulation 593/2008 can also manifest by the language in which contractual information is presented to the consumer or the currency in which the contract is paid. However, this factor is only

[43] *Bundesverband* (2008), C-298/07, EU:C:2008:572, 16 October.

[44] See e.g. Dropbox. (2020) *Contact Dropbox Support*. [online] Dropbox. Available from: https://www.dropbox.com/support [Accessed 13 January 2020].

[45] *Hotel Alpenhof* (2010), C-585/08 and C-144/09, EU:C:2010:740, paragraphs 77, 91, and 94, 7 December.

[46] The list of language indicators is available as a switch at the bottom of the website, see Facebook. (2020) *Facebook*. [online] Facebook. Available from: https://www.facebook.com/ [Accessed 13 January 2020].

[47] The list of language indicators is available as a switch at the bottom of the website, see Microsoft. (2020) *Microsoft*. [online] Available from: https://onedrive.live.com/about/en-gb/ [Accessed 13 January 2020].

relevant if the language or the currency is different than the one usually used in the country where the professional is established.[48] The reservation does not undermine the usefulness of that factor for cloud computing contracts. To attract users, the providers often present the information on the website in the language used in the visitor's country. It is thus not uncommon to offer multiple translations. For example, the *Dropbox* website is available in 22 language versions,[49] the *Microsoft* – in 93,[50] while the *Facebook* – in 110.[51] Moreover, providers are usually established in countries where the official language is English (i.e. they focus their activities mainly in the USA, the UK and Ireland). Therefore, the presentation of contractual information in other languages used in the country where the consumer is domiciled may demonstrate the intention required under Article 6(1)(b) of Regulation 593/2008.

Furthermore, the law of the country of consumer's habitual residence may apply to the contract if the professional indicates that his or her customers compose of people domiciled in various countries, particularly if the professional presents accounts of such customers.[52] According to some scholars, this factor is often present in the case of cloud computing contracts.[53] In my opinion, however, the factor may not always be useful because not all providers emphasize concluding contracts with customers from different countries or collect their feedback. Nevertheless, at least some providers adopt such a business model (e.g. providers of social media or booking services). Therefore, the factor may offer valuable information as to whether the provider intended to enter into contracts with consumers domiciled in a specific country.

Finally, the *Court of Justice of the European Union* decided that the causal link between the presentation of information on the professional's website and the conclusion of the contract is not necessary for the application of Article 6(1)(b) of Regulation 593/2008.[54] The link may, however,

[48] *Hotel Alpenhof* (2010), C-585/08 and C-144/09, EU:C:2010:740, paragraph 84, 7 December.

[49] Dropbox. *Main page*. [online] Available from: https://www.dropbox.com [Accessed 13 January 2020].

[50] Microsoft. (2020) *Microsoft*. [online] Available from: https://onedrive.live.com/about/en-gb/ [Accessed 13 January 2020].

[51] Facebook. (2020) *Facebook*. [online] Facebook. Available from: https://www.facebook.com/ [Accessed 13 January 2020].

[52] *Hotel Alpenhof* (2010), C-585/08 and C-144/09, EU:C:2010:740, paragraph 83, 7 December.

[53] Haibach, G. (2015) Cloud computing and European Union private international law. *Journal of Private International Law*, 11 (2), p. 263.

[54] *Emrek* (2013), C-218/12, EU:C:2013:666, paragraphs 26 and 29, 17 October.

demonstrate that the professional envisaged doing business in the country where the consumer has his or her habitual residence. This comment may also apply to cloud computing contracts. However, the factor should not be overemphasized, because the causal link is often present in the case of these agreements. The consumer usually enters into cloud computing contracts by using electronic means of communications. In contrast, the consumer rarely concludes such contracts in other forms, particularly in writing.

4.4. NEGATIVE FACTORS

The *Court of Justice of the European Union* also formulated a list of factors that do not substantiate the application of Article 15(1)(c) of Regulation 44/2001. The list may also be used for Article 6(1)(b) of Regulation 593/2008. Consequently, it should be noted that mere access to the professional's website is insufficient to assume that the provider intended to do business in the country where the consumer is domiciled.[55] This includes "interactive" websites, i.e. pages which allow the parties to enter into a contract only by using electronic means of communication.[56] Similarly, the marketing of goods or services supplied over the Internet, as such, does not result in the application of Article 6(1)(b) of Regulation 593/2008.[57] These comments are relevant for cloud computing contracts which are not only concluded, but also perform using electronic means of communication, especially websites. Therefore, plain access to the website does manifest the provider's intention to direct the activities to the country where the consumer has his or her habitual residence.

Furthermore, mandatory information presented on the professional's website is also insufficient to determine his or her intention regarding doing business in the country of the consumer's domicile.[58] This factor is also important for cloud computing contracts. It should be noted that consumer protection in the *European Union* is based on the assumption that the consumer is the weaker party because he or she does not have the same information as the professional. Therefore, European law aims to eliminate the information asymmetry by imposing extensive information obligations on the professional. These obligations are particularly important in the case

[55] *Hotel Alpenhof* (2010), C-585/08 and C-144/09, EU:C:2010:740, paragraphs 74 and 94. See Recital 24 of Regulation 593/2008, 7 December.

[56] *Hotel Alpenhof* (2010), C-585/08 and C-144/09, EU:C:2010:740, paragraph 79, 7 December.

[57] *Hotel Alpenhof* (2010), C-585/08 and C-144/09, EU:C:2010:740, paragraph 73, 7 December.

[58] *Hotel Alpenhof* (2010), C-585/08 and C-144/09, EU:C:2010:740, paragraph 78, 7 December.

of cloud computing contracts which are subject not only to Directive 2000/31,[59] but also to Directive 2011/83[60] and soon – to Directive 2019/770.[61] As a result, it can be expected that the provider is required to present a considerable amount of information to the consumer. However, this information cannot be used as a decisive argument when determining the provider's intention regarding the country where the provider intended to do business.

5. CONCLUSION

The ubiquity of cloud computing facilitates entering into contracts with consumers from various countries. Consequently, the question of the law applicable to these agreements may often arise, especially if the contract is concluded between a consumer and a professional. The considerations presented in this article confirm that the current legal framework is sufficient for consumer protection. Contrary to concerns raised by some scholars, it can be assumed that the law of the country where the consumer is domiciled will often govern at least some obligations arising from cloud computing contracts. However, the application of Article 6 of Regulation 593/2008 may not always be free from doubts. In particular, the analysis indicates that the factors previously considered relevant may not offer valuable information about the provider's intention to enter into contracts with consumers domiciled in a specific country. Instead, other factors highlighted by the *Court of Justice of the European Union* may help clarify this issue. To determine the law applicable to cloud contracts concluded with consumers, the quality rather than the quantity of information presented by the provider should be taken into account. As a result, the intention of the provider to direct their professional activities to a specific Member

[59] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). *Official Journal of the European Communities* (2000/L-178/1), 17 July. Available from: http://data.europa.eu/eli/dir/2000/31/oj [Accessed 13 January 2020].

[60] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council. *Official Journal of the European Union* (2011/L-304/64), 22 November. Available from: http://data.europa.eu/eli/dir/2011/83/2018-07-01 [Accessed 13 January 2020].

[61] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services. *Official Journal of the European Union* (2019/L-136/1), 22 May. Available from: http://data.europa.eu/eli/dir/2019/770/oj [Accessed 13 January 2020].

State may be indicated in particular by a high level of detail of the information given to the consumer, the language of the information, methods of communication with the consumer or the name of the top-level domain.

LIST OF REFERENCES

[1] Andrews, C.D. and Newman, J.M. (2013) Personal Jurisdiction and Choice of Law in the Cloud. *Maryland Law Review*, 73

[2] Bogdan, M. (2011) Website Accessibility as Basis for Jurisdiction under the Brussels I Regulation. *Masaryk University Journal of Law and Technology*, 5 (1)

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

[4] *Brussels Convention on jurisdiction and the enforcement of judgments in civil and commercial matters*, 1968, (1972/L 299/32). Available from: https://curia.europa.eu/common/recdoc/convention/en/c-textes/brux.htm [Accessed 13 January 2020].

[5] Castro, C., Reed, Ch. and de Queiroz, R. (2013) On the Applicability of the Common European Sales Law to some Models of Cloud Computing Services. *European Journal of Law and Technology*, 4 (3). Available from: http://ejlt.org/article/view/186/409 [Accessed 13 January 2020].

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

[7] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts. *Official Journal of the European Communities* (1993/95-L-29), 21 April. Available from: http://data.europa.eu/eli/dir/1993/13/oj [Accessed 13 January 2020].

[8] Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. *Official Journal of the European Union* (2001/12-L/1), 16 January. Available from: http://data.europa.eu/eli/reg/2001/44/oj [Accessed 13 January 2020].

[9] De Filippi, P. and McCarthy, S. (2012) Cloud Computing: Centralization and Data Sovereignty. *European Journal of Law and Technology*, 3 (2). Available from: http://ejlt.org/article/view/101 [Accessed 13 January 2020].

[10] De Filippi, P. and Belli, L. (2012) Law of the Cloud v Law of the Land: Challenges and Opportunities for Innovation. *European Journal of Law and Technology*, 3 (2). Available from: http://ejlt.org/article/view/156 [Accessed 13 January 2020].

[11] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). *Official Journal of the European Communities* (2000/L-178/1), 17 July. Available from: http://data.europa.eu/eli/dir/2000/31/oj [Accessed 13 January 2020].

[12] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council. *Official Journal of the European Union* (2011/L-304/64), 22 November. Available from: http://data.europa.eu/eli/dir/2011/83/2018-07-01 [Accessed 13 January 2020].

[13] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services. *Official Journal of the European Union* (2019/L-136/1), 22 May. Available from: http://data.europa.eu/eli/dir/2019/770/oj [Accessed 13 January 2020].

[14] Dropbox. *Main page*. [online] Available from: https://www.dropbox.com [Accessed 13 January 2020].

[15] Dropbox. (2019) *Dropbox Terms of Service*. [online] Dropbox. Available from: https://www.dropbox.com/terms?view_en#terms [Accessed 13 January 2020].

[16] Dropbox. (2019) *Join Us Around the World*. [online] Available from: https://www.dropbox.com/jobs/locations [Accessed 13 January 2020].

[17] Dropbox. (2020) *Contact Dropbox Support*. [online] Dropbox. Available from: https://www.dropbox.com/support [Accessed 13 January 2020].

[18] Facebook. (2019) *Terms of Service*. [online] Facebook. Available from: https://www.facebook.com/legal/terms [Accessed 13 January 2020].

[19] Facebook. (2020) *Facebook*. [online] Facebook. Available from: https://www.facebook.com [Accessed 13 January 2020].

[20] Google. (2019) *Google Cloud Platform Terms of Service*. [online] Available from: https://cloud.google.com/terms/ [Accessed 13 January 2020].

[21] Haibach, G. (2015) Cloud computing and European Union private international law. *Journal of Private International Law*, 11 (2).

[22] Irion, K. (2015) Your Digital Home is No Longer Your Castle: How Cloud Computing Transforms the (Legal) Relationship Between Individuals and Their Personal Records. *International Journal of Law and Information Technology*, 23.

[23] Judgment of 16 October 2008, *Bundesverband*, C-298/07, EU:C:2008:572.

[24] Judgment of 14 May 2009, *Ilsinger*, C-180/06, EU:C:2009:303.

[25] Judgment of 7 December 2010, *Hotel Alpenhof*, C-585/08 and C-144/09, EU:C:2010:740.

[26] Judgment of 6 September 2012, C-190/11, *Mühlleitner*, EU:C:2012:542.

[27] Judgment of 14 March 2013, *Česká spořitelna*, C-419/11, EU:C:2013:165.

[28] Judgment of 17 October 2013, *Emrek*, C-218/12, EU:C:2013:666.

[29] Judgment of 28 January 2015, *Kolassa*, C-375/13, EU:C:2015:37.

[30] Judgment of 25 January 2018, *Schrems*, C-498/16, EU:C:2018:37.

[31] McGillivray, K. (2016) A Right Too Far? Requiring Cloud Service Providers to Deliver Adequate Data Security to Consumers. *International Journal of Law and Information Technology*, 25.

[32] Mell, P. and Grance, T. (2011) *The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology*. [online] Gaithersburg: National Institute of Standards and Technology. Available from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf [Accessed 13 January 2020].

[33] Microsoft. (2019) *Microsoft Cloud Agreements by Region and Language*. [online] Available from: https://docs.microsoft.com/en-us/partner-center/agreements [Accessed 13 January 2020].

[34] Microsoft. (2020) *Microsoft Office Locations Around the World*. [online] Available from: https://www.microsoft.com/en-us/worldwide.aspx [Accessed 13 January 2020].

[35] Microsoft. (2020) *Microsoft*. [online] Available from: https://onedrive.live.com/about/en-gb/ [Accessed 13 January 2020].

[36] Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I). *Official Journal of the European Union* (2008/177-L/6), 4 July. Available from: http://data.europa.eu/eli/reg/2008/593/oj [Accessed 13 January 2020].

[37] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast). *Official Journal of the European Union* (2012/351--L/1), 20 December. Available from: http://data.europa.eu/eli/reg/2012/1215/2015-02-26 [Accessed 13 January 2020].

[38] Rustad, M.L. and Onufario, M.V. (2012) Reconceptualizing Consumer Terms of Use for a Globalized Knowledge Economy. *University of Pennsylvania Journal of Business Law*, 14 (4).

[39] Spotify. (2019) *Spotify Terms and Conditions of Use*. [online] Available from: https://www.spotify.com/legal/end-user-agreement/ [Accessed 13 January 2020].

[40] Spotify. (2020) *About Us*. [online] Available from: https://www.spotify.com/about-us/contact/ [Accessed 13 January 2020].

[41] Wauters, E., Lievens, E. and Valcke, P. (2014) Towards a Better Protection of Social Media Users: a Legal Perspective on the Terms of Use of Social Networking Sites. *International Journal of Law and Information Technology*, 22.

DOI 10.5817/MUJLT2020-1-5

DOCUMENT SIMILARITY OF CZECH SUPREME COURT DECISIONS[*]

by

TEREZA NOVOTNÁ[**]

Retrieval of court decisions dealing with a similar legal matter is a prevalent task performed by lawyers as it is a part of a relevant decision-making practice review. In spite of the natural language processing methods that are currently available, this legal research is still mostly done through Boolean searches or by contextual retrieval. In this study, it is experimentally verified whether the doc2vec method together with cosine similarity, can automatically retrieve the Czech Supreme Court decisions dealing with a similar legal issue as a given decision. Furthermore, the limits and challenges of these methods and its application on the Czech Supreme Court decisions are discussed.

KEY WORDS

Automatic Court Decisions Processing, Cosine Similarity, Czech Supreme Court, Document Semantic Similarity, Doc2Vec

1. INTRODUCTION AND MOTIVATION

Although the Czech legal system belongs to continental legal systems based on the statutes and regulations, the role of the top-tier court's decisions is significant. This role is continuously theoretically examined by legal scholars and academics in order to find its position in the common law and continental law spectrum.[1] There is a consensus among the Czech legal professional public that judicial decisions are not generally binding as they

[*] Author gratefully acknowledges the institutional support of *Masaryk University*.

[**] tereza.novotna@mail.muni.cz, Ph.D. candidate at the Institute of Law and Technology, Masaryk University in Brno, The Czech Republic.

[1] See: MacCormick, N., Summers, R. S. (1997) *Interpreting Precedents. A Comparative Study*. Dartmouth: Aldeshot; Smejkalová, T. (2019) Judikatura, nebo precedens? *Právník. Teoretický časopis pro otázky státu a práva*, 158 (9), pp. 852–864.

are in the common law systems.[2] As nowadays we see the binding effect of the decisions more as a spectrum then a binary option[3], the question is where in this spectrum Czech top-tier court decisions lie. Therefore, there are several characteristics to be taken into account when it comes to the binding effect of the highest court decisions in the Czech Republic. One of the attributes of the role of court decisions of *Supreme*, *Supreme Administrative*, and *Constitutional Court* is the consistency of decision--making practice. The decision-making practice should be predictable and repetitive in order to fulfil the conditions of the principle of legal certainty.

In spite of the fact that the reality is usually more complicated, the analysis of previous decision-making practice in the similar matter is still a significant part of work of every judge, lawyer, legal scholar or student. Furthermore, the analysis of court decisions takes a great part in the academic journals, scientific publications, students' books or different kinds of commentaries. In the Czech legal society, whole journals are dedicated to overview current court decisions[4], other journals have special sections for the overview and annotations of current decisions[5], famous legal focused accounts on social media provide actualities from the current decision-making practice of individual courts,[6] or generally used commercial systems provide the newest decisions in special sections.

The *Czech Supreme Court* publishes approximately between 5 and 7 thousands of decisions per year, and this number is continuously increasing (see Figure 1).[7]

[2] Different legal scholars come up with different approaches to tackle the binding effect of decisions. See for example: Harvánek, J. et al. (2008) *Teorie práva*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, p. 261; Gerloch, A. (2017) *Teorie práva*. 7th ed. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, p. 90; Kubů, L., Hungr P. and Osina P. (2007) *Teorie práva*. Praha: Linde, p. 56; Bobek, M. et al. (2013) *Judikatura a právní argumentace*. 2nd ed. Praha: Auditorium, pp. 112, 113, 117, 118.

[3] The idea of the spectrum was formulated in: Peczenik, A. (1997) The Binding Force of Precedent. In: MacCormick, N., Summers, R. S. (eds.). *Interpreting Precedents. A Comparative Study*. Dartmouth: Aldeshot, pp. 461–479.

[4] For example Czech journal *Soudní rozhledy* from *C. H. Beck*.

[5] For example Czech journal *Revue pro právo a technologie* contains special section "Aktuální judikatura" dealing with recently published court decisions.

[6] For example Czech *Facebook* account *Iuridum daily* or Czech TV series *Týden v justici*.

[7] Data statistics of the *Supreme Court* decisions contained in the *Czech Court Decisions Corpus*. See: Novotná, T. and Harašta, J. (2019) *The Czech Court Decisions Corpus (CzCDC): Availability as the First Step*. ArXiv:1910.09513. [online] Available from: http://arxiv.org/abs/1910.09513 [Accessed 20 January 2020].

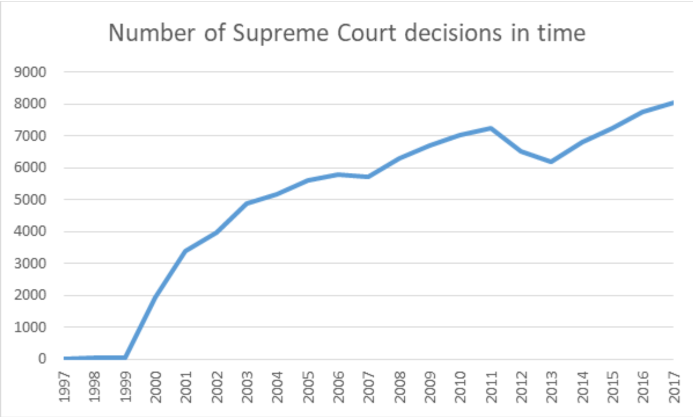

Figure 1: The time evolution of the number of Supreme Court decisions

The *Supreme Court* has a whole department just for analysis of its decisions. The employees of the *Supreme Court* are manually reading through the decisions and classifying them in order to create different kinds of collections with decisions related to different codes and articles, different keywords and topics etc. These collections then serve for better orientation in the court decisions for the judges and assistants. The manual processing of texts of court decisions is time-consuming and subjectively affected.

In this study, I choose a natural language processing (hereby *"NLP"*) method *doc2vec*[8] to automatically process the *Supreme Court* decisions and *cosine similarity* measure to compute the similarity value of the decisions[9]. *NLP* is a computer science and linguistic field dedicated to automatically process natural language in order to perform different tasks. These tasks lead in particular to better information retrieval. Different methods and different approaches are used to obtain more and more accurate and efficient results from the information retrieval systems. *NLP* methods are recently mainly based on machine learning methods and language statistics. The most common tasks in legal language processing are segmentation of legal texts[10], its summarization[11], extraction of different parts of legal texts (citations, entities etc.)[12], extraction of topics or keywords[13] and semantic similarity counting[14], just to name a few.

[8] This method was introduced in: Le, Q. and Mikolov, T. (2014) Distributed representations of sentences and documents. In: *Proceedings of the 31st International Conference on Machine Learning (ICML 2014)*, Beijing, China, pp. 1188–1196.

[9] Gomaa, W. H. and Fahmy, A. A. (2013) A survey of text similarity approaches. *International Journal of Computer Applications*, 68 (13), pp. 13–18.

I apply the methods in order to experimentally answer the following hypothesis: the court decisions with a high *cosine similarity* of their *doc2vec* representations are dealing with the qualitatively similar legal issue. The hypothesis is created on the hypothetical situation where a lawyer disposes of one decision in a specific matter. She wants to obtain the *Supreme Court* decisions in a similar matter to help her to build an argumentation in her pending case. That is a standard task that every lawyer needs to perform – to review recent decision-making practice in order to choose the right strategy in a legal case. The hypothesis is based on the previous work in the similarity of the legal documents, and specifics of the Czech language described in Section 2.[15] The methodology and the data is described in Section 3. The result of this experiment and its general evaluation is in Section 4. The limits of the method, possible development and improvement as well as future work are described in Section 5. Section 6 is concluding the study with a short summarization.

2. RELATED WORK

The *doc2vec* method is based on the *word2vec* method that was originally proposed by *Mikolov et al.*[16] The *doc2vec* was proposed by *Mikolov and Le* as an extension of *word2vec* using the neural vector embedding for

[10] For example: Savelka, J. and Ashley, K. D. (2018) Segmenting U.S. Court Decisions into Functional and Issue Specific Parts. In: Palmirani, M. (ed.). *Legal Knowledge and Information Systems JURIX 2018*. IOS Press Ebooks, pp. 111–120. Available from: http://ebooks.iospress.nl/volume/legal-knowledge-and-information-systems-jurix-2018-the-thirty-first-annual-conference [Accessed 20 January 2020]; Harašta, J. et al. (2019) Automatic Segmentation of Czech Court Decision into Multi-Paragraph Parts. *Jusletter IT*, 23 May 2019, pp. 1–11.

[11] For example: Barzilay, R. and Elhadad, M. (1997) Using Lexical chains for Text Summarization. In: *Proceedings of the ACL Workshop on Intelligent Scalable Text Summarization*, pp. 10–17. Hearst, M. A. (1997) TextTiling: Segmenting Text into Multi-paragraph Subtopic Passages. *Computational Linguistics*, 23 (1), pp. 33–64.

[12] For example: Harašta, J. et al. (2018) Annotated Corpus of Czech Case Law for Reference Recognition Tasks. In: *Text, Speech, and Dialogue: 21st International Conference proceeding*, pp. 239–250; Kríž, V. et al. (2014) Statistical Recognition of References in Czech Court Decisions. In: *Proceedings of MICAI*, pp. 51–61.

[13] For example: Ercan, G. and Cicekli, I. (2007) Using Lexical Chains for Keyword Extraction. *Information Processing & Management*, 43 (6), pp. 1705–1714.

[14] For example: Hearst, M. A. (1997) TextTiling: Segmenting Text into Multi-paragraph Subtopic Passages. *Computational Linguistics*, 23 (1), pp. 33–64; Wagh, R. and Anand, D. (2017) Application of citation network analysis for improved similarity index estimation of legal case documents: A study. In: *2017 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC)*, pp. 1–5. Available from: doi:10.1109/ICCTAC.2017.8249996 [Accessed 20 January 2020].

[15] See notes 31–33.

[16] Mikolov, T. et al. (2013) Efficient estimation of word representations in vector space. In: *Proceedings of Workshop at the International Conference on Learning Representations*, Scottsdale, USA.

the whole documents (sentences, paragraphs etc.).[17] Original *word2vec* method is based on the principle, where the text is split into unique words and these words are embedded with a vector representation. Vectors emerge from the large text corpora training models in a way where the model predicts the current word from the word neighborhood (the words that the current word is often surrounded). The output of this method is a vector space model where the semantically similar words are embedded with similar vector representations.[18] The *doc2vec* is a subsequent work based on the same principles. This method is generally applicable to the text segments of any length – from sentences to whole documents. The methodology is very similar to the *word2vec*, except entire segments (referred as "paragraphs" in the original paper[19]) are embedded with a vector representation as well as unique words in the text. Furthermore, the prediction of a current word is based on both segment and word vectors. In this way, it is possible to capture the semantic context of the text segments.[20]

There is a large number of applications of this method in different fields, including legal text analysis. The empirical work proving the highest efficiency of the *doc2vec* is the one from *Lau and Baldwin*, where the authors compare the method to other embedding-based methods.[21]

The *doc2vec* is used to classify different types of documents. *Trieu, Tran and Tran* used this method to classify *Twitter* news according to their topics (or labels).[22] These news-based documents were transformed into vectors using the *doc2vec* method. The label for a current document is chosen according to the vector similarity of other document vectors in the pre-

[17] Le, Q. and Mikolov, T. (2014) Distributed representations of sentences and documents. In: *Proceedings of the 31st International Conference on Machine Learning (ICML 2014)*, Beijing, China, pp. 1188–1196.

[18] This method was proposed with the use of two possible architectures: continuous bag-of--words and skip-gram, where in the skip-gram the word *neighborhood* is predicted based on the current word. Furthermore, the continuous bag-of-words respect word orders. For more detailed information see: Mikolov, T. et al. (2013) Efficient estimation of word representations in vector space. In: *Proceedings of Workshop at the International Conference on Learning Representations*, Scottsdale, USA.

[19] Detailed information about the *doc2vec* in: Le, Q. and Mikolov, T. (2014) Distributed representations of sentences and documents. In: *Proceedings of the 31st International Conference on Machine Learning (ICML 2014)*, Beijing, China, pp. 1188–1196.

[20] Ibid.

[21] Lau, J. H. and Baldwin, T. (2016) An Empirical Evaluation of doc2vec with Practical Insights into Document Embedding Generation. In: *Proceedings of the 1st Workshop on Representation Learning for NLP*, Berlin: Association for Computational Linguistics, pp. 78–86. Available from: https://www.aclweb.org/anthology/W16-1609.pdf [Accessed 20 January 2020].

-trained model. Sentiment analysis, as *Bilgin and Şentürk* suggest in their study, is another use of the *doc2vec*.[23]

Sentiment analysis is an analysis of emotions contained in the text. Authors successfully used *doc2vec* on the *Twitter*-based text corpus in order to define the specific product feedbacks as positive, negative or neutral. The opinion mining[24] is a method close to the semantic analysis retrieving public opinion on the specific matter. As such, this method is widely used for social media analysis. The study from *Maslova and Potapov* proves the usability for flexional languages as well (authors use Russian texts).

Recommendation of similarly focused new texts is the last example to show the possible use of *doc2vec*. In the comparative empirical study performed on the news texts, *Nandi et al.* showed that this method outperforms other widely used *NLP* methods, such as *Latent semantic analysis* and *Latent Dirichlet allocation*.[25] This study shows that the recommendation model based on *doc2vec* retrieved more contextually similar news to the original text than the two other compared methods.

All of the above-suggested uses of *doc2vec* are performed to the relatively short texts. In the legal domain, the documents are mostly longer than tweets or news articles. Despite that, successful studies applying *doc2vec* to longer legal documents were published. Firstly, the *doc2vec* can be used to determine and merge controversial issues in the case law.[26] In the *Tian*

[22] Trieu, L. Q., Tran, H. Q. and Tran, M.-T. (2017) News Classification from Social Media Using Twitter-based Doc2Vec Model and Automatic Query Expansion. In: *Proceedings of the Eighth International Symposium on Information and Communication Technology*. Nha Trang City, Viet Nam: Association for Computing Machinery, pp. 460–467. Available from: doi:10.1145/3155133.3155206 [Accessed 20 January 2020]; Kim, D. et al. (2019) Multi-co-training for document classification using various document representations: TF–IDF, LDA, and Doc2Vec. In: *Information Sciences*, 477, pp. 15–29. Available from: doi:10.1016/j.ins.2018.10.006 [Accessed 20 January 2020].

[23] Bilgin, M. and Şentürk, I. F. (2017) Sentiment analysis on Twitter data with semi-supervised Doc2Vec. In: *2017 International Conference on Computer Science and Engineering (UBMK)*, pp. 661–666. Available from: doi:10.1109/UBMK.2017.8093492 [Accessed 20 January 2020].

[24] Maslova, N. a Potapov, V. (2017) Neural Network Doc2vec in Automated Sentiment Analysis for Short Informal Texts. In: Karpov, A. et al. (eds.). *Speech and Computer*. Cham: Springer International Publishing, pp. 546–554. Lecture Notes in Computer Science. Available from: doi:10.1007/978-3-319-66429-3_54 [Accessed 20 January 2020].

[25] Nandi, N. R. et al. (2018) Bangla News Recommendation Using doc2vec. In: *2018 International Conference on Bangla Speech and Language Processing (ICBSLP)*, pp. 1–5. Available from: doi:10.1109/ICBSLP.2018.8554679 [Accessed 20 January 2020].

[26] Tian, X. et al. (2018) K-Means Clustering for Controversial Issues Merging in Chinese Legal Texts. In: Palmirani, M. (ed.). *Legal Knowledge and Information Systems JURIX 2018*. IOS Press Ebooks, pp. 215–219. Available from: http://ebooks.iospress.nl/volume/legal-knowledge-and-information-systems-jurix-2018-the-thirty-first-annual-conference [Accessed 20 January 2020].

et al. published paper, the causes of action are analyzed in order to define the controversial issue in them.

Alternatively, counting the similarity of the legal document combined with *cosine similarity* measure or retrieval of similar court decisions are common tasks to apply *doc2vec* to the legal documents. *Renjit and Idicula* applied *doc2vec* to both statutes and precedents in order to obtain the most similar to the in-hand legal document.[27] *Barco Ranera, Solano and Oco* achieved high accuracy of semantically similar court decisions retrieved using *doc2vec* model comparing to the expert evaluation.[28] A comparison of several legal court decision retrieval methods from *Mandal et al.* showed that *doc2vec* outperformed other well knows methods for legal text analysis.[29] The *cosine similarity* was compared to the network analysis in the work from *Wagh and Anand* in combination with different vector--based *NLP* method. In this study, citation network analysis had more accurate results than the *cosine similarity* of document vectors.[30]

However, there are not many studies in legal analysis field using vector embedding for the Czech language. *Novotný and Ircing* compared *doc2vec* method application on English dataset and two Czech datasets to state the high efficiency in the classification tasks even for Czech texts.[31] *Kocmi* used document embedding for machine translation in his dissertation.[32]

Additionally, there is general unavailability of the Czech legal texts corpora. In this experiment, the recently published *Czech Court Decisions*

[27] Renjit, S. and Idicula, S. M. (2019) CUSAT NLP@AILA-FIRE2019: Similarity in Legal Texts using Document Level Embeddings. In: Bhattacharya, P. et al. *Overview of the FIRE 2019 AILA track: Artificial Intelligence for Legal Assistance*. Proc. Of FIRE, pp. 12–15.

[28] Ranera, L. T. B., Solano, G. A., and Oco, N. (2019) Retrieval of Semantically Similar Philippine Supreme Court Case Decisions using Doc2Vec. In: *2019 International Symposium on Multimedia and Communication Technology (ISMAC)*. IEEE, pp. 1–6; Mandal, A. et al. (2017) Measuring similarity among legal court case documents. In: *Proceedings of the 10th Annual ACM India Compute Conference*, pp. 1–9.

[29] Mandal, A. et al. (2017) Measuring similarity among legal court case documents. In: *Proceedings of the 10th Annual ACM India Compute Conference*, pp. 1–9.

[30] Wagh, R. and Anand, D. (2017) Application of citation network analysis for improved similarity index estimation of legal case documents: A study. In: *2017 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC)*, pp. 1–5. Available from: doi:10.1109/ICCTAC.2017.8249996 [Accessed 20 January 2020].

[31] Novotný, J. and Ircing, P. (2018) The Benefit of Document Embedding in Unsupervised Document Classification. In: Karpov, A. et al. (eds.). *Speech and Computer*. Cham: Springer International Publishing, pp. 470–478. Lecture Notes in Computer Science. Available from: doi:10.1007/978-3-319-99579-3_49 [Accessed 20 January 2020].

[32] Kocmi, T. (2020) Exploring Benefits of Transfer Learning in Neural Machine Translation. [pre-print] Available from: https://arxiv.org/abs/2001.01622 [Accessed 20 January 2020].

Corpus was used as a source dataset of the decisions of the *Czech Supreme Court*.[33] The dataset is further described in Section 3.

3. METHODOLOGY

The *NLP* method to count the semantic similarity was chosen having regard to the nature of the documents. The *doc2vec* is a generally applicable method based on *word2vec* method transforming whole documents into vectors while building vector space model. There are several reasons why this method was chosen. First of all, *doc2vec* outperforms other vector space model methods.[34] Secondly, this method can capture the semantics of the texts because it respects the order of words.[35] Furthermore, as it was described, it can be used to the documents of different lengths.[36] Another reason is that *doc2vec* generally does not require a lemmatization step (as it will be discussed below),[37] which is very time saving considering the corpus size. Finally, *doc2vec* is easily applicable through further described python-based libraries.

The *doc2vec* method was applied to the whole dataset of the *Supreme Court* decisions available in the *Czech Court Decisions Corpus 1.0*. It was proven that this algorithm performs better for large corpora of texts[38], such as the whole corpus of *Supreme Court* decisions published which was used.

3.1. DATA

Publicly available *Czech Court Decisions Corpus 1.0* was used to build a vector space model. This dataset contains plain texts of decisions of the *Supreme Court* published between 1st January 1993 and 30th September 2018. The dataset consists of 111,977 decisions in total. According

[33] Novotná, T. and Harašta, J. (2019) *The Czech Court Decisions Corpus (CzCDC): Availability as the First Step*. ArXiv:1910.09513. [online] Available from: http://arxiv.org/abs/1910.09513 [Accessed 20 January 2020].

[34] See note 25 or 29.

[35] Le, Q. and Mikolov, T. (2014) Distributed representations of sentences and documents. In: *Proceedings of the 31st International Conference on Machine Learning (ICML 2014)*, Beijing, China, pp. 1188–1196.

[36] *Czech Supreme Court* decisions vary in length from half-page documents to several pages length decisions.

[37] Hrala, M. and Král, P. (2013) Evaluation of the Document Classification Approaches. In: Burdul, R. et al. (eds.). *Proceedings of the 8th International Conference on Computer Recognition Systems CORES 2013*. Heidelberg: Springer International Publishing, pp. 877–885. Advances in Intelligent Systems and Computing. Available from: doi:10.1007/978-3-319-00969-8_86 [Accessed 20 January 2020].

[38] Mikolov, T. et al. (2013) Efficient estimation of word representations in vector space. In: *Proceedings of Workshop at the International Conference on Learning Representations*, Scottsdale, USA.

to the accompanying description, it contains approximately 91 % of all decisions of the *Supreme Court* issued within the relevant time range. These decisions are already anonymized and contain all the parts of the decisions, including the metadata heading. The heading is contained since the decisions were downloaded from the court website. The texts of the decisions are in Czech language and unstructured.

Several steps of data preprocessing must have been performed in order to build a vector space model and to process the decisions. First of all, the texts where tokenized. Tokenization means splitting the texts into predefined tokens. In this case, words were used as tokens. The second step was punctuation removal. Further off, lemmatization of tokens is a usual following step.[39] The lemmatization is a transformation of the words (as tokens) into their "lemmas". The lemma is the dictionary form of a word in the languages where a word can take different forms. This step is desirable when processing inflected languages such as the Czech language. In this particular case, using lemmatization was considered but not used in the final training model. According to the relevant literature, the lemmatization of texts does not generally improve the performance of the *doc2Vec* method.[40] As the required time when lemmatizing the model increases significantly and better performance is not expected, the lemmatization was not used in this particular case.

The last preprocessing step was the stop words removal. Stop words are words in the natural text that do not bear any meaning from the perspective of semantics, and those words are usually prepositions, conjunctions etc. Removing these words can help to increase the accuracy of text transformation, although the question of whether to remove stop words is uncertain. This is because since the vector space model is based on the statistical appearance of unique words, removing common words without a specific meaning helps to highlight other, meaningful words. For

[39] See for example: Schweighofer, E., Winiwarter, W. and Merkl, D. (1995) Information filtering: the computation of similarities in large corpora of legal texts. In: *Proceedings of the 5th international conference on Artificial intelligence and law*, p. 119–126; Kannan, Subbu and Gurusamy, V. (2014) Preprocessing techniques for text mining. *International Journal of Computer Science & Communication Networks*, 5 (1), pp. 7–16.

[40] Hrala, M. and Král, P. (2013) Evaluation of the Document Classification Approaches. In: Burdul, R. et al. (eds.). *Proceedings of the 8th International Conference on Computer Recognition Systems CORES 2013*. Heidelberg: Springer International Publishing, pp. 877–885. Advances in Intelligent Systems and Computing. Available from: doi:10.1007/978-3-319-00969-8_86 [Accessed 20 January 2020].

this task, I used the general list of Czech stop words available for the *Python* libraries.[41]

Unique tasks described above are the standard preprocessing steps for many *NLP* techniques and methods.[42] It is obvious that after this process, the texts are represented rather as sets of single words (tokens), which is desirable input for many different methods of the *NLP*.

3.2. TRAINING VECTOR SPACE MODEL

The sets of words are then transformed into vectors using the *doc2vec* method. This method is based on the *word2vec* method based on machine learning. Both documents and words are represented as vectors of the dimension of N, this dimension (or length) are chosen arbitrarily according to the length of documents that are transformed. The principle of this method is a prediction of the current word according to its context (word surrounding).[43] This way, the words that usually appear in the same context (close to each other) have similar vector embeddings (such as "Supreme Court"). Creation of these vectors is taking place in the training phase of the process. The algorithm goes through all the words in many repetitions and gradually refines vector representations of unique words.

The training is based on several parameters such as the length of the vectors, the number of epochs, which is the number of iterations during the training, or the statistical limits of words that are ignored during the training. These limits are based on the prediction that words appearing in the text less than the limit do not bear any vital information about the text. Although this is a relative statistical prediction, in the case of court decisions, it is applicable, since we are looking for the common words among the individual documents. When the parameters are set, the model is trained. The training time of a model of 111,977 *Supreme Court* decisions is approximately 30 hours. Parameters can be reset, and the model can be trained again to achieve better performance of the model when the results

[41] This *Python* library is available from: https://pypi.org/project/stop-words/

[42] See for example: Schweighofer, E., Winiwarter, W. and Merkl, D. (1995) Information filtering: the computation of similarities in large corpora of legal texts. In: *Proceedings of the 5th international conference on Artificial intelligence and law*, p. 119–126; Kannan, Subbu and Gurusamy, V. (2014) Preprocessing techniques for text mining. *International Journal of Computer Science & Communication Networks*, 5 (1), pp. 7–16.

[43] In the case contiuous bag-of-words algorithm is used. If skip-gram is used, then the surrounding is predicted on the base of a current word.

are unsatisfying. This is very time-consuming since every new training takes approximately the same number of hours. Once the model is successfully trained, it can be stored and used repeatedly.

3.3. COSINE SIMILARITY OF DOCUMENTS

Cosine similarity of vectors is a common method for computing semantic similarity of different text parts. It counts the *cosine value* of an angle between two vectors as two documents.[44]

In this case, I trained a vector space model consisting of vector representations of the decisions from the dataset of the *Supreme Court* decisions. To prove or disprove the initial hypothesis, I use the evaluation based on a comparison of the one decision that a lawyer possesses in the beginning, as it was set in Section 1. This decision is pre-processed in the same way as the decisions contained in the model, and then it is transformed into a vector. This vector is compared to the trained model, and the *cosine similarity* is computed in order to obtain the most similar vectors out of the training dataset. Using this methodology, I was able to obtain the list of most semantically similar decisions relatively fast.

There is a second way of how to count the similarity among the documents. Within this method, after the model training, every vector is compared to every other. This method is very time-consuming and very demanding as regards computational capacity. On the other hand, it can provide more information on the semantic similarity among the whole dataset of documents. This approach is desirable when building a network for the network or cluster analysis.

3.4. TASK DEFINITION

For the evaluation of the method and proving the hypothesis, let us consider the situation from the Section 1 as a legal information retrieval query. Let us assume that a lawyer has a *Supreme Court* decision, *26 Cdo 1471/2013*, dealing mainly with the lease agreement and its validity. She wants to obtain more *Supreme Court* decisions dealing with the same matter – the lease agreement. Therefore, according to the methodology and

[44] Gomaa, W. H. and Fahmy, A. A. (2013) A survey of text similarity approaches. *International Journal of Computer Applications*, 68 (13), pp. 13–18; Wagh, R. and Anand, D. (2017) Application of citation network analysis for improved similarity index estimation of legal case documents: A study. In: *2017 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC)*, pp. 1–5. Available from: doi:10.1109/ICCTAC.2017.8249996 [Accessed 20 January 2020].

the process described in Section 3, we compare the decision *26 Cdo 1471/2013* to the vector space model. As a result, a set of 10 most semantically similar decisions is retrieved. The number of the most similar decision is chosen mostly arbitrarily regarding the scope of this article. This number can vary according to the needs of the hypothetical lawyer from the example situation.

4. RESULTS

The list of 10 the most semantically similar decisions and their *cosine similarity* values are in Table 1.

The evaluation methodology is a qualitative analysis of retrieved decisions and its comparison from the legal point of view. Retrieved decisions were manually analyzed in order to extract the most important legal issue. These issues are in the third column of Table 1. It was observed whether the clue legal issue is thematically related to the original decision concerning the validity of a lease agreement. The *cosine similarity* value between the vector representations of a certain decision and the original decision is in the second column of Table 1.

Docket number	**Similarity value**	**Legal Issue**
20 Cdo 1003/2000	0.5084	The implicitly concluded lease agreement
26 Cdo 1143/2004	0.4667	The transition of lease of an apartment, evidence
26 Cdo 761/2003	0.4655	The termination of the lease
26 Cdo 1136/2003	0.4617	The termination of the lease
26 Cdo 567/2009	0.4611	The validity of lease agreement
33 Cdo 2593/2015	0.4605	The termination of the lease
26 Cdo 4331/2011	0.4576	Procedural decision – dismissal
26 Cdo 4801/2016	0.4572	The validity of lease agreement
26 Cdo 4898/2008	0.4536	The conclusion of lease agreement

Table 1: The most similar decisions retrieved from the model

The *doc2vec* model retrieved the 10 most semantically similar decisions to the original decision in a hierarchical order. All of the decisions are decisions arising from a civil procedure. We can observe that 8 out of the 10 decisions were decided by the same senate. Generally, senates of the *Supreme Court* are divided according to the specific matters they deal with. Furthermore, 9 of these are dealing with relatively close topics – it is either the validity of the lease agreement itself or its conclusion, termination or transition. The question of the validity of an agreement is strongly related mainly to the question of concluding or termination of the agreement.

However, there is also a procedural dismissal – *26 Cdo 4331/2011*. This decision is very short, only a few sentences and the heading. When taking a deeper look, one can discover that the problematic issue here is the heading. The heading is very similar to the heading of the original decision; these decisions are decided by the same judges, which means that the heading contains a number of identical words. As the decision is very short, the heading forms a great part of the whole text of the decision. This uncovers one of the limits of the *doc2Vec* method, that is further discussed in following section. This method does not perform very well when combining relatively long and short texts as in this example. This is due to the fact that the dimension of word and paragraph vectors is the same for every word and document not regarding the length difference of unique documents.

Generally, it can be concluded that the hypothesis was proved – it can be stated that the semantically similar decisions are dealing with similar legal issues. However, this method has certainly many limits, and the evaluation is further discussed in Section 5.

5. DISCUSSION AND FUTURE WORK

There are a few issues to be discussed concerning mainly the method and its limits, but also data and its preprocessing and the evaluation of the experiment.

The data preprocessing part is mostly straightforward and standardized, although there are some questions to be addressed. The first is the list of stop words. The general list used in this study contains natural language Czech stop words. As the legal language is very specific from the natural one, this list could be extended with legal words bearing no important meaning. Words as court, procedure, civil etc. are words frequently appearing in the resulted decisions, although they are very general with no specific meaning for the context. For this task to be performed transparently, I suggest using a statistical density of unique words in the dataset of *Supreme Court* decisions and removing those generally most common.

To avoid the mistake of receiving the procedural dismissal not relevant to the legal information retrieval query, the document segmentation task and removal of some parts of the texts would be suitable. It is upon further discussion what parts of decisions are relevant for this specific method, however facts or argumentation parts usually bear the most important information about the case, on the contrary, the heading or even the metadata heading should be removed.

Regarding the method itself and the vector space model training, different parameters can be set to refine the results. At this point, the length of the vectors and the limits for word occurrences should be emphasized. The limits are closely related to the stop words and potentially could be stressed within the word density analysis .

The discussion on the limits of the *doc2vec* method highlights the fact that this method performed worse on the set of long texts. This issue could be partly solved with document segmentation, although the argumentation part is usually the longest one in the court decision. Therefore, I do not expect a significant improvement in this regard.

The evaluation is the last issue discussed in this Section. Although the results are transparent, the limits of qualitative analysis do not allow for comparison with different studies with a similar topic. For the experiment to be comparable, information retrieval measures such as precision and recall should be computed. For the qualitative evaluation itself, the evaluation group rather than only one evaluator should be considered, and the relevant assessment should be involved.

6. CONCLUSION

In this experimental study, I used the *doc2vec* method to count semantic similarity of the *Czech Supreme Court* decisions to prove the hypothesis that decisions with high semantic similarity deal with a similar legal issue.

I used a whole dataset of the *Supreme Court* decisions from the *Czech Court Decisions Corpus 1.0* to build a training vector space model, that was used afterwards to compute the *cosine similarity* between the decisions. I used the pre-selected *Supreme Court* decision as a test one to retrieve decisions most similar to it out of the dataset, and I qualitatively analyzed the legal issue concerned in the decisions to evaluate the method. Finally, I stated that 9 out of 10 retrieved decisions dealt with a similar legal issue, and I considered the hypothesis proven. The retrieved documents dealt mainly with conclusion or termination of a rent agreement taken into account that the initial decision dealt with the validity of the rent agreement. From a legal point of view, these questions are related.

The *doc2vec*, as well as data preprocessing and evaluation method, have their limits that influence the performance of the method. These limits were discussed further, and possible improvements were suggested.

LIST OF REFERENCES

[1] Barzilay, R. and Elhadad, M. (1997) Using Lexical chains for Text Summarization. In: *Proceedings of the ACL Workshop on Intelligent Scalable Text Summarization*, pp. 10–17.

[2] Bilgin, M. and Şentürk, I. F. (2017) Sentiment analysis on Twitter data with semi--supervised Doc2Vec. In: *2017 International Conference on Computer Science and Engineering (UBMK)*, pp. 661–666. Available from: doi:10.1109/UBMK.2017.8093492 [Accessed 20 January 2020].

[3] Bobek, M. et al. (2013) *Judikatura a právní argumentace*. 2nd ed. Praha: Auditorium.

[4] Ercan, G. and Cicekli, I. (2007) Using Lexical Chains for Keyword Extraction. *Information Processing & Management*, 43 (6), pp. 1705–1714.

[5] Gerloch, A. (2017) *Teorie práva*. 7th ed. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk.

[6] Gomaa, W. H. and Fahmy, A. A. (2013) A survey of text similarity approaches. *International Journal of Computer Applications*, 68 (13), pp. 13–18.

[7] Harašta, J. et al. (2018) Annotated Corpus of Czech Case Law for Reference Recognition Tasks. In: *Text, Speech, and Dialogue: 21st International Conference proceeding*, pp. 239–250.

[8] Harašta, J. et al. (2019) Automatic Segmentation of Czech Court Decision into Multi--Paragraph Parts. *Jusletter IT,* 23 May 2019, pp. 1–11.

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

[10] Hearst, M. A. (1997) TextTiling: Segmenting Text into Multi-paragraph Subtopic Passages. *Computational Linguistics*, 23 (1), pp. 33–64.

[11] Hrala, M. and Král, P. (2013) Evaluation of the Document Classification Approaches. In: Burdul, R. et al. (eds.). *Proceedings of the 8th International Conference on Computer Recognition Systems CORES 2013*. Heidelberg: Springer International Publishing, pp. 877–885. Advances in Intelligent Systems and Computing. Available from: doi:10.1007/978-3-319-00969-8_86 [Accessed 20 January 2020].

[12] Kannan, Subbu and Gurusamy, V. (2014) Preprocessing techniques for text mining. *International Journal of Computer Science & Communication Networks*, 5 (1), pp. 7–16.

[13] Kim, D. et al. (2019) Multi-co-training for document classification using various document representations: TF–IDF, LDA, and Doc2Vec. In: *Information Sciences*. 477, pp. 15–29. Available from: doi:10.1016/j.ins.2018.10.006 [Accessed 20 January 2020].

[14] Kocmi, T. (2020) *Exploring Benefits of Transfer Learning in Neural Machine Translation*. [preprint] Available from: https://arxiv.org/abs/2001.01622 [Accessed 20 January 2020].

[15] Kríž, V. et al. (2014) Statistical Recognition of References in Czech Court Decisions. In: *Proceedings of MICAI*, pp. 51–61.

[16] Kubů, L., Hungr, P. and Osina, P. (2007) *Teorie práva*. Praha: Linde.

[17] Lau, J. H. and Baldwin, T. (2016) An Empirical Evaluation of doc2vec with Practical Insights into Document Embedding Generation. In: *Proceedings of the 1st Workshop on Representation Learning for NLP*, Berlin: Association for Computational Linguistics, pp. 78–86. Available from: https://www.aclweb.org/anthology/W16-1609.pdf [Accessed 20 January 2020].

[18] Le, Q. and Mikolov, T. (2014) Distributed representations of sentences and documents. In: *Proceedings of the 31st International Conference on Machine Learning (ICML 2014)*, Beijing, China, pp. 1188–1196.

[19] MacCormick, N. and Summers, R. S. (1997) *Interpreting Precedents. A Comparative Study*. Dartmouth: Aldeshot.

[20] Mandal, A. et al. (2017) Measuring similarity among legal court case documents. In: *Proceedings of the 10th Annual ACM India Compute Conference*, pp. 1–9.

[21] Maslova, N. and Potapov, V. (2017) Neural Network Doc2vec in Automated Sentiment Analysis for Short Informal Texts. In: Karpov, A. et al. (eds.). *Speech and Computer*. Cham: Springer International Publishing, pp. 546–554. Lecture Notes in Computer Science. Available from: doi:10.1007/978-3-319-66429-3_54 [Accessed 20 January 2020].

[22] Mikolov, T. et al. (2013) Efficient estimation of word representations in vector space. In: *Proceedings of Workshop at the International Conference on Learning Representations*. Scottsdale, USA.

[23] Nandi, N. R. et al. (2018) Bangla News Recommendation Using doc2vec. In: *2018 International Conference on Bangla Speech and Language Processing (ICBSLP)*, pp. 1–5. Available from: doi:10.1109/ICBSLP.2018.8554679 [Accessed 20 January 2020].

[24] Novotná, T. and Harašta, J. (2019) *The Czech Court Decisions Corpus (CzCDC): Availability as the First Step*. ArXiv:1910.09513. [online] Available from: http://arxiv.org/abs/1910.09513 [Accessed 20 January 2020].

[25] Novotný, J. and Ircing, P. (2018) The Benefit of Document Embedding in Unsupervised Document Classification. In: Karpov, A. et al. (eds.). *Speech and Computer. Cham: Springer International Publishing*, pp. 470–478. Lecture Notes in Computer Science. Available from: doi:10.1007/978-3-319-99579-3_49 [Accessed 20 January 2020].

[26] Peczenik, A. (1997) The Binding Force of Precedent. In: MacCormick, N., Summers, R. S. (eds.). *Interpreting Precedents. A Comparative Study*. Dartmouth: Aldeshot, pp. 461–479.

[27] Ranera, L. T. B., Solano, G. A. and Oco, N. (2019) Retrieval of Semantically Similar Philippine Supreme Court Case Decisions using Doc2Vec. In: *2019 International Symposium on Multimedia and Communication Technology (ISMAC)*. IEEE, pp. 1–6.

[28] Renjit, S. and Idicula, S. M. (2019) CUSAT NLP@AILA-FIRE2019: Similarity in Legal Texts using Document Level Embeddings. In: Bhattacharya, P. et al. *Overview of the FIRE 2019 AILA track: Artificial Intelligence for Legal Assistance*. Proc. of FIRE, pp. 12–15.

[29] Savelka, J. and Ashley, K. D. (2018) Segmenting U.S. Court Decisions into Functional and Issue Specific Parts. In: Palmirani, M. (ed.). *Legal Knowledge and Information Systems JURIX 2018*. IOS Press Ebooks, pp. 111–120. Available from: http://ebooks.iospress.nl/volume/legal-knowledge-and-information-systems-jurix-2018-the-thirty-first-annual-conference [Accessed 20 January 2020].

[30] Schweighofer, E., Winiwarter, W. and Merkl, D. (1995) Information filtering: the computation of similarities in large corpora of legal texts. In: *Proceedings of the 5th international conference on Artificial intelligence and law*, p. 119–126.

[31] Smejkalová, T. (2019) Judikatura, nebo precedens? *Právník. Teoretický časopis pro otázky státu a práva*, 158 (9), pp. 852–864.

[32] Tian, X. et al. (2018) K-Means Clustering for Controversial Issues Merging in Chinese Legal Texts. In: Palmirani, M. (ed.). *Legal Knowledge and Information Systems JURIX 2018*. IOS Press Ebooks, pp. 215–219. Available from: http://ebooks.iospress.nl/volume/legal-knowledge-and-information-systems-jurix-2018-the-thirty-first-annual-conference [Accessed 20 January 2020].

[33] Trieu, L. Q., Tran, H. Q. and Tran, M.-T. (2017) News Classification from Social Media Using Twitter-based Doc2Vec Model and Automatic Query Expansion. In: *Proceedings of the Eighth International Symposium on Information and Communication Technology*. Nha Trang City, Viet Nam: Association for Computing Machinery, pp. 460–467. Available from: doi:10.1145/3155133.3155206 [Accessed 20 January 2020].

[34] Wagh, R. and Anand, D. (2017) Application of citation network analysis for improved similarity index estimation of legal case documents: A study. In: *2017 IEEE International*

Conference on Current Trends in Advanced Computing (ICCTAC), pp. 1–5. Available from: doi:10.1109/ICCTAC.2017.8249996 [Accessed 20 January 2020].

DOI 10.5817/MUJLT2020-1-6

PUBLIC PROVOCATION TO COMMIT A TERRORIST OFFENCE: BALANCING BETWEEN THE LIBERTIES AND THE SECURITY[*]

by

KRISTINA RAMEŠOVÁ[**]

Modern terrorism is global and decentralized like cyberspace. While the Darknet is mostly used by terrorists for fundraising campaigns and illicit trading, publicly accessible social platforms such as Twitter, Facebook or YouTube are abused for terrorist propaganda. Combating terrorism remains one of the top priorities of the European union (hereinafter as "the EU"). The approach towards the online content possibly connected to terrorist propaganda has become stricter.

This paper focuses on the development of the EU legislation on the offence related to terrorist activities: the public provocation to commit a terrorist offence, as well as on the obligations of hosting service providers. It also analyses the impact of the Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. The article observes a changing attitude on private monitoring of online information in the development of the EU legislation. It analyses changes in the Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online. These changes signify a shift in the perception of the necessary level of freedom to receive and impart information through the internet.

[*] The article has been supported under the grant No. SVV 260 359 financed by the *Faculty of Law, Charles University*.

[**] kristina.ramesova@email.cz, Ph.D. Candidate at the Department of Administrative Law and Administrative Science, Faculty of Law, Charles University, The Czech Republic.

KEY WORDS

Dissemination of Terrorist Content Online, Hosting Service Providers, Provocation to Commit a Terrorist Offence, Terrorism

1. INTRODUCTION

Social media have become an important part of everyday life. About 95 % of all information on the planet is digital, most of it is accessible via computer networks.[1] Approximately 3 billion people have accounts on *Facebook, Instagram, Messenger* and (or) *WhatsApp*.[2]

A general agreement on a universal legal definition of terrorism does not exist.[3] Numerous international treaties and declarations use their own definitions. The *Arab Convention for the Suppression of Terrorism* defines terrorist acts as:

> *"any act or threat of violence, whatever its motives or purposes, that occurs in the advancement of an individual or collective criminal agenda and seeking to sow panic among people, causing fear by harming them, or placing their lives, liberty or security in danger, or seeking to cause damage to the environment or to public or private installations or property or to occupying or seizing them, or seeking to jeopardise a national resource."*[4]

The *Council of Europe Convention on the Prevention of Terrorism* defines a terrorist offence as *"any of the offences within the scope of and as defined in one of the treaties listed in the Appendix"* of the aforementioned convention.[5] Regardless of numerous sector specific international treaties and definitions of terrorism, the *Special Tribunal for Lebanon* has ruled on the basis

[1] Hilbert, M. and López, P. (2011) The World's Technological Capacity to Store, Communicate, and Compute Information. *Science*, 332 (6025), pp. 60–65. Available from: http://science.sciencemag.org/content/332/6025/60 [Accessed 16 May 2020].

[2] Facebook. (2020) *Facebook Q1 2020 Results. Investor Relations.* [online] Available from: https://s21.q4cdn.com/399680738/files/doc_financials/2020/q1/Q1-2020-FB-Earnings-Presentation.pdf [Accessed 16 May 2020].

[3] Sanyal, S. (2015) International Laws to Control Terrorism: A Comparative Study. *AAKROSH Asian Journal on Terrorism and Internal Conflicts,* p. 3. Available from: http://dx.doi.org/10.2139/ssrn.3232739 [Accessed 16 May 2020].

[4] Art. 1(2) *Arab Convention for the Suppression of Terrorism. Adopted by the Council of Arab Ministers of the Interior and the Council of Arab Ministers of Justice,* 22 April 1998. Available from: https://www.unodc.org/images/tldb-f/conv_arab_terrorism.en.pdf [Accessed 16 May 2020].

[5] Art. 1(1) *Council of Europe Convention on the Prevention of Terrorism,* 16 May 2005. Available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016808c3f55 [Accessed 16 May 2020].

of treaties, *United Nations* resolutions and the legislative and judicial practice of States: There is a customary rule of international law regarding the international crime of terrorism in time of peace,[6] pursuant to which terrorism requires the following three key elements: (i) the intent (*dolus*) of the underlying crime and (ii) the special intent (*dolus specialis*) to spread fear or coerce authority; (iii) the commission of a criminal act, and (iv) that the terrorist act be transnational.[7]

The EU is facing a range of terrorists attacks both from networked groups and lone actors.[8] Cyberspace[9] enables terrorists to find a suitable target and to lead an attack almost from anywhere.[10] According to *Europol*, religiously motivated terrorist groups use the internet and social media to gain instruments of crime and to share information secretly via electronic services as *WhatsApp*, *Viber* or *Skype*; social platforms as *Facebook* and *Twitter* have been used for propaganda, recruitment or sharing information inside closed groups.[11] The EU is aware of growing threat of terrorism and the abuse of cyberspace, particularly the use of internet for propaganda, recruitment, effective communication, planning etc. Combating terrorism remains one of the top priorities of the EU.[12]

According to *Europol*:

> *"[a]s the line between online and offline communities becomes increasingly blurred, terrorist propaganda preying on human suffering abroad reaches*

[6] *Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging.* (2011) STL-11-01/1, Special Tribunal for Lebanon, 16 February 2011. Available from: https://www.refworld.org/cases,STL,4d6280162.html [Accessed 16 May 2020].

[7] Op. cit., para. 85.

[8] EUROPOL. (2019) *The European Union Terrorism Situation and Trend Report 2019*. Available from: https://www.europol.europa.eu/activities-services/main-reports/terrorism-situation-and-trend-report-2019-te-sat [Accessed 16 May 2020].

[9] Virtual environment of interconnected computer devices and networks, i.e. space enabling sharing information and mutual communication. See Barlow, J. P. (1990) Crime and Puzzlement: in advance of the law on the electronic frontier. *Whole Earth Review*, pp. 44–57.

[10] EUROPOL. (2016) *Changes in Modus Operandi of Islamic State (IS) Revisited.* Available from: https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-revisited [Accessed 16 May 2019]; United Nations. (2019) *New technologies, artificial intelligence aid fight against global terrorism.* [press release] September 4. Available from: https://news.un.org/en/story/2019/09/1045562 [Accessed 16 May 2020].

[11] Op. cit., pp. 4, 11–12; EUROPOL. (2019) *Internet Organised Crime Threat Assessment (IOCTA)*, p. 48. Available from: https://www.europol.europa.eu/iocta-report [Accessed 16 May 2020].

[12] European Council. (2018) *EU Counter-Terrorism Strategy*. Available from: https://www.consilium.europa.eu/en/policies/fight-against-terrorism/eu-strategy/ [Accessed 16 May 2020].

> *audiences in Europe to unprecedented extents, inciting some to act and driving others to embrace extremist views on the opposite end."*[13]

Furthermore:

> *"IS*[14] *succeeded in maintaining an online presence largely thanks to unofficial supporter networks and pro-IS media outlets. Pro-IS and pro--al-Qaeda channels promoted the use of alternative platforms and open source technologies."*[15]

Terrorist groups continue to exploit a wide array of online service providers, including forums, file sharing sites, video streaming and sharing sites, blogs, messaging and broadcast applications, social media sites etc.[16] Social platform propaganda is powerful: the stronger and the more vivid the online content is, the more it is going to be perceived as likely to occur in the future, even if not experienced personally.[17]

Understandably, the EU approach towards online content possibly connected to terrorist propaganda has become stricter. Claiming to ensure a smooth functioning of the Digital market, the *European Commission* (hereinafter as "the Commission") presented a draft of a new regulation on 12 September 2018: the *Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online*[18] (hereinafter as "the proposal of online terrorist content regulation" or "the Proposal"), which has been introduced at the end of transposition period of the Directive 2017/541/EU on combating terrorism[19] (hereinafter as "the Counter-Terrorism directive") on 8 September 2018.

[13] EUROPOL. (2019) The *European Union Terrorism Situation and Trend Report 2019*, p. 5. Available from: https://www.europol.europa.eu/activities-services/main-reports/terrorism-situation-and-trend-report-2019-te-sat [Accessed 16 May 2020].

[14] Islamic State, hereinafter as "IS".

[15] Op. cit., p. 7.

[16] EUROPOL. (2019) *Internet Organised Crime Threat Assessment (IOCTA) 2019*, p. 48. Available from: https://www.europol.europa.eu/iocta-report [Accessed 16 May 2020].

[17] Plous, S. (1993) *The Psychology of Judgement and Decision Making*. New York: McGraw-Hill, p. 126.

[18] Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018/640 final). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN [Accessed 16 May 2020].

[19] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. *Official Journal of the European Union.* Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549825019861&uri=CELEX:32017L0541 [Accessed 16 May 2020].

The transposition has not yet been completed in all the EU member states.[20] Also, the Commission's report assessing the extent to which member states have taken measures to comply with the Counter-Terrorism directive and the report assessing its added value, were both not submitted yet.[21]

This paper aims to analyse the development of the EU legislation regarding an offence related to terrorist activities which could be easily perpetrated online: public provocation to commit a terrorist offence. The focus is put on the legislation. As the danger consists of targeting different audiences, worldwide accessibility and possible influence on wide international public opinion,[22] the phenomenon is currently used in the process of advocating new legislative endeavours concerning the prevention of disseminating terrorist content online.[23]

The definition of public provocation to commit a terrorist offence has been clarified in the Counter-Terrorism directive, which also regulates provisions regarding criminal liability, imposes an obligation to criminalise aiding and abetting, inciting and attempting, and determines the possibility for criminal liability of legal persons.[24] However, it seems the measures set up in the Counter-Terrorism directive are not sufficient. Another legislation that shall be directly applicable in all the EU member states has been proposed. Therefore, following questions arise: what is the Counter--Terrorism directive's legal regulation of public provocation to commit a terrorist offence? What changes are suggested by the proposal of online terrorist content regulation and why? What do these changes signify?

[20] Greece, Cyprus and Luxembourg did not comply with the transposition before the deadline. See National transposition measures communicated by the Member States concerning: Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. Available from: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32017L0541 [Accessed 16 May 2020].

[21] According to Art. 29 of the Counter-Terrorism directive, reports shall be given to the European Parliament and to the Council by 8 March 2020 and 8 September 2021.

[22] Broadhurst, R. et al. (2017) *Cyber terrorism: research report of the Australian National University Cybercrime Observatory for the Korean Institute of Criminology*, p. 67. Available from: https://ssrn.com/abstract=2984101 or http://dx.doi.org/10.2139/ssrn.2984101 [Accessed 16 May 2020].

[23] Proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018/640 final). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN [Accessed 16 May 2020].

[24] Art. 5, 13–14, 17–18 Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. *Official Journal of the European Union.* Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549825019861&uri=CELEX:32017L0541 [Accessed 16 May 2020].

A short insight to the development of legislation on terrorism and terrorist offences in the EU and an analysis of the term "public provocation to commit a terrorist offence" are presented. The wording of the Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism, amended by the Decision 2008/919/JHA (hereinafter as "Framework Decision 2008")[25] is compared with the Counter-Terrorism directive. The objectives of the legislation are emphasized and problematic parts in the Counter-Terrorism directive's interpretation are pointed out. The definition of public provocation to commit a terrorist offence is compared with the terrorist content definition presented in the proposal of online terrorist content regulation.

2. DEVELOPMENT OF LEGISLATION AND HARMONISATION OF TERRORIST OFFENCES IN THE EU

The EU started harmonising definitions of terrorist offences in the member states' legislation after terrorist attacks on the *World Trade Centre* on 11 September 2001. Along with the *Council Common Position* of 27 December 2001 on the application of specific measures to combat terrorism, definitions of eleven terrorist acts were adopted.[26] Until recently the cornerstone of criminal response to counter terrorism had been the Framework Decision 2008[27] which has defined a "public provocation to commit a terrorist offence" for the first time as:

> *"the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of one of the offences listed in Article 1(1)(a) to (h), where such conduct, whether or not directly*

[25] Council Framework Decision of 13 June 2002 on combating terrorism and Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism. *Official Journal of the European Union*. Consolidated version Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX: 02002F0475-20081209 [Accessed 16 May 2020].

[26] According to Art. 3 of the Council Common Position of 27 December 2001 on the application of specific measures to combat terrorism, for an act to be considered a terrorist act, there have to be (1) intention, (2) serious damage for a country or an international organisation, (3) being the offence under national law, and (4) presence of at least one of three particularly stipulated motives.

[27] Council Framework Decision of 13 June 2002 on combating terrorism and Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism. *Official Journal of the European Union*. Consolidated version Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX: 02002F0475-20081209 [Accessed 16 May 2020].

> *advocating terrorist offences, causes a danger that one or more such offences may be committed."*[28]

After the adoption of the Framework Decision 2008, most of the EU member states introduced measures criminalising public provocation to commit a terrorist offence. According to the Commission's report from 2014, less than half of the EU member states had adopted specific provisions explicitly criminalising the dissemination of messages to the public:

> *"with a view to inciting terrorist offences, closely aligned to the wording of the Framework Decision 2008".*

However, many of the member states remained on a general level, i.e. criminalising incitement, provocation, facilitation and support of terrorist offences.[29] Different terms used in national legislations left some room for interpretation. According to the Commission, relying on more general terms, instead of relying on the mere intent to incite terrorist offences, might lead to the risk that only *"direct provocation"* not also *"indirect provocation"* would be criminalised.[30] Regarding the incitement to terrorism, national courts have opposed broad definitions in favour of narrow interpretation in order to avoid restricting the freedom of expression and comply with the Article 10 of the *European Convention on Human Rights*.[31] The Framework Decision 2008 did not satisfactorily answer questions on where the free speech ends and the incitement begins. Demands on defining limits between public provocation to commit a terrorist offence and the freedom of speech in a clearer way persisted and

[28] Op. cit., Art. 3 (1) (a).

[29] European Commission. (2008) *The Report from the Commission to the European Parliament and the Council on the implementation of Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism*, p. 5. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52014DC0554 [Accessed 16 May 2020].

[30] In 2014 the provisions were explicitly limited to the direct provocation in Belgium, France and Estonia. A risk of not criminalising the indirect provocation existed in Italy, Hungary, Malta and Lithuania. See op. cit., p. 6.

[31] In 2007, when ruling in the case of a Basque punk band accused for a song referencing the Guardía Civil as the targets of ETA, a Basque separatist organisation, the Spanish Supreme Court ruled that a narrow interpretation of the incitement provision in Spanish criminal code is needed in order to comply with the Article 10 of the ECHR. Rediker, E. (2015) The Incitement of Terrorism on the Internet: Legal Standards, Enforcement, and the Role of the European Union. *Michigan Journal of International Law*, 36 (2), pp. 338–342. Available from: https://repository.law.umich.edu/mjil/vol36/iss2/3/ [Accessed 16 May 2020].

proposals to replace old framework decisions with a new directive appeared.[32]

On 12 December 2015 the Commission proposed a draft of the new Counter-Terrorism directive. The draft aimed not only to adapt the EU legislation to the dissemination of messages, images and other material related to terrorism online, but also to clarify what shall be considered as terrorist offences in the EU. On 15 March 2017 the EU adopted the Counter-Terrorism directive in order to harmonise legislation on fighting terrorism and to adapt legal norms to specific transnational nature. The Counter-Terrorism directive replaced the Framework Decision 2008 and amended parts of the Decision 2005/671/JHA on sharing information and on the cooperation concerning terrorist offences. Regarding online social media, the Counter-Terrorism directive aims particularly to address online propaganda,[33] recruitment[34], and other auxiliary behaviour[35], all of which increase the risk that terrorist offence would be committed.[36]

3. OFFENCES WITHIN THE GENERAL CONCEPT OF TERRORISM

The Counter-Terrorism directive's strength consists in approximation of definitions of terrorist offences, offences related to a terrorist group, and offences related to terrorist activities in all the EU member states.[37] Legal provisions of fight to counter terrorism have been strengthened by criminalisation of behaviour that is a preparatory phase of crime, such

[32] Ibid.

[33] Art. 5–6 Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. *Official Journal of the European Union*. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549825019861&uri=CELEX:32017L0541 [Accessed 16 May 2020].

[34] Op. cit., Art. 6.

[35] Op. cit., Art. 7–12.

[36] Shamieh, L. and Szenes, Z. (2015) The Propaganda of ISIS/DAESH through the Virtual Space. *Defence Against Terrorism Revue*, 7 (1), p. 9. Available from: http://www.coedat.nato.int/publication/datr/volumes/datr10.pdf [Accessed 16 May 2020]. For simplified and unified model of radicalisation process see Hunter, R. and Heinke, D. H. (2011) Radicalization of Islamist Terrorists in the Western World. *FBI Law Enforcement Bulletin*, 9 (80), pp. 25–31. Available from: https://leb.fbi.gov/articles/perspective/perspective-radicalization-of-islamist-terrorists-in-the-western-world [Accessed 16 May 2020].

[37] With an exception of United Kingdom, Ireland and Denmark. Rec. 41–42 of the Counter--Terrorism directive.

as recruitment (Art. 6), providing training for terrorism (Art. 8) or travelling for the purpose of terrorism (Art. 9).

The Counter-Terrorism directive recognises three groups of offences: (i) terrorist offences, (ii) offences related to a terrorist group and (iii) offences related to terrorist activities. The list of terrorist offences is exhaustive and encompasses only intentional acts explicitly mentioned in Art. 3, defined as offences under national law and, given their nature or context, being able to seriously damage a country or an international organisation, and in the case they were committed with the terrorist intention.[38] The notion of terrorist intention must apply to all the elements of crime. Outside these conditions a misuse of information and communications technology (hereinafter as "ICT") for propaganda, recruitment or dissemination of training instructions with the intent to commit or to contribute to the commission of any terrorist offence could be considered as offence related to terrorist activities. The offences linked to terrorist activities fall within the scope of the general concept of terrorism.[39]

3.1. PUBLIC PROVOCATION TO COMMIT A TERRORIST OFFENCE

Among offences related to terrorist activities a particular interest is put on the offence of public provocation to commit a terrorist offence, which shall comprise glorification or justification of terrorism or dissemination of messages or images in order to gain support for terrorist purposes.[40] Public provocation to commit a terrorist offence is defined as:

> *"the distribution, or otherwise making available by any means, whether online or offline, of a message to the public, with the intent to incite the commission of one of the offences listed in points (a) to (i) of Article 3(1), where such conduct, directly or indirectly, such as by the glorification of terrorist acts, advocates the commission of terrorist offences, thereby*

[38] Art. 3 (2) Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. *Official Journal of the European Union.* Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549825019861&uri=CELEX:32017L0541 [Accessed 16 May 2020].

[39] Judgement of 31 January 2017, Lounani, C-573/14, ECLI:EU:C:2017:71, para. 50–51.

[40] Rec. 10 Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. *Official Journal of the European Union.* Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549825019861&uri=CELEX:32017L0541 [Accessed 16 May 2020].

causing a danger that one or more such offences may be committed, is punishable as a criminal offence when committed intentionally."[41]

The EU member states shall criminalise not only aiding and abetting but also inciting the offence.[42] In comparison to the Framework Decision 2008 the criminalisation of involvement in public provocation to commit a terrorist offence has been extended to inciting.[43]

It is apparent that the definition is broader than the previous one in the Framework Decision 2008. The Counter-Terrorism directive's definition emphasizes that the distribution (or otherwise making available) of the message to the public may occur by any means, either online or offline. Also, it stipulates expressly that it is not important if such distribution advocates the commission of listed terrorist offences directly or indirectly, because the Commission was afraid that the indirect provocation would not be criminalised in all member states.[44] Another extension of the definition presents the list of terrorist offences intended to be incited by the provocation. Art. 3 (1) i) of the Counter-Terrorism directive provides for a new terrorist offence of illegal system interference;[45] a disposure of radiological weapons and development of radiological or nuclear weapons are added to the definition of terrorist offence.[46]

The further change concerns a fault which is presented in the definition of the offence itself. The Counter-Terrorism directive's definition of public provocation to commit a terrorist offence has emphasized the intent *("… is punishable as a criminal offence when committed intentionally"),*[47] whether

[41] Op. cit., Art. 5.

[42] Op. cit., Art. 14 (1) (2).

[43] Art. 4 (2) Council Framework Decision of 13 June 2002 on combating terrorism and Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism. *Official Journal of the European Union*. Consolidated version Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02002F0475-20081209 [Accessed 16 May 2020]; Art. 14 (2) Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. *Official Journal of the European Union.* Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549825019861&uri=CELEX:32017L0541 [Accessed 16 May 2020].

[44] See Chapter 1.

[45] Art. 3 (1) i) Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. *Official Journal of the European Union.* Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549825019861&uri=CELEX:32017L0541 [Accessed 16 May 2020].

[46] Op. cit., Art. 3 (1) f).

[47] Op. cit., Art. 5.

the Framework Decision 2008 mentioned the intent in another provision, when demanding criminalisation of expressly stipulated *intentional* acts, such as public provocation to commit a terrorist offence.[48] In the definition of public provocation to commit a terrorist offence itself, the Framework Decision 2008 mentioned the intent only when stipulating *"the intent to incite the commission of one of the offences listed in Article 1(1)(a) to (h)."*[49] Nevertheless, the interpretation of fault should stay the same as in the Framework Decision 2008: the Framework Decision 2008 has stipulated that the distribution or otherwise making available of a message to the public, has to be perpetrated with the intent to incite the commission of one of the listed offences.[50] Such distribution could be hardly committed in negligence, i.e. with no intent, as a perpetrator necessarily had to act with the particular intent to incite the commission of at least one of the offences listed in Article 1(1)(a) to (h) of the Framework Decision 2008.[51]

Regarding the body of crime, the Counter-Terrorism directive evidently does not distinguish between online and offline environment. For the criminal liability it is not important. Nevertheless, it underlines that such conduct should be punishable when it causes a danger that terrorists acts may be committed; such danger should be considered regarding the addressee of the message.[52] As the online illegal content spreads easily and reaches disproportionately more audiences (addressees) as possible, committing crime online may be considered as an aggravating circumstance. On the other hand, a particularly injurious effect of the crime committed online is disputable, as the actual effect of online propaganda in individual radicalisation of a perpetrator is not so clear. According to *Heinke*, even though an ideological framing may happen individually through the internet, yet in most cases social contacts with peers are more important; radicalisation does not often happen only after observing

[48] Art. 3 (2) a) Council Framework Decision of 13 June 2002 on combating terrorism and Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism. *Official Journal of the European Union*. Consolidated version Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02002F0475-20081209 [Accessed 16 May 2020].

[49] Op. cit., Art. 3 (1) a).

[50] Op. cit., Art. 3 (1).

[51] Ibid.

[52] Rec. 10 Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. *Official Journal of the European Union*. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549825019861&uri=CELEX:32017L0541 [Accessed 16 May 2020].

a terrorist propaganda video or reading online radicalising message but through closer social relationships in a radicalised community of peers.[53] Consequently, the effect of any particular offence should be addressed and evaluated in each individual case.

Further amendment to the previous definition of public provocation to commit a terrorist offence set by the Framework Decision 2008, is the causality between a distribution of the message to the public and the danger that any terrorist offence may be committed: it is explicitly stated that the indirect provocation is sufficient. The aim was to harmonise national legislation so that the indirect provocation would be criminalised in all the EU member states without an exception.[54] Nevertheless, the interpretation of indirect provocation by national courts may still vary; a preliminary question to the *Court of Justice of the EU* has not yet been asked. The danger that a terrorist offence would be actually committed, should be judged according to specific circumstances of the case, such as who the author and the addressee of the message were and in which context the act is committed.[55]

The Counter-Terrorism directive particularly proclaims that any of its provisions cannot be interpreted as the reduction or restriction to the dissemination of information for scientific, academic or reporting purposes; furthermore:

> *"the expression of radical, polemic or controversial views in the public debate on sensitive political questions, falls outside the scope of this directive and, in particular, of the definition of public provocation to commit terrorist offences."*[56]

[53] Heinke, D. H. (2016) Countering Radicalisation and Recruitment of so-called Jihadists – Proscription of Radicalization Hubs. *Defence Against Terrorism Revue*, 8, p. 92.

[54] The Report from the Commission to the European Parliament and the Council on the implementation of Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism (COM/2014/554 final) Available from: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/crisis-and-terrorism/general/docs/report_on_the_implementation_of_cfd_2008-919-jha_and_cfd_2002-475-jha_on_combating_terrorism_en.pdf [Accessed 4 June 2020].

[55] Rec. 10 Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. *Official Journal of the European Union.* Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549825019861&uri=CELEX:32017L0541 [Accessed 16 May 2020].

[56] Op. cit., Rec. 10 and 40.

Interestingly, the wording of the proposal of online terrorist content regulation is not so strict, stipulating:

> *"the expression of radical, polemic or controversial views in the public debate on sensitive political questions should not be considered terrorist content."*[57]

The scope of freedom of speech, when it comes to terrorist propaganda, remains blurred due to many indefinite legal terms used, which might be problematic regarding principles of foreseeability and unambiguity of criminal law. These principles are meant to secure that a person has to know whether she would commit a crime by particular act.[58]

3.2. COUNTER-TERRORISM DIRECTIVE AND HOSTING SERVICE PROVIDERS' OBLIGATIONS

Legal persons may be held criminally liable for public provocation to commit a terrorist offence under the conditions of Art. 17 (1) (2) of the Counter-Terrorism directive. The provision is particularly important to hosting service providers (hereinafter as "HSP") as they enable uploading third party content. It is strictly stipulated that a legal person may be held liable in the situation where the lack of supervision or control by a person in the particular leading position has made possible the commission of public provocation to commit a terrorist offence, for the benefit of the legal person by a person under its authority.

The obligation to remove or to block online terrorist content is imposed as a preventive measure[59] and is presumed to be adopted promptly,

[57] Rec. 9 Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018/640 final). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN [Accessed 16 May 2020].

[58] For the complexities of the right to the free speech on the internet in different jurisdictions, see Lessig, L. and Resnick, P. (1999) Zoning Speech on the Internet: A Legal and Technical Model. *Michigan Law Review*, p. 395–396. Available from: https://cyber.harvard.edu/wg_home/uploads/200/1999-06.pdf [Accessed 16 May 2020]; Barnhizer for example describes the U.S. approach to the limitations on free speech with the phrase *"sticks and stones can break the bones but words can never hurt"*, in comparison to the European world in which *"the beliefs of many ethnic and religious groups are closely related to pride, honor and shame."* Barnhizer, D. R. (2007) *Reverse Colonization: Islam, Honor Cultures and the Confrontation between Divine and Quasi-Secular Natural Law.* Cleveland-Marshall Legal Studies Paper No. 07-142, p. 5. Available from: https://ssrn.com/abstract=980687 [Accessed 16 May 2020].

[59] Art. 21 Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. *Official Journal of the European Union.* Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549825019861&uri=CELEX:32017L0541 [Accessed 16 May 2020].

i.e. without any link to criminal or other proceedings. It is expressly stipulated that no general obligation to monitor transmitted or stored information nor to actively seek out the facts or circumstances indicating illegal activity should be imposed on service providers. The actual knowledge of illegal activity and awareness of the facts is still essential for their liability.[60] Although no obligation regarding private monitoring is imposed, the endeavours are welcomed. The Counter-Terrorism directive presumes either public or judicial action, enhancing particularly voluntary action of the Internet industry,[61] such as forming the Global Internet forum to Counter Terrorism by *Facebook*, *Microsoft*, *Twitter* and *YouTube* in July 2017[62] or the cooperation of *Facebook*, *Twitter*, *Google* and *Microsoft* in using the software *PhotoDNA* to detect extremist online content, such as violent terrorist imagery or recruitment videos.[63] The cooperation is based on sharing an industry database of "hashes", i.e. unique digital fingerprints for violent terrorist imagery or videos that have been removed from their services. Only the most extreme content is shared in the database, the one most likely to violate all of the respective companies' content policies.[64]

Even though the number of HSP who have put in place measures dealing with terrorist content on their services rises, the Commission does not consider voluntary frameworks and partnerships sufficient enough, as not all affected HSP engaged in the voluntary cooperation.[65] To speed up the procedures dealing with terrorist content on the services of information society service providers in the EU, a new regulation on preventing the dissemination of terrorist content online has been proposed.

[60] Op. cit., Rec. 23.

[61] Op. cit., Rec. 22.

[62] GIFCT. *Global Internet Forum to Counter Terrorism: Evolving an Institution.* [online] Available from: https://gifct.org/about/ [Accessed 16 May 2020].

[63] Facebook. (2016) *Partnering to Help Curb Spread of Online Terrorist Content.* [press release] 5 December. Available from: https://newsroom.fb.com/news/2016/12/partnering-to-help-curb-spread-of-online-terrorist-content/ [Accessed 16 May 2020].

[64] Ibid.

[65] Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018/640 final), p. 1. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN [Accessed 16 May 2020].

4. PROPOSAL FOR A NEW REGULATION ON PREVENTING THE DISSEMINATION OF TERRORIST CONTENT ONLINE

Legal basis for the new regulation should be Art. 114 of the Treaty on the functioning of the EU providing for the adoption of measures approximating the establishment and functioning of the internal market.[66] Although the proposed provisions are primarily focused to tackle online terrorist propaganda, the Commission itself repeats the motive to intervene against the dissemination of terrorist content. Chosen legal basis and alleged obstacles for economic activity in the EU as the main goal of new regulation are rather questionable. The first paragraph of the explanatory memorandum itself refers to the terrorist attacks and the misuse of internet by terrorists aiming to glorify their atrocities.[67] Nevertheless, a proclaimed goal of the legislation is:

> *"to guarantee the smooth functioning of the Digital Single Market, whilst ensuring trust and security."*[68]

By setting a minimum set of obligations for the HSP directing their services to the EU, the Commission believes in preventing the misuse of internet for terrorist purposes, improving accountability and transparency of HSP offering services in the EU, and clarifying their liability rules.[69] New regulation should lead to detection and removal or blocking of online terrorist content by the HSP offering services in the EU irrespective of their place of main establishment.[70] However, the scope of applicability is narrowed by a definition of "to offer services in the EU" and by demanding either an establishment in the EU, a significant number of users, or targeting the activities to at least one member state.[71]

Liability benefit in Art. 14 of the E-commerce directive[72] stipulating specific conditions under which HSP are not liable for the stored

[66] Op. cit., p. 4.

[67] Op. cit., p. 1.

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

[69] Op. cit., p. 2. See also Art. 1 Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018/640 final). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN [Accessed 16 May 2020].

[70] Art. 1 (2) Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018/640 final). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN [Accessed 16 May 2020].

[71] Op. cit., Art. 2 (3).

information, should not be affected by any pro-active measures adopted on the basis of the regulation.[73] However, Art. 15 (1) of the E-commerce directive expressly specifies that no general obligation to monitor the transmitted or stored information, nor to actively seek facts or circumstances indicating illegal activity shall be imposed on HSP. The prohibition of general monitoring in the E-commerce directive compared with the proactive monitoring for terrorist content online shows a clear change of perception on the necessary level of virtual freedom. Even though Rec. 19 of the Proposal proclaims that any proportionate and specific proactive measures should not present a general obligation to monitor,[74] it is also mentioned that grave risks of terrorist content dissemination may justify a derogation from this principle under the EU framework and the HSP shall take proactive measures against the dissemination of terrorist content.[75] The negotiating position of the Council of the EU adopted on 6 December 2018 which agreed on the proposed rules, is also signaling the shift in the attitude towards monitoring illegal and harmful online content.[76]

On the other hand, the *European Parliament* (hereinafter as "EP") in the legislative resolution of 17th April 2019 on the Proposal, adopted many amendments aiming to emphasize the freedom to receive and impart information and ideas in an open and democratic society, the rule of law and the perception of terrorist content as a part of a broader problem of illegal content online, and the general obligation for HSP to monitor

[72] Art. 14 of the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. *Official Journal of the European Union*. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549827901048&uri=CELEX:32000L0031 [Accessed 16 May 2020]. (hereinafter as "E-commerce directive")

[73] Rec. 5 Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018/640 final). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN [Accessed 16 May 2020].

[74] Op. cit., Rec. 19.

[75] Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018/640 final), pp. 3–5. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN [Accessed 16 May 2020].

[76] Council of the EU. (2018) *Terrorist Content Online: Council adopts negotiating position on new rules to prevent dissemination.* [press release] 6 December. Available from: https://www.consilium.europa.eu/en/press/press-releases/2018/12/06/terrorist-content-online-council-adopts-negotiating-position-on-new-rules-to-prevent-dissemination/ [Accessed 16 May 2020].

stored information or to actively seek facts indicating illegal activity has been refused.[77]

Although the Proposal introduces a completely new definition of terrorist content on the basis of the Counter-Terrorism directive, it does not have an impact on definitions of terrorist offences set in the Counter--Terrorism directive. Under Art. 2 (5) terrorist content should mean following information:

> *a) inciting or advocating, including by glorifying, the commission of terrorist offences, thereby causing a danger that such acts be committed;*
> *b) encouraging the contribution to terrorist offences;*
> *c) promoting the activities of a terrorist group, in particular by encouraging the participation in or support to a terrorist group within the meaning of Art. 2(3) of the directive on combating terrorism or*
> *d) instructing on methods or techniques for the purpose of committing terrorist offences.*[78]

According to Art. 5 of the Counter-Terrorism directive the essence of public provocation to commit a terrorist offence is the message intending to incite commission of terrorist offence. The Proposal introduces a broader definition of terrorist content, which comprises inciting and advocating, but also promoting and instructing on the activities related to terrorist offences. Such definition enables to remove (or block access to) a wider set of online content particularly through the indefinite "activities" of a terrorist group. The EP's amendments have narrowed the definition with the link to the terrorist offences in the Counter-Terrorism directive and the notion

[77] Compare the Amendments 2–4, 6, 10, 12, 15, 21, 27, 43, 45, 46, 61, 62, 85, 86, 87, 88, 100, 103, 104, 106, 107, 110, 147 adopted by the EP. European Parliament legislative resolution of 17 April 2019 on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM(2018) 0640 – C8-0405/2018 – 2018/0331(COD)). Available from: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=EP:P8_TA(2019)0421 [Accessed 16 May 2020].

[78] Art. 2(5) Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018/640 final). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN [Accessed 16 May 2020].

of intent,[79] but did not clarify the activities of a terrorist group under Art. 2(5) c) of the Proposal.[80]

Assessment of whether an information is or is not a terrorist content shall be done both by public authorities and HSP. Some rules are offered, but the guidance is only general.[81] Overbroad definitions are criticised as the text introduces risks of arbitrariness in the removal of online content.[82] Even though the Proposal enhances adoption of proactive measures regarding the monitoring of online content by HSP to prevent dissemination of terrorist content, the distinction of free speech and illegal terrorist content is not improved, while fundamental conditions could have been stipulated in terms and conditions of each HSP.[83] The EP has deleted the latter provision that could be perceived as a step towards fragmentation of the freedom to receive and share information online.[84]

HSP should apply measures to prevent dissemination of terrorist content and to determine what appropriate, proportionate and effective proactive measure should be put in place, while in the same time they are not encouraged to perform general monitoring.[85] Empowering other bodies than judicial to decide on the implemented measures has been criticised by the *Committee on Internal Market and Consumer Protection of the European*

[79] Amendment 53, 54. European Parliament legislative resolution of 17 April 2019 on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM(2018)0640 – C8-0405/ 2018 – 2018/0331(COD)). Available from: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=EP:P8_TA(2019)0421 [Accessed 16 May 2020].

[80] Op. cit., Amendment 55.

[81] Rec. 9 Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018/640 final). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN [Accessed 16 May 2020].

[82] EDRI. (2018) *The EU Council's general approach on Terrorist Content Online proposal: A step towards pre-emptive censorship*. [press release] 11 December. Available from: https://edri.org/the-eu-councils-general-approach-on-terrorist-content-online-proposal-a-step-towards-pre-emptive-censorship/ [Accessed 16 May 2020].

[83] See Art. 3 (2) Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018/640 final). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN [Accessed 16 May 2020].

[84] Amendment 63 European Parliament legislative resolution of 17 April 2019 on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM(2018)0640 – C8-0405/2018 – 2018/0331 (COD)). Available from: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=EP:P8_TA (2019)0421 [Accessed 16 May 2020].

[85] Rec. 16 Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018/640 final). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN [Accessed 16 May 2020].

Parliament (hereinafter as "IMCO").[86] The IMCO has made amendments to Rec. 37 of the Proposal so that administrative authorities may only issue removal orders on the basis of a court decision, but may not impose penalties.[87] A provision regarding a "competent authority" which shall mean only *"a designated national judicial authority in the Member State"*, has been added.[88] The changes signalised distrust in the arrangement where non-judicial (public or private) authorities would gain broad powers in the online content supervision system. Consequently, the EP has amended Rec. 37 and proposed, that the competent authority shall be:

> *"a single designated judicial authority or functionally independent administrative authority in the Member State."*[89]

Another obligation of HSP is to comply with legal order requesting to remove or to disable access to terrorist content within one hour from receiving the order from competent authority.[90] Considerable financial penalties for the HSP who would fail to do so are suggested.[91] The one-hour limit for the removal was regarded as too short and unrealistic.[92] Therefore, the EP has obliged the HSP to remove terrorist content or disable access to it *"as soon as possible"*, but as the rule *"within one hour from receipt of the removal order"* has stayed,[93] the obligation is even stricter. Choice of competent authority with the power to issue a removal order is on the member states;

[86] Draft Opinion of the Committee on the Internal Market and Consumer Protection for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (2018/0331 (COD)). Available from: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-632.028+01+DOC+PDF+V0//EN&language=EN [Accessed 16 May 2020].

[87] Op. cit., Amendment 30.

[88] Op. cit., Amendments 48, 88.

[89] Amendment 60 European Parliament legislative resolution of 17 April 2019 on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM(2018)0640 – C8-0405/2018 – 2018/0331 (COD)). Available from: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=EP:P8_TA (2019)0421 [Accessed 16 May 2020].

[90] Art. 4 (2) Proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018/640 final). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN [Accessed 16 May 2020].

[91] Op. cit., Art. 18 (4).

[92] Draft Opinion of the Committee on the Internal Market and Consumer Protection for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (2018/0331 (COD)). Available from: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-632.028+01+DOC+PDF+V0//EN&language=EN [Accessed 16 May 2020].

it could be single designated judicial authority or functionally independent administrative authority.[94] Possibility to have removal orders issued from other than judicial authorities might be problematic as the removal orders can intervene with the right to share and receive information. Possible variant would be to have the public authority issue a removal order in preliminary proceedings. Interim and precautionary measures are typical in civil and criminal court proceedings throughout the EU[95] and may be imposed on a defendant or an accused person by a court before the final judgement on the merits is rendered. As the removal orders according to Art. 4 (2) of the Proposal will definitely interfere with the right to the free speech and freedom to share and receive information, the competent authority with the power to issue them should be the court. On the other hand, courts are not specialised in particular agenda as the administrative bodies are, and court proceedings may be lengthier. A fast reaction needed to block or remove online terrorist content effectively could be jeopardized.

5. CONCLUSION

Manifestations of terrorists' beliefs and activities are visible online as terrorists use online social media platforms to magnify impact of their acts or to promote their crimes publicly. Even though social contact is deemed more important for individual radicalisation, online terrorist propaganda plays a particular role. The HSP offering their services in the EU are encouraged to identify terrorist online content and to remove it immediately from all their respective services and platforms. Many HSP started to participate in voluntary frameworks and partnerships to share information and cooperate.

While the Counter-Terrorism directive focuses on harmonisation of terrorist offences' definitions and obliges the EU member states to ensure prompt removal of such online terrorist content, the proposal of online terrorist content regulation clearly imposes the obligations to prevent dissemination of terrorist content online, including the choice of proactive

[93] Amendment 69 European Parliament legislative resolution of 17 April 2019 on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM(2018)0640 – C8-0405/2018 – 2018/0331 (COD)). Available from: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=EP:P8_TA (2019)0421 [Accessed 16 May 2020].

[94] Op. cit., Amendment 60.

[95] European Union. (2019) *Interim and precautionary measures. European e-justice.* [online] Available from: https://e-justice.europa.eu/content_interim_and_precautionary_measures-78-en.do?init=true [Accessed 16 May 2020].

measures, on HSP. Risks that the measures might unlawfully restrict the right to information have been described. The demands to define the limits between public provocation to commit a terrorist offence and the freedom of speech persist. The burden of assessment whether online information does or does not constitute a terrorist content will be shifted more on HSP who will become the actual jurors of legality. Even though this approach is understandable due to the immense amount of online information and the abuse of social platforms for terrorist propaganda and recruitment, risks for freedom to receive and impart information is apparent. There is a clear change of perception on the necessary level of online control and monitoring in the EU.

The approach of prioritizing security before liberties of digital society has led the Commission to present the proposal of online terrorist content regulation. Generally approving attitude of the Council on preventive regulation of the internet regarding online terrorist content and the changes in secondary legislation reflect considerable shift in the perception of individuals' freedoms in online environment. The EP's amendments, on the other hand, emphasized the liberties of online environment. Remedies ensuring due review of removal and blocking of alleged illegal online content must be secured. HSP should be encouraged to remove terrorist content online and to cooperate with member states' law enforcement agencies and *Europol*. Nevertheless, implemented measures should be decided by the public authorities in the proceedings with a possibility of judicial review.

Balancing between liberty and security is persistent in the political environment since the terrorist attacks of 11 September 2001.[96] In adopting specific counter-measures against the risk of terrorism, the analysis performed by decision makers is likely to be tilted towards the interest on security than the one on liberty.[97] The terrorist attacks experienced during recent years have accelerated and influenced the legislative process in the EU significantly and might be leading to undervaluation of liberty, particularly the right to receive and impart information as a basic principle of information society.

[96] Waldron, J. (2011) Safety and Security. *Nebraska Law Review*, 85. Available from: http://digitalcommons.unl.edu/nlr/vol85/iss2/5/ [Accessed 16 May 2020].

[97] Gross, O. (2018) *Security vs. Liberty: An Imbalanced Balancing.* Minnesota Legal Studies Research Paper No. 09-42, pp. 2–3. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1471634 [Accessed 16 May 2020].

LIST OF REFERENCES

[1] *Arab Convention for the Suppression of Terrorism. Adopted by the Council of Arab Ministers of the Interior and the Council of Arab Ministers of Justice*, 22 April 1998. Available from: http://www.unodc.org/images/tldb-f/conv_arab_terrorism.en.pdf [Accessed 16 May 2020].

[2] Barlow, J. P. (1990) Crime and Puzzlement: in advance of the law on the electronic frontier. *Whole Earth Review.*

[3] Barnhizer, D. R. (2007) *Reverse Colonization: Islam, Honor Cultures and the Confrontation between Divine and Quasi-Secular Natural Law.* Cleveland-Marshall Legal Studies Paper No. 07-142. Available from: https://ssrn.com/abstract=980687 [Accessed 16 May 2020].

[4] Broadhurst, R. et al. (2017) *Cyber terrorism: research report of the Australian National University Cybercrime Observatory for the Korean Institute of Criminology.* Available from: https://ssrn.com/abstract=2984101 or http://dx.doi.org/10.2139/ssrn.2984101 [Accessed 16 May 2020].

[5] Council Framework Decision of 13 June 2002 on combating terrorism and Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism. *Official Journal of the European Union*. Consolidated version available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02002F0475-20081209 [Accessed 16 May 2020].

[6] *Council of Europe Convention on the Prevention of Terrorism*, 16 May 2005. Available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016808c3f55 [Accessed 16 May 2020].

[7] Council of the EU. (2018) *Terrorist Content Online: Council adopts negotiating position on new rules to prevent dissemination.* [press release] 6 December. Available from: https://www.consilium.europa.eu/en/press/press-releases/2018/12/06/terrorist-content-online-council-adopts-negotiating-position-on-new-rules-to-prevent-dissemination/ [Accessed 16 May 2020].

[8] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. *Official Journal of the European Union*. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549827901048&uri=CELEX:32000L0031 [Accessed 16 May 2020].

[9] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. *Official Journal of the European Union.*

Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549825019861&uri=CELEX:32017L0541 [Accessed 16 May 2020].

[10] Draft Opinion of the Committee on the Internal Market and Consumer Protection for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (2018/0331 (COD)). Available from: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-632.028+01+DOC+PDF+V0//EN&language=EN [Accessed 16 May 2020].

[11] EDRI. (2018) *The EU Council's general approach on Terrorist Content Online proposal: A step towards pre-emptive censorship*. [press release] 11 December. Available from: https://edri.org/the-eu-councils-general-approach-on-terrorist-content-online-proposal-a-step-towards-pre-emptive-censorship/ [Accessed 16 May 2020].

[12] European Commission. (2008) *The Report from the Commission to the European Parliament and the Council on the implementation of Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism*. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52014DC0554 [Accessed 16 May 2020].

[13] European Council. (2018) *EU Counter-Terrorism Strategy*. Available from: https://www.consilium.europa.eu/en/policies/fight-against-terrorism/eu-strategy/ [Accessed 16 May 2020].

[14] European Parliament legislative resolution of 17 April 2019 on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM(2018)0640 – C8-0405/2018 –2018/0331 (COD)). Available from: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=EP:P8_TA(2019)0421 [Accessed 16 May 2020].

[15] European Union. (2019) *Interim and precautionary measures. European e-justice.* [online] Available from: https://e-justice.europa.eu/content_interim_and_precautionary_measures-78-en.do?init=true [Accessed 16 May 2020].

[16] EUROPOL. (2016) *Changes in Modus Operandi of Islamic State (IS) Revisited.* Available from: https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-revisited [Accessed 16 May 2019].

[17] EUROPOL. (2019) *Internet Organised Crime Threat Assessment (IOCTA)*. Available from: https://www.europol.europa.eu/iocta-report [Accessed 16 May 2020].

[18] EUROPOL. (2019) *The European Union Terrorism Situation and Trend Report 2019*. Available from: https://www.europol.europa.eu/activities-services/main-reports/terrorism-situation-and-trend-report-2019-te-sat [Accessed 16 May 2020].

[19] Facebook. (2016) *Partnering to Help Curb Spread of Online Terrorist Content.* [press release] 5 December. Available from: https://newsroom.fb.com/news/2016/12/partnering-to-help-curb-spread-of-online-terrorist-content/ [Accessed 16 May 2020].

[20] Facebook. (2020) *Facebook Q1 2020 Results. Investor Relations.* [online] Available from: https://s21.q4cdn.com/399680738/files/doc_financials/2020/q1/Q1-2020-FB-Earnings-Presentation.pdf [Accessed 16 May 2020].

[21] GIFCT. *Global Internet Forum to Counter Terrorism: Evolving an Institution.* [online] Available from: https://gifct.org/about/ [Accessed 16 May 2020].

[22] Gross, O. (2018) *Security vs. Liberty: An Imbalanced Balancing.* Minnesota Legal Studies Research Paper No. 09-42. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1471634 [Accessed 16 May 2020].

[23] Hilbert, M. and López, P. (2011) The World's Technological Capacity to Store, Communicate, and Compute Information. *Science*, 332 (6025). Available from: http://science.sciencemag.org/content/332/6025/60 [Accessed 16 May 2020].

[24] Heinke, D. H. (2016) Countering Radicalisation and Recruitment of so-called Jihadists – Proscription of Radicalization Hubs. *Defence Against Terrorism Revue*, 8.

[25] Hunter, R. and Heinke, D. H. (2011) Radicalization of Islamist Terrorists in the Western World. *FBI Law Enforcement Bulletin*, 9 (80). Available from: https://leb.fbi.gov/articles/perspective/perspective-radicalization-of-islamist-terrorists-in-the-western-world [Accessed 16 May 2020].

[26] *Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging.* (2011) STL-11-01/1, Special Tribunal for Lebanon, 16 February 2011. Available from: https://www.refworld.org/cases,STL,4d6280162.html [Accessed 16 May 2020].

[27] Judgement of 31 January 2017, Lounani, C-573/14, ECLI:EU:C:2017:71.

[28] Lessig, L. and Resnick, P. (1999) Zoning Speech on the Internet: A Legal and Technical Model. *Michigan Law Review*. Available from: https://cyber.harvard.edu/wg_home/uploads/200/1999-06.pdf [Accessed 16 May 2020].

[29] National transposition measures communicated by the Member States concerning: Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and

amending Council Decision 2005/671/JHA. Available from: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32017L0541 [Accessed 16 May 2020].

[30] Plous, S. (1993) *The Psychology of Judgement and Decision Making.* New York: McGraw-Hill.

[31] Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM/2018/640 final). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN [Accessed 16 May 2020].

[32] Rediker, E. (2015) The Incitement of Terrorism on the Internet: Legal Standards, Enforcement, and the Role of the European Union. *Michigan Journal of International Law*, 36 (2). Available from: https://repository.law.umich.edu/mjil/vol36/iss2/3/ [Accessed 16 May 2020].

[33] Sanyal, S. (2015) International Laws to Control Terrorism: A Comparative Study. *AAKROSH Asian Journal on Terrorism and Internal Conflicts*. Available from: http://dx.doi.org/10.2139/ssrn.3232739 [Accessed 16 May 2020].

[34] Shamieh, L. and Szenes, Z. (2015) The Propaganda of ISIS/DAESH through the Virtual Space. *Defence Against Terrorism Revue*, 7 (1). Available from: http://www.coedat.nato.int/publication/datr/volumes/datr10.pdf [Accessed 16 May 2020].

[35] The Report from the Commission to the European Parliament and the Council on the implementation of Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism (COM/2014/554 final). Available from: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/crisis-and-terrorism/general/docs/report_on_the_implementation_of_cfd_2008-919-jha_and_cfd_2002-475-jha_on_combating_terrorism_en.pdf [Accessed 4 June 2020].

[36] United Nations. (2019) *New technologies, artificial intelligence aid fight against global terrorism.* [press release] September 4. Available from: https://news.un.org/en/story/2019/09/1045562 [Accessed 16 May 2020].

[37] Waldron, J. (2011) Safety and Security. *Nebraska Law Review*, 85. Available from: http://digitalcommons.unl.edu/nlr/vol85/iss2/5/ [Accessed 16 May 2020].

Cyberspace 2019 Partners

vodafone

Vodafone Czech Republic
www.vodafone.cz

Wolters Kluwer

Wolters Kluwer ČR
www.wkcr.cz

Zákony pro lidi.cz

Zákony pro lidi - AION CS
www.zakonyprolidi.cz

§ CODEXIS®

CODEXIS - ATLAS consulting
www.codexis.cz

Notes for Contributors

Focus and Scope

Masaryk University Journal of Law and Technology (ISSN on-line 1802-5951, ISSN printed 1802-5943) is a peer-reviewed academic journal which publishes original articles in the field of information and communication technology law. All submissions should deal with phenomena related to law in modern technologies (e.g. privacy and data protection, intellectual property, biotechnologies, cyber security and cyber warfare, energy law). We prefer submissions dealing with contemporary issues.

Structure of research articles

Each research article should contain a title, a name of the author, an e-mail, keywords, an abstract (max. 1 500 characters including spaces), a text (max. 45 000 characters including spaces and footnotes) and list of references.

Structure of comments

All comments should contain a title, a name of the author, an e-mail, keywords, a text (max. 18 000 characters) and a list of references.

Structure of book reviews

Each book review should contain a title of the book, a name of the author, an e-mail, a full citation, a text (max. 18 000 characters) and a list of references.

Structure of citations

Citations in accordance with AGPS Style Guide 5th ed. (Harvard standard), examples:

Book, one author: Dahl, R. (2004) *Charlie and the Chocolate Factory*. 6th ed. New York: Knopf.
Book, multiple authors: Daniels, K., Patterson, G. and Dunston, Y. (2014) *The Ultimate Student Teaching Guide.* 2nd ed. Los Angeles: SAGE Publications, pp.145-151.
Article: Battilana, J. and Casciaro, T. (2013) The Network Secrets of Great Change Agents. *Harvard Business Review*, 91(7) pp. 62-68.
Case: *Evans v. Governor of H. M. Prison Brockhill* (1985) [unreported] Court of Appeal (Civil Division), 19 June.
Citation Guide is available from: https://journals.muni.cz/public/journals/36/download/Citationguide.pdf

Formatting recommendations

Use of automatic styles, automatic text and bold characters should be omitted.
Use of any special forms of formatting, pictures, graphs, etc. should be consulted.
Only automatic footnotes should be used for notes, citations, etc.
Blank lines should be used only to divide chapters (not paragraphs).
First words of paragraphs should not be indented.
Chapters should be numbered in ordinary way – example: "5.2 Partial Conclusions".

Submissions

Further information available at
https://journals.muni.cz/mujlt/about

LIST OF ARTICLES