6th International Conference of
PhD Students and Young Researchers

DIGITALIZATION IN LAW

CONFERENCE PAPERS

03 – 04 May 2018
Vilnius University Faculty of Law
Vilnius, Lithuania

Information about the Conference:

Venue: Vilnius University Faculty of Law, Vilnius, Lithuania

Date: 03 – 04 May 2018

Scientific Committee of the Conference:

- Part. Prof. dr. Ramūnas Birštonas, Faculty of Law, Vilnius University
- Prof. dr. Tomas Davulis, Dean of the Faculty of Law, Vilnius University
- Dr. Donatas Murauskas, Faculty of Law, Vilnius University
- Assoc. Prof. dr. Vigita Vėbraitė, Faculty of Law, Vilnius University

Conference Papers Edition composed by

- Karolina Mickutė, Faculty of Law, Vilnius University
- Ieva Marija Ragaišytė, Faculty of Law, Vilnius University
- Assoc. Prof. dr. Vigita Vėbraitė, Faculty of Law, Vilnius University

ISBN 978-609-459-986-6 (PDF)

FOREWORD BY THE ORGANISERS

We are delighted to present you already the sixth edition of international conference papers of the PhD students and young researchers. This year once again the international conference has been devoted to very live and challenging and many different ideas raising topic “Digitalization in law”. Digitalization is a cross - cutting, interdisciplinary phenomenon and it is obvious that there is also a strong need for action regarding digitalization in law. Even though the legal field is undergoing a transformation and lawyers are beginning to show interest in incorporating technology into practice, till now there is not much research on digitalization in law.

Themes of papers span from algorithms in decision making to the legal aspects of digital economy; from cybercrimes to the right to be offline; from protection of personal data to online dispute resolution. This shows that all aspects of law are influenced nowadays by the digitalization and such influence will be felt more in the years to come. Conference papers are presented by PhD students and young scholars from Belgium, Brazil, Denmark, France, Germany, Italy, Latvia, Lithuania, the Netherlands, Poland and Spain. This shows that in 2014 established International Network of Doctoral Studies in Law by Vilnius University Faculty of Law, Frankfurt am Main J.W. Goethe University Faculty of Law, Paris Nanterre University Faculty of Law and Lodz University Faculty of Law and Administration already created an international platform to develop academic and scientific activities, to enhance quality of doctoral studies in law and to help the interchange of information and ideas among PhD students and professors.

We hope that while we wait for the next year conference, this edition of papers will be a perfect way to deepen knowledge in many relevant aspects of digitalization in law and influence of technologies for different aspects of life for students, scholars and practitioners in different fields of interest.

TABLE OF CONTENT

DISPARITY BETWEEN CURRENT LEGAL FRAMEWORKS AND DIGITAL TRANSFORMATION DEVELOPMENT IN GCC STATES

Al Aridi Alaa[1]

Abstract

The use of digital technology and the race between states in the digital transformation era has resulted rapid growth in this technology albeit variations between countries due to their economic and technological capabilities. According to Gartner Inc. the world by 2016 had 6.4 billion connected devices, and by 2020 this number will reach 21 billion. Such transformation offers wide range of development opportunities at the same time increase the states' vulnerability to cyber-crimes and cyber-attacks if not supported by strong legislative and cyber defense regulations and instruments, as traditional cyber strategies are no longer effective.

Rapid growth in digitalization across the globe has been noticed especially in GCC states that invested heavily in technology following the governments' plans to diversify the regions hydrocarbon-dependent economy, for e.g. Smart Dubai, vision 2030 KSA, e.oman. But at same time it has made those states an attractive target to security breaches. This paper will focus on the effectiveness of legal and enforcement measures, as well the cooperation and harmonization between GCC states to combat cyber-crimes especially when it comes to the cyber threats or attacks on critical infrastructures and GCC's collective self-defense measures to armed attacks. Moreover it will shed the light on International and regional agreements such as the Budapest Convention and the Arab Convention on Combating Information Technology Offences.

Keywords: Cyber security, Cyber-crime law, GCC

Introduction

Globally, companies and governments are embracing technologies such as Internet of Things (IoT) , big data , cloud and mobility, sensing that digital age has begun to change how we work and operate, therefore we are currently witnessing once in a life time digital transformation in every industry and business in an unexpected pace. Our infrastructure control systems become more digitally connected, by which companies now can control and monitor everything from nuclear reactors to small building meters remotely. This rapid evolution in technology forced changes across industries; not only in the way they work and operate but also in the way they protect information and systems from security breaches. Gartner Inc. estimated that by 2020 the world will have 21 billion connected devices, while International Business Machines (IBM) predicting 30 billion autonomously connected devices by the same year. All fields of operational technology, industrial automation and control systems of critical and national infrastructures such as power plant, oil and gas is becoming more and more connected to networks.

The digital transformation is opening the door for more investment opportunities where states are competing to develop digital capabilities to boost the economy and digitalize their infrastructure, enabling industries to cut costs and replace manpower. Digitization boosts the engagement of customers, empowerment of employees, optimization of operation and reinvention of products or services[2]. However, as technology leads and laws follow, the latter have to change in order to conform to the new technology.

It is clearly noticed that recently cyber-attacks are increasing in sophistication by being more asymmetric, anonymous and unpredictable with transnational character at which crimes can be committed and emerge in Internet of Things era. Such challenge assures the need for a comprehensive approach to

[1] *Alaa Al Aridi, Bachelor degree in law and Diploma in International Law and diplomacy From Beirut Arab University, Master Degree in International and EU Law Vilnius University, currently a PhD candidate, faculty of Law, Public Law department at Vilnius University, Dissertation: "The Problem of Hybrid War in International Law." Email: Alaa_G_Aridi@hotmail.co.uk*

[2] 'Research shows surging GCC investment in digital transformation' [01 March 2018] Press release Thomson Reuters ZAWYA https://www.zawya.com/mena/en/story/Research_shows_surging_GCC_investment_in_digital_transformation-ZAWYA20180301094311/.

cyber security requiring a systematic development, interpretation and application of legal areas[3], and instruments covering areas of information's society and telecommunication, cyber-crime and national security that can be breached by attacks reaching the intensity of armed ones. Moreover, According to Tallinn Manual: "Technology has outpaced the law or at least full understanding of how extent law governs emerging cyber capabilities"[4]. In this matter, *Lex Informatica* that has evolved based on sets of rules on information flows imposed by technology and information networks requires full understanding of technology to enforce and establish an acceptable balance[5].

Gulf Cooperation Council States (GCC States) Digitalization Plans

Rapid Growth in digitalization across the globe has been noticed particularly in Gulf cooperation council states hereinafter "GCC states" (KSA, UAE, Qatar, Kuwait, Bahrain and Oman) though in different levels. Ambitions by these states for digital transformation based on short and long term plans such as Smart Dubai and the UAE ICT 2021 strategy that includes the application of rapid adoption of new disruptive technologies across sectors[6]. The Saudi Arabia's national transformation plan 2020 (NTP), as well as Vision 2030 KSA[7], E.oman and the Kuwaiti e-government program as well as others to comply with diversification plans of GCC economies to reduce their reliance on hydrocarbons sector[8], expansion of the region's digital capabilities, smart infrastructure networked devices and high level of internet and mobile penetration by which 76% of GCC population are internet users[9]. Cities such as Dubai in particular position itself among the world's first smart cities using wide ranging smart technology. Smart cities are the cities that use smart technologies, data analysis and innovation to improve the quality of life, services and competitiveness while it ensures it meets the needs of present and future generations with respect to economic, social, environmental and cultural aspects[10]. Recent surveys showed that 68% of the GCC companies will invest 5% of their revenues in digital transformation in 2018, especially in cloud computing, internet of things or industry 4.0, business intelligence as well as robotics[11].

This article will give an overview of the GCC approach to digital transformation, and then will highlight the gaps in current laws, as well the importance of regional and international cooperation to encounter cyber threats in digital transformation era with main focus on the vulnerability of critical infrastructure to cyber-attacks and concluding with recommendations.

Challenges and Overview

A region that is enjoying a rapid digital transformation does not come without consequences and challenges. According to Mohit Shrivastava, a senior analyst for information security at consultant Markets & Markets: "The rapid adoption of digitalization in the UAE and the GCC countries has made the region an attractive target for a wide array of security breaches"[12]. As digital transformation is in an increasing pace, the emerging threat of cyber-attacks is growing, while traditional cyber defense strategies are no longer effective especially when it comes to the emerging threat vectors and speed of change imposed by digital revolution[13]. In this matter, GCC states have experienced numerous amount of malicious cyber-attacks by which for example 58% of Saudis have experienced cyber-crimes, a rate 10 % points above the global average[14]. Moreover, United Arab Emirates is placed at the fifteenth position as a victim of

[3] E. Tikk, 'Comprehensive legal approach to cyber security' (Tartu: University press 2011).
[4] Tallinn Manual, p. 116.
[5] E. Tikk, *Ibid*., p. 13.
[6] E. Durou and S. Nazir, 'National Transformation in the Middle East "A Digital journey"' [2017] Deloitte & Touche, pp. 16-17.
[7] 'Saudi Arabia Vision 2030'. http://vision2030.gov.sa/en.
[8] J. Hakmeh, 'Cybercrime and the Digital economy in the GCC countries' [June 2017] Chathamhouse publications, p. 1.
[9] ITU, 'Measuring the information society Report 2016', ITU, pp. 240-247, www.Itu.int. Accessed March 2017.
[10] E. Durou and S. Nazir, *Ibid*., p. 53.
[11] 'Research shows surging GCC investment in digital transformation', *Ibid*.
[12] M. Habboush, G. Ackerman and M. Riley, 'Hack of Saudi Arabia exposes Middle East Cybersecurity Flaws' (Bloomberg December 2016).
[13] 'Cyber Resilience in the Digital Age, Implications for the GCC region' [2017] EY, p. 5, http://www.ey.com/Publication/vwLUAssets/ey-cyber-resilience-inthe-digital-age-implications-for-the-gcc-region/$File/ey-cyber-resilience-inthe-digital-age-implications-for-the-gcc-region.pdf.
[14] 'Cybercrimes hit 6.5m in kingdom last year' [11 August 2016] Arab News, www.arabnews.com/node/967966/saudi-arabia.

cyber-attacks due to the high density of established commercial and government organizations in the country. Such attacks have targeted previously critical infrastructure in KSA, such as the Shamoon (W32.disttrack) the aggressive disk-wiping malware that targeted Saudi energy sector Aramco 2012, and the ransomware attack on the NHS , as well the region was alerted by the Muddywater attack and more widely publicized WannaCry ransomware attack by 2017 that infected more than 200K computers in more than 150 countries; all these incidents obliged people, businesses and governments to start taking cybersecurity issues into action.

GCC states have taken cybersecurity concern seriously on board since 2006, states have reacted by investing heavily in the cybersecurity market that will be estimated to grow to over than 10.41 bl. $ by the end of 2022 according to a 2016 report BIS research[15] . More challenges will occur by the time the world's largest Oil company (ARAMCO) prepares for what likely to be the largest *Initial Public Offering* (IPO) of all time to attract investors around the globe. IPO will seek to diversify the Saudi economy and use the outcome of the sale to develop and underwrite modernization efforts. ARAMCO which is considered critical infrastructure might be targeted by Malware such as Triton the most difficult attribution cases that failed but was the first to attack safety systems to a critical infrastructure. Similar attacks have also been penetrated against a nuclear plant in South Korea in 2014[16], and in 2016 causing a massive power outage in the Ukrainian city of Kiev- Ukraine[17], noting that such attacks on vulnerable targets can cause casualties and losses that cross by its intensity the threshold of an armed attack.

Important to note that, Technology is not the main line of defense of an organization in cyber sphere, investments in technology is not the solution to keep the states safe from cyber-attacks. Nobody should use or develop a product or service without sufficient attention for the mandatory pervasive legal framework of digitization, by which digital law has become Chefsache[18]. Lack of laws against cyber criminals is what is deterring the industry from making solid progress, focusing on the vulnerability of critical infrastructure that face high risks of more sophisticated cyber-attacks in the emerging Internet of Things (IoT) era. Therefore and according to UNESCWA, proposing legislative measures, developing methods and mechanism to enforce laws, promoting presence of an adopt judiciary and enhancing regional and international cooperation are some of main tasks governments need to accomplish[19].

Overview of cyber security laws in GCC states

The Gulf Region is a lively cyber conflict zone, by which KSA and UAE are the most targeted MENA countries according to Symantec's annual internet security threat Report[20]. Generally, cybercrimes legislations aim to define what acts constitute offences based on *the No Crime without Law* Principle, as well as a balancing tool for society needs for security, privacy and freedom of speech[21].In the same sense, All GCC have cyber-crime laws focusing on criminalization of such actions, but don't extend to other areas of law such as procedural power and international cooperation which are cardinal to legislations being fit for purpose. Therefore no legal regulatory part to enforce laws such as that found in UK and USA which has regulations to empower authorities and organizations. In this matter, Faisal Al Bannai, CEO of UAE-based DarkMatter, emphasizes the need for a new approach to cybersecurity, and stresses that "The

[15] 'GCC Cyber Security Market: Focus on Solutions (Network Security, Endpoint Security & Others), Services (Consulting, Risk Assessment, and Others), Application (BFSI, Telecommunication & Others) – Estimation & Forecast, 2016' [2016] BIS Research, https://bisresearch.com/industry-report/gcc-cyber-security-market-research-report-forecast-629.html.

[16] J. McCurry, 'South Koream Nuclear operator hacked amid cyber-attack fears' [December 2014] The Guardian.

[17] A. Greenberg, 'Crash Override: The Malware that took down a Power Grid' [6 December 2017] www.wired.com.

[18] V. A. de Pous, 'Legal Framework for Digital Transformation increases confidence in information society' [February 2017], Cloud Community Europe Netherlands, p. 5, http://www.cloudcommunityeurope.org/documents/2017/06/legal-framework-for-digital-transformation-increases-confidence-in-information-society.pdf.

[19] UNESCWA, 'Policy recommendations on Cyber Safety and combating cyber-crimes in Arab region' [2015].

[20] 'Symantec Annual Internet Security Threat Report' [April 2017] Symantec Volume 22, https://digitalhubshare.symantec.com/content/dam/Atlantis/campaigns-and-launches/FY17/Threat%20Protection/ISTR22_Main-FINAL-JUN8.pdf?aid=elq_12438.

[21] United Nations Office on Drugs and Crime (UNODC), 'Comprehensive study on Cybercrime' [Draft – February 2013], p. 53.

prevalence of the energy sector in the region, and the rapid digital transformation of critical national infrastructure has brought with it an increases attack surface for utility companies [22]".

Cyber legislation activities were introduced firstly by the Kingdom of Bahrain with Law 28/2002 on e-Transaction[23] including articles related to cyber-crimes and then new cybercrime law in 2015 countering illegal access to IT systems. Similarly, Kuwait issued a law No. 63/2016 cyber-crime law stating punishments for illegal access to computers and information systems or network, or actions illegally acquiring confidential personal/government data and which contains provisions that severely restrict freedom of expression on the internet. On the other hand, the UAE has the most detailed and comprehensive cyber-crime law in the region which is concerning combatting IT crimes, the UAE law No.5/2012 replaced the earlier combating cyber-crimes law 2006[24] , this law was later expanded to ensure alignment between UAE legislation and International Treaties such as Budapest Convention on Cyber-crime[25]. Important to note that Honeywell Company has established the first industrial cyber security of excellence (COE) at its middle east HQ in Dubai, aiming to strengthen cyber security defenses amidst growing digital transformation across industries. Moreover, Kingdom of Saudi Arabia issued a law addressing electronic transactions 2007, followed closely by a similar law in the Sultanate of Oman in May 2008. On the other hand, Qatar issued the electronic transaction law issued in 2010[26], followed by an Anti-Cybercrime law in recognition of the growing problem of cyber threats in the region. Qatar has as well launched the *National Cyber Security Strategy (NCSS)* in support to its efforts to address current and emerging threats, risks and to protect the national critical information infrastructure by providing safe and secure online environment for different sectors[27]. One of the main objectives is to establish a legal and regulatory framework to enable a safe and vibrant cyber space[28] by increasing capabilities to combat cyber-crimes, develop and implement laws, regulations and national policies to address cyber security and cyber-crime, monitor and enforce compliance with cybersecurity and cyber-crimes, and most important is build and maintain strong international relationships to establish cyber security norms and standards[29]

However, laws related to cyber security are being gradually implemented but many of them are vague and ineffective to combat cyber-crimes generated on daily basis and transnationally, as such laws are implemented to tackle internal threats. In KSA as an example, there is lack of legal entity to notify breaches occurring by leaving it to the courts to litigate cases based on general Sharia principles[30]. While some other laws such as UAE criminalize acts that are conducted by organizations threating the national security but in a broad term, for example Article 46 that states the following: "The use of the computer network, the Internet, any electronic information system, a website or any information technology means shall be considered an aggravating factor when committing any crime not specified by the present Decree-Law. Shall also be considered as an aggravating factor the commission of a crime specified in this Decree-Law to the account or benefit of a foreign country or any terrorist group, or illegal group, association, organization or body."[31] UAE Federal law 5/2012 broadened the range of offences, definition of privacy violation and monetary penalties, with strict laws against cybercrimes and fines of up to 900 thousand $[32]. While none of the Penal Code, Cyber-crimes law or data protection law contains a definition of Cybersecurity or cybercrime[33].

[22] N. King, 'Taking on the GCC's Cyber Criminals' [January 2018] Gulf Business, http://gulfbusiness.com/taking-gcc-cyber-criminals/.
[23] 'LEGISLATIVE DECREE NO.28 of 2002 WITH RESPECT TO ELECTRONIC TRANSACTIONS' [14 September 2002].
[24] UAE Federal Decree Law No (5) of 2012 On Combating Cybercrimes, abrogating: Federal law no.2/2006 dated 3/1/2006.
[25] N. Purin, 'Cyber threats in the GCC, Building legislative defense shields' [March 27, 2017] Executive.
[26] UNESCWA, 'The ESCWA Cyber Legislation Digest, Regional Harmonization to promote knowledge society in the Arab region' (New York: United Nations 2013) pp. 3-4.
[27] Qatar National Cyber Security Strategy, Ministry of Transport and Communication [May 2014], www.ictqatar.qa.
[28] *Ibid*., p. 9
[29] *Ibid*., p. 11
[30] A. Unwala, 'The Risks and Rewards of Digitizing the Middle East' [2 June 2017] Special Report.
[31] UAE Federal Decree Law No (5) of 2012 On Combating Cybercrimes, *Ibid*.
[32] M. Imranuddin, 'A study of Cyber Laws in the United Arab Emirates' (The Rochester Institute of Technology 2017) pp. 47-48.
[33] B. Hopps and S. Paterson, 'Herbert Smith Freehills' [January 2018] Cyber Security United Arab Emirates.

Saudi Anti-Cybercrimes Law that was issued by Royal Decree M/17 at 26th of march 2007 aims at combating cyber-crimes by identifying such crimes and determining their punishments to ensure information security, safeguards rights on the legitimate use of computers and information networks, protection of public interest and morals, as well protection of national economy[34]. While this law is designed to protect users from cyber-crimes, it also contains clauses that limit freedom of expression. For example, the ACCL criminalizes "producing something that harms public order, religious values, public morals, the sanctity of private life, or authoring, sending, or storing it via an information network"[35]. It seems that such laws includes the protection of critical infrastructure such as ARAMCO, however it lacks the regulations that can get along with the new technologies, such laws issued in 2007 were not updated to cover the new era of IoT and digital transformation. And in recent incident, Cyber criminals in 2016 attacked various departments of Saudi governments including Saudi Authority of civil aviation, destroying thousands of computers in the Saudi air office with the so called "Digital Bomb"[36]. However, King Salman issued in 2017 several royal decrees aimed to centralize authority in cyber security, counter-terrorism and domestic intelligence as majority of security institutes and ministries develop their own rules and infrastructures ,as well as their own security systems and measures with little central coordination[37]. This puts the country on a stake of more cyber threats that can invest gaps in non-centralized and coordinated cyber defense strategies.

In an overview of the regions legal framework to cyber-crime laws it is clear that laws are inadequate, undeveloped and not fully implemented with no common approach in GCC. Difference in the substance of cybercrimes including the very definition of cybercrime poses problems for global policy coordination. The mentioned laws set out punishments for respective crimes but don't have any obligatory measures for companies to implement protective measures against cyber-crimes. Although regulations and strategies been implemented focusing on cyber security resilience however lack of harmonization is a key problem, GCC lacks overarching regulatory body or legislative framework that applies unilaterally across all member states of the GCC, as each jurisdiction has a slightly different mechanism for detecting and criminalizing cybercrime[38]. Moreover, GCC states lacks data protection laws except in Qatar that issued legislation by way of law No.13/2016 on personal data privacy. And it is recommended for GCC to follow the same practice of the European Union that introduced the General Data Protection regulations (GDPR) which will come into force in May 2018 by placing stricter obligations on those handling data EU citizens, and we have heard about how important and thorough this law during the hearings of Mark Zuckerberg Facebook CEO before the House of Committee on commerce and energy, how he is willing to extend European Data Protections Worldwide[39].

GCC states have been investing heavily in digital transformation especially in critical infrastructure such as transportation, communication, health sector and oil amidst all the cyber threats in the region, increase in tension with Iran and border conflicts in Yemen. Cyber-attacks are in increasing pace, taking into consideration that GCC is considered as well as a regional security organization due to the common interest of its member states. What isn't frequently focused on is the impact of cyber-attacks to critical infrastructure, while it is very important as hackers aim for different goals and risks have much higher consequences on human life than normal data breach.

At the Manama- Bahrain summit in December 2000, the member states concluded the GCC Joint Defense Agreement in order to provide a framework for collective defense based on the principle that any aggression against a member state would be considered against all the GCC states[40], therefore any attack against critical infrastructure could cause an armed conflict triggering self or collective self-defense,

[34] M. Amrutha, 'Saudi Arabia Cyber Crime Laws' [August 2017] STA Law firm blog, www.stalawfirm.com.
[35] M. Hathaway, F. Spidalieri and F. Alsowailm, 'Kingdom of Saudi Arabia Cyber Readiness at a Glance, Cyber Readiness Index 2.0' [2017] Potomac Institute for Policy Studies, p. 15.
[36] M. Amrutha, 'Saudi Arabia Cyber Crime Laws', *Ibid*.
[37] M. Hathaway, F. Spidalieri and F. Alsowailm, 'Kingdom of Saudi Arabia Cyber Readiness at a Glance, *Ibid*., pp. 6-7.
[38] R. Kelly and D. McDonald, 'Managing Cyber Risks' [July/August 2017], www.morganlewis.com, p. 25.
[39] S. Jeong, 'Zucherberg says Facebook will extend European Data protections worldwide' [11 April 2018], https://www.theverge.com/2018/4/11/17224492/zuckerberg-facebook-congress-gdpr-data-protection.
[40] C. Koch, 'The GCC as a Regional Security Organization' [2010] KAS International Reports, p. 28.

However GCC military integration and interoperability remains limited[41]. Recent cyber security events clearly points out that abilities for large scale attacks on critical infrastructure have grown dramatically, by which previously such infrastructures were isolated and based on operational safety, however with development of "IoT" or Industry 4.0 it is important to maintain the continuity and timeliness of the defensive measures parallel to the rapid transformation of industry[42]. At UAE there are no laws or regulations that specifically address cyber threats to critical infrastructure or specific sectors as well lacks industry standards or code of practice on cybersecurity, however many organization adopted voluntary *ISO 27001* and in compliance with ISO the National Electronic security Authority (NESA) produced set of standards and guidance for government entities in certain critical sectors[43]. In addition, sharing information with competent authorities regarding cyber threats or crimes is not framed by law, set of guidance or procedures but made voluntary, although failure to report a crime in the UAE could bring penalties under the Penal Code. UAE is taking cybersecurity issues seriously but the challenge of the development of cybersecurity regulations is the long lead time for new laws to become enacted and to follow the digital transformation and criminal new methods[44]. A lesson can be learned for example from the UK as the department of digital, culture, Media and Sports (DCMS) warns that organization risks fines of up to 17 Million Pounds if they don't have effective cyber security measures in place especially when it comes to Critical infrastructure[45]. GCC shall address this issue and adopt regulations and directives that specify the critical infrastructure of the states and harmonize their efforts against cyber-attacks that might target GCC's essential infrastructure. GCC cyber center for excellence can be launched to monitor, regulate and direct this process.

Harmonization and International Cooperation of GCC states

The transnational character of cyber-attacks, anonymity and high speed at which crimes can be committed requires regional and international cooperation and harmonization to tackle such threats. Policy makers and academics have invested all their efforts to study the nature of cyber-attacks and avoid the problem of attribution due to its complexity in an interconnected world. This challenge has evolved with the digital transformation era and has been noticed as a main challenge to the GCC states. For example all GCC states are signatory of the Arab convention on combatting information technology offences 2010 that is being criticized for vague and inadequate definitions , however none of the GCC cyber-crime laws mentioned the rules of this agreement, despite the fact that article 1 of chapter V of the convention stipulates that competent authorities shall take the domestic procedures necessary for the implementation of this convention, therefore coordination between the member states to the convention remain ineffective[46]. Additionally, Saudi Arabia is not a party to nor is in the process of joining any of the global anti cyber-crime agreements, like the Council of Europe's "Convention on Cybercrime" (the Budapest Convention) which came into effect on 1 July 2004, is a key regional treaty aimed at harmonizing national cybercrime legislation, building national capabilities to investigate cybercrime and strengthening cooperation in this field[47]. Similarly, KSA is not party to the Shanghai Cooperation Organization's (SCO) "Agreement on Cooperation in the Field on Ensuring International Information Security." As Cooperation is a key element to combat cyber threats, I agree with Joyce Hakmeh that regulatory, legal and technological tools need to be developed collective and updated on a continuous basis especially within the digital transformation era[48]. While GCC is not party to any international Anti-Cybercrime agreements such as Budapest Agreement, therefore it is required from the GCC states to engage in international police and judicial cooperation by signing the Budapest convention. Alternatively, as mentioned before

[41] M. Wahba, 'GCC: A Force for Regional Stability' [February 2017] The Cipher Brief, www.thecipherbrief.com/gcc-a-force-for-regional-stability.
[42] I. Koese, 'Critical infrastructure and Industry 4.0: The View is missing for the Whole' [August 2017], www.CSPI.com.
[43] B. Hopps and S. Paterson, 'Herbert Smith Freehills', *Ibid*.
[44] *Ibid*.
[45] E. Boiten, 'Critical Infrastructure firms face crack down over poor cybersecurity' [January 2018] The Conversation.
[46] J. Hakmeh, 'Cybercrime and the Digital Economy in the GCC Countries' [June 2017] Chatham House.
[47] Escwa, 'Policy recommendations on Cybersafety and Combating Cybercrime in the Arab Region' (New York 2015) p. 2.
[48] J. Hakmeh, *Ibid.*, p. 9.

GCC states are member states of the Arab Convention on combating information technology offences [49], but the convention has not been formally activated and coordinated between its member states due to political and domestic interests and concerns. While GCC intra cooperation relies on bilateral relationships such as police to police agency (KSA_KUWAIT) or agency to agency cooperation[50]. But practice proved that there is also a consensus on the need for solid cooperation mechanisms at national, regional and international level, that unfortunately it won't be seen in the near future due to the intra-state tensions especially between majority of GCC states and Qatar. Moreover, most GCC cybercrime laws do not provide an adequate legal framework for cooperation, nor do they include clear procedural provisions for implementation[51]. GCC states could rely on the United Nation conventions against transnational organized crimes (UNTOC) that provides broad scope of international cooperation, which could in some cases establish platform for international cooperation , however main objectives should be protecting national's interest from cyber threats, at same time take into consideration the respect of Human rights such as privacy, access to information and freedom of speech, especially that it has been noticed that some cybercrimes laws are addressed in a broad term and could constitute restrictions on human rights. This has been explicitly stated by the UN human rights council resolution 20/8 that same level of protection should apply to the online realm as to the offline ones[52]. GCC states should adopt directives similar to the Security of Network and Information System (NIS directive) that was adopted by the EU parliament in July 2016 where states were given 21 months for national implementation and 6 months to identify operators of essential services[53]. Cooperation and harmonization between states by addressing the effectiveness of legal and enforcement measures to combat cyber threats and GCC states must move forward towards that more than ever.

Conclusion

Digital transformation is occurring in a rapid pace and evolving in all sectors; states are investing heavily in technologies to follow this digital evolution; however such transformation doesn't come without consequences as the cyber-attacks are increasing at same and even more rapid levels. GCC states have been witnessing a digital transformation along with plans to diversify their economy, but this digital evolution is not followed with adequate and comprehensive legal and regulatory approach. Cyber-crime laws that are introduced in all GCC states and being gradually implemented many of them are vague and ineffective to combat cyber-crimes especially that none of the Penal Code, Cyber-crimes law or data protection law contains a definition of Cybersecurity or cybercrime.

Moreover, laws focus on criminalization of cyber-crimes without any regulations to ensure full compliance of organizations and companies to take all necessary measures to combat cyber threats. On the other hand, The increase of interconnectivity and information exchange is followed by an increase in cyber vulnerabilities especially for Critical infrastructure as the most essential for the state's security, however the regions legal framework to cyber-crime laws are inadequate, undeveloped and not fully implemented with no common approach at GCC Level. Difference in the substance of cybercrimes including the very definition of cybercrime poses problems for global policy coordination. Lack of harmonization due to political reasons has its negative impact on the regions cyber security and implementation of The Arab Convention as well the understanding and accession to Budapest Convention will be the right step. GCC states in order to tackle the disparity between the digital transformation and legal frameworks, more adequate and developed legislations must be updated and adopted taking into consideration that such laws must not violate the freedom of expression and human rights. Cyber-attacks

[49]'Arab Convention on Combatting Information Technology offences' [2010], http://www.lasportal.org/ar/legalnetwork/Pages/typicalarablaws.aspx (in Arabic).
[50]J. Hakmeh, *Ibid*., p. 12.
[51]*Ibid*., p. 13.
[52] UN Human Rights council resolution 20/8, on "the promotion, protection and enjoyment of human rights on the internet'" [29 June 2012] A/HRC/20/L.13, United Nations General Assembly, https://documents-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement.
[53]E. Boiten, *Ibid*.

and crimes are one of the means used by adversaries to destabilize any order, and meanwhile such threats are imposed by Hybrid forms to achieve political gains, and with laws that don't fully cover all aspects of cybersecurity and impose regulations on organizations and companies to take all necessary measures to protect infrastructures from such threats, states will be facing malicious attacks and threats that can lead to worse scenarios.

Bibliography

1. M. Amrutha, 'Saudi Arabia Cyber Crime Laws' [August 2017] STA Law firm blog, www.stalawfirm.com.
2. 'Arab Convention on Combatting Information Technology offences' [2010], http://www.lasportal.org/ar/legalnetwork/Pages/typicalarablaws.aspx (in Arabic).
3. E. Boiten, 'Critical Infrastructure firms face crack down over poor cybersecurity' [January 2018] The Conversation.
4. 'Cyber Resilience in the Digital Age, Implications for the GCC region' [2017], EY, p. 5, http://www.ey.com/Publication/vwLUAssets/ey-cyber-resilience-inthe-digital-age-implications-for-the-gcc-region/$File/ey-cyber-resilience-inthe-digital-age-implications-for-the-gcc-region.pdf.
5. Cybercrimes hit 6.5m in kingdom last year' [11 August 2016] Arab News, www.arabnews.com/node/967966/saudi-arabia.
6. E. Durou and S. Nazir, 'National Transformation in the Middle East "A Digital journey"' [2017] Deloitte & Touche
7. Escwa, 'Policy recommendations on Cybersafety and Combating Cybercrime in the Arab Region' (New York 2015).
8. GCC Cyber Security Market: Focus on Solutions (Network Security, Endpoint Security & Others), Services (Consulting, Risk Assessment, and Others), Application (BFSI, Telecommunication & Others), Estimation & Forecast, BIS research report 2016.
9. A. Greenberg, 'Crash Override: The Malware that took down a Power Grid' [6 December 2017], www.wired.com.
10. M. Habboush, G. Ackerman and M. Riley, 'Hack of Saudi Arabia exposes Middle East Cybersecurity Flaws' (Bloomberg December 2016).
11. J. Hakmeh, 'Cybercrime and the Digital economy in the GCC countries' [June 2017] Chathamhouse publications.
12. M. Hathaway, F. Spidalieri and F. Alsowailm, 'Kingdom of Saudi Arabia Cyber Readiness at a Glance, Cyber Readiness Index 2.0' [2017] Potomac Institute for Policy Studies.
13. B. Hopps and S. Paterson, 'Herbert Smith Freehills' [January 2018] Cyber Security United Arab Emirates.
14. M. Imranuddin, 'A study of Cyber Laws in the United Arab Emirates' (The Rochester Institute of Technology 2017).
15. ITU, 'Measuring the information society Report 2016', ITU, pp 240-247, www.Itu.int. Accessed March 2017.
16. S. Jeong, 'Zucherberg says Facebook will extend European Data protections worldwide' [11 April 2018], https://www.theverge.com/2018/4/11/17224492/zuckerberg-facebook-congress-gdpr-data-protection.
17. R. Kelly and D. McDonald, 'Managing Cyber Risks' [July/August 2017], www.morganlewis.com.
18. N. King, 'Taking on the GCC's Cyber Criminals' [January 2018] Gulf Business, http://gulfbusiness.com/taking-gcc-cyber-criminals/.
19. C. Koch, 'The GCC as a Regional Security Organization' [2010] KAS International Reports.
20. I. Koese, 'Critical infrastructure and Industry 4.0: The View is missing for the Whole' [August 2017], www.CSPI.com.
21. 'LEGISLATIVE DECREE NO.28 of 2002 WITH RESPECT TO ELECTRONIC TRANSACTIONS' [14 September 2002].
22. J. McCurry, 'South Koream Nuclear operator hacked amid cyber-attack fears' [December 2014], The Guardian.
23. V. A. de Pous, 'Legal Framework for Digital Transformation increases confidence in information society' [February 2017] Cloud Community Europe Netherlands, p.5,

http://www.cloudcommunityeurope.org/documents/2017/06/legal-framework-for-digital-transformation-increases-confidence-in-information-society.pdf.
24. N. Purin, 'Cyber threats in the GCC, Building legislative defense shields' [March 27, 2017] Executive.
25. Qatar National Cyber Security Strategy, Ministry of Transport and Communication [May 2014], www.ictqatar.qa.
26. 'Research shows surging GCC investment in digital transformation' [01 March 2018] Press release Thomson Reuters ZAWYA https://www.zawya.com/mena/en/story/Research_shows_surging_GCC_investment_in_digital_transformation-ZAWYA20180301094311/
27. Saudi Arabia Vision 2030'. http://vision2030.gov.sa/en.
28. 'Symantec Annual Internet Security Threat Report' [April 2017] Symantec Volume 22, https://digitalhubshare.symantec.com/content/dam/Atlantis/campaigns-and-launches/FY17/Threat%20Protection/ISTR22_Main-FINAL-JUN8.pdf?aid=elq_12438.
29. E. Tikk, 'Comprehensive legal approach to cyber security' (Tartu: University press 2011).
30. UAE Federal Decree Law No (5) of 2012 On Combating Cybercrimes, abrogating: Federal law no.2/2006 dated 3/1/2006.
31. 'UN Human Rights council resolution 20/8, on "the promotion, protection and enjoyment of human rights on the internet"' [29 June 2012] A/HRC/20/L.13, United Nations General Assembly, https://documents-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement.
32. UNESCWA, 'The ESCWA Cyber Legislation Digest, Regional Harmonization to promote knowledge society in the Arab region' (New York: United Nations 2013).
33. UNESCWA, 'Policy recommendations on Cyber Safety and combating cyber-crimes in Arab region' [2015].
34. United Nations Office on Drugs and Crime (UNODC), 'Comprehensive study on Cybercrime' [Draft – February 2013].
35. A. Unwala, 'The Risks and Rewards of Digitizing the Middle East' [2 June 2017] Special Report.
36. M. Wahba, 'GCC: A Force for Regional Stability' [February 2017] The Cipher Brief, www.thecipherbrief.com/gcc-a-force-for-regional-stability.

ADMINISTRATIVE ALGORITHMIC DECISION-MAKING

Annequin Vincent[1]

Abstract

The growing use of artificial intelligence and algorithms in many fields of activity offers hope for a better functioning of our society, but also represents a significant danger. Hope, because computer algorithms must result in a greater rationality, a greater security and a better allocation of resources. But danger, because these relatively vain wishes would come true especially if the construction and the use of these computer tools are virtuous. Indeed, it has already been demonstrated many times that artificial intelligence could only repeat or increase the current inequalities.

It is accepted that algorithms are already an integral part of the legal field, whether algorithms are used by judges, lawyers or even litigants. For these reasons, this study will focus on the emerging but rapidly developing practice of algorithmic decision-making by the Administration. This phenomenon raises many questions that are essential for jurists, especially regarding the protection of citizens facing this Administration boosted with algorithms (personal data, discriminations...). Other issues rely more on the very nature of the administrative decision: who is the real author of this administrative algorithmic decision? Is it legitimate to entrust decisions aimed at the general interest and the common good to artificial intelligence?

To address these questions, it seems necessary to study the importance of the algorithm type to evaluate its impact on the administrative decision, but also the current administrative algorithmic decision's main problems and framework. The study will focus notably on French and European law, which are going through huge changes on this subject at the time.

Keywords: Digitalisation, algorithms, administrative decisions, public law, personal data.

Introduction

"Technological evolution shifts the boundary between the possible and the impossible, and requires to redefine the boundary between the desirable and the undesirable".[2] This is a quote from the French administrative authority regulating data protection's last report on the ethical use of artificial intelligence and algorithms.[3] This is a serious message, but this affirmation has a stronger meaning for the public administration, particularly regarding the administrative algorithmic decision-making, which is a pure expression of the Administration's power.

Despite this ambivalence, it is clear that the public authorities are increasingly using this computer tool, whether in Europe[4] or in the rest of the world.[5] Since the development of the administrative algorithmic decision seems inevitable, how is it possible to support this process so that the administrative algorithmic decision can be virtuous? Obviously, one must question the scope of the concept of "virtue" in this context. As part of the administrative decision, it would mean for the Administration to pursue a general interest's objective (for example the proper operation of the legal system), while infringing as little as possible on citizens' rights (for instance the right of protection of personal data). Indeed, the public action is crossed by this research of a balance between the public interest and the private interests of each individual.

---

[1] *PhD candidate in Public Law, Université Paris Nanterre, Centre de recherche en droit public (CRDP). Dissertation's topic: "Service public et intelligence artificielle" [Public service and artificial intelligence]. Research Interests: Public Law, Public Procurement Law, Digital Law. Email: vincent.annequin@live.fr*

[2] CNIL, 'Comment permettre à l'homme de garder la main? Les enjeux éthiques des algorithmes et de l'intelligence artificielle' [2017] p. 24.

[3] *Ibid*.

[4] See for example La Republicca, 'Scuola, continuano le proteste dei docenti. Giannini: "Ci stiamo occupando della mobilità"' [2016], http://www.repubblica.it/scuola/2016/08/08/news/scuola_giannini_proteste_docenti_mobilita_-145605988/.

[5] A. Liptak, 'Sent to Prison by a Software Program's Secret Algorithms' [2017], https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html.

In addition, it is also necessary to settle on a definition of algorithm. Not to mention the genesis of its name[6], an algorithm, "as the word is used today, can be summarised as a computable set of steps to achieve a desirable result".[7] The current interest of computer scientists explains why this notion is generally taken only under the sole prism of computer science. Therefore, it is the computer algorithm that will be discussed in this contribution, an algorithm written in the form of a source code, so that it can be readable and executed by a machine.[8] More precisely, the "Article 29 data protection working party" Guidelines gives a definition of what must be understood by "automated decision-making": "Solely automated decision-making is the ability to make decisions by technological means without human involvement". For instance, "imposing speeding fines purely on the basis of evidence from speed cameras is an automated decision-making process".[9] This example is interesting because it clearly shows how an administrative decision can be taken by an algorithm.

An administrative decision can be defined as the realisation of the Administration's will, through the adoption of unilateral administrative acts that are established themselves. The administrative decision is therefore an important means for the Administration to conduct its activities aimed at the general interest.

In this way, thinking about the administrative algorithmic decision-making must go through the identification of the algorithm on which the Administration relies to make its decisions. Indeed, the characteristics of the algorithm has an impact on this recent mode of decision-making for the Administration and on the recipients of the administrative decision. This preliminary work will study the main problems that have been noticed in the development of administrative algorithmic decision-making, but also the current controls that have been implemented by the French and the European Union law.

1. The impact of the algorithm type on the administrative decision

To understand the growing influence of the algorithm on public law, and more specifically on the administrative decision, it seems important to organise a typology of algorithms. A greater understanding of the impact of the algorithm on the administrative decision will result from this distinction.

First, a preliminary work to identify a typology of algorithms requires a distinction related to the "*nature*" of computer algorithms. At first, it is possible to distinguish the traditional algorithms. Indeed, they are parameterised ahead by computer scientists, humans settle the choice and the weighting of the criteria on which the algorithm will work, and they also choose the data sets to reach the desired result. Therefore, this first type of algorithm is characterised by a strong determinism, their operation and the processed data remain dependent on the will of their creators.

Then, thanks in particular to progress in processing a significant amount of data, (the notion of "Big data" is thus closely linked to algorithmic processing[10]), it has been possible to develop learning algorithms. They use machine learning techniques, one of the fields of study of artificial intelligence. These machine learning techniques are numerous and more or less sophisticated (supervised / unsupervised learning, reinforcement / deep learning, etc.). These techniques have recently allowed artificial intelligence to make remarkable progress.[11] These learning algorithms are defined by their "*probabilism*": if their initial configuration remains crucial, it is especially their functioning which will progressively modify their way of processing the data, and thus the results. Moreover, according to the data processed by the machine learning algorithm, the algorithm will modulate automatically its configuration, including the criteria and their weighting. This is why the relevance of data (in terms of quantity and quality) is so important for machine learning algorithms.

---

[6] S. Brentjes, 'Encyclopaedia of Islam' (Leiden: 2017) pp. 1-7.

[7] *Ibid*.

[8] As a reminder, initially, the notion of algorithm referred to "the art of counting", see J.-B. Duclercq, 'le droit public à l'ère des algorithmes' [2017] Lextenso n°5, p. 1401.

[9] Article 29 data protection working party, 'Guidelines on Automated inidivudal decision-making and Profiling for the purposes of Regulation 2016/679' [2017] p. 8.

[10] For more information on Big Data, see D. Boyd and K. Crawford, 'Six Provocations for Big Data A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society' [2011].

[11] AlphaGo with Go is a famous example, see C. Metz, 'What the AI Behind AlphaGo Can Teach Us About Being Human' [2016] Wired.com, https://www.wired.com/2016/05/google-alpha-go-ai/.

The distinction between these two types of algorithm is not trivial for the administrative algorithmic decision. Indeed, at first sight, it seems more acceptable for citizens that administrative decisions are the result of a traditional algorithm, because it is by nature consistent with the calibration provided by their creators. Therefore, it is very likely to be consistent with the general interest pursued by the Administration.

On the contrary, a machine learning algorithm that adopt directly decision in the name of the Administration is much more questionable, notably for the legitimacy of such administrative algorithmic decision. In fact, artificial intelligence could have developed in a way that do not coincide with the Administration's will. Thus, if the machine learning algorithm does not correspond to the public authorities' wishes, it is highly likely that the algorithmic decision will no longer be compatible with the general interest and the common good. Especially regarding deep learning, there is no systematic technique that always provides a clear explanation for a given decision.[12] This is why machine learning algorithm does not seem compatible at the moment with a public decision-making: it is currently inappropriate for any situation where there is a socially important decision. Consequently, and more generally, a report entitled "*AI now 2017 report*" recommends, that "*core public agencies, such as those responsible for criminal justice, healthcare, welfare, and education (e.g "high stakes" domains) should no longer use "black box" AI and algorithmic systems*".[13] Indeed, "*the use of such systems by public agencies raises serious due process concerns, and at a minimum they should be available for public auditing, testing, and review, and subject to accountability standards*".[14]

Alongside this distinction of computer algorithms according to their nature, it is possible to apprehend them according to their function. Five main functions can be distinguished: algorithms can produce knowledge, allow the meeting of supply and demand ("matching") and the allocation of resources,[15] recommend personalised offers,[16] predict[17] (even if a more relevant term would be "*probabilise*" here) and help or even adopt decisions directly.[18] Of course, the first four functions have a preponderant role in the digital sector today, and may have an important role ahead of any decision. Nonetheless, it is the decision-making function that mostly gathers the issues related to the use of algorithms in the administrative action. Indeed, according to the "Article 29 data protection working party", "*automated decision-making can pose significant risks for individuals' rights and freedoms which require appropriate safeguards*".[19]

2. The main problems of administrative algorithmic decision-making

In this regard, it is generally admitted that the Administration's purpose should be the general interest, the common good, contrary to individuals acting for their own private interest. This is why Administration has generally more power than individuals or private entities and why the following issues potentially caused by algorithmic administrative decisions are even more serious than in the private sphere.

This part of our discussion will linger over the main problems of administrative algorithmic decision-making, since the amount of questions raised by this recent Administration's evolution leads to focus on the crucial ones. For this purpose, the French case of "Admission Post-Bac" (abbreviated "APB"), a digital platform managed by the French Education Administration until 2017, is a good case study. This digital platform was the way for French high school students to enter in postgraduate studies. In summary, during

[12] B. Georges, 'Le talon d'Achille de l'intelligence artificielle' [2017] LesEchos.fr, https://www.lesechos.fr/15/05/2017/lesechos.fr/0212088042490_le-talon-d-achille-de-l-intelligence-artificielle.htm.

[13] A. Campolo, M. Sanfilippo, M. Whittaker and K. Crawford, 'IA now Report 2017' [2017] p. 1.

[14] *Ibid*.

[15] See for example C. Cook, R. Diamond, J. Hall, J. A. List and P. Oyer, 'The Gender Earnings Gap in the Gig Economy: Evidence from over a Million Rideshare Drivers' [2018].

[16] See for example D. Inglod and S. Soper, 'Amazon Doesn't Consider the Race of Its Customers. Should It?' [2016] Bloomberg, https://www.bloomberg.com/graphics/2016-amazon-same-day/?cmpid=google.

[17] See for example M. Benesty, 'L'open data et l'open source, des soutiens nécessaires à une justice predictive fiable?' [2017] Journal of Open Access to Law vol. 5 no. 1.

[18] A. Liptak, *Ibid*.

[19] Article 29 data protection working party, *Ibid*., p. 5.

the last year of high school, they must fill their wishes on the platform. Then, each higher education establishment chose the successful candidates, on the basis of a range of criteria (such as their high school marks or their cover letter). Then, an algorithm used by the French Education Administration organises the final classification on a national level, and determines which candidates are selected for which higher education institution. In this example, the algorithm constitutes the decision's real origin, and in the context of APB, the French Administration had to replace this digital platform by a new one, "Parcoursup",[20] because of the consequences of using an algorithm to adopt an administrative decision.

Indeed, algorithmic decision of the Administration can indicate a lack of transparency regarding its manner of working. For instance, high school students who registered on APB could not know how the algorithm worked and how the decision was taken.[21] Some of them did not even know that an algorithm was choosing their future, because the APB website did not mention it explicitly. Transparency is one of the biggest problem when it comes to using algorithms today. Thus, Members States are exploring today different solutions, such as publishing the source code (that was the case for APB in France[22]), or the development of framework for explaining decisions made by algorithms in the United Kingdom.[23]

Furthermore, the administrative algorithmic decision-making can of course harm the principle of the protection of personal data. On this subject, the Administration behind APB, which organised the entrance in postgraduate studies for more than 800.000 students in 2017, did not specify the obligation regarding the security of personal data to its subcontractor.[24] Furthermore, the institutions offering non-selective training had access to all the data of the candidates who had selected them in their wishes.[25]

So far, in terms of liability in case of malfunctions or damages created by the algorithm, APB is a virtuous example: indeed, the French administrative jurisdiction (the "Conseil d'Etat") have already admitted the State malfunctions for APB in several cases in 2017.[26] But, facing the possibility that several thousands of students could file a plea against the French Education Administration, and in order to let the Government modify the digital platform and the algorithm, the French administrative jurisdiction has postponed the effects of such decisions to 2018.[27] The liability regime in case of algorithmic decision creating a damage is thus far from being decided: Should it be the creator of the algorithm that is designated responsible? Its users? Should we create a joint responsibility? An *ad hoc* scheme?

Especially, when it comes to an administrative decision, the legitimacy of such a decision is a very important question. In the case of APB, the decision was not made by one or more agents of the Administration, but by an algorithm, and without any possibility of submission to an administrative agent. Is it acceptable that an algorithm decides for things as important as academic orientation for several hundred thousand high school students?

In any case, for these problems, whether real or potential, the administrative algorithmic decision has to be regulated. Therefore, the development of artificial intelligence in the administrative sphere is a major challenge for the present and the future of the Administration. The current response in France and in the European Union is the enactment of rules, which are supposed to limit the risks induced by the administrative algorithmic decision.

---

[20] S. Graveleau, 'Parcoursup, la plate-forme qui succède à Admission post-bac, a ouvert' [2018] Le Monde, http://www.lemonde.fr/campus/article/2018/01/15/parcoursup-qui-succede-a-admission-post-bac-ouvre-ce-lundi_5241663_4401467.html?xtmc=parcoursup&xtcr=35.

[21] CNIL, 'Décision mettant en demeure le ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation' [2017] MED-2017-053.

[22] S. Graveleau, 'APB: révélation du code source qui affecte les bacheliers à l'université' [2016], http://www.lemonde.fr/campus/article/2016/10/18/apb-revelation-du-code-source-qui-affecte-les-bacheliers-a-l-universite_5015778_4401467.html.

[23] D. W. Hall and J. Pesenti, 'Growing the Artificial Intelligence Industry in the UK' [2017] p. 5.

[24] *Ibid*.

[25] *Ibid*.

[26] Association SOS Education et association Promotion et Défense des Etudiants, Cases 410562, 410640 [2017] CE; Association SOS Education, Promotion et défense des étudiants et Droits des Lycéens, Cases 410561, 410641, 411913 [2017] CE.

[27] *Ibid*.

3. The current framework of the administrative algorithmic decision in France and in the European Union

The French legislator and[28] the European Union have already taken measures to save algorithmic decisions, and in particular, administrative algorithmic decisions, from being harmful to society. This framework seems to be two-headed.

Before the administrative algorithmic decision, there are obligations placed on the Administration. Thereby, algorithms used by the Administration must respect the obligations common to all processing of personal data, and notably the General Data Protection Regulation (GDPR),[29] which will apply from 25 May 2018 in all Member States.

Hence, all algorithmic decisions used by the Administration has to respect the GDPR, in particular article 5, which establishes principles related to the processing of personal data: personal data must be processed lawfully, fairly, in a transparent manner, collected for specified, legitimate, explicit and limited purposes. Data shall be kept for a limited amount of time, and its confidentiality and integrity must be ensured. It is interesting to note that this European regulation defines the liability regime by appointing the controller as the supervisor for the respect of the obligations enshrined by article 5. This clarification is useful, but, as a reminder, the GDPR does not affect algorithms that do not employ personal data. Thus, the liability problem in administrative algorithmic decisions and more generally all algorithms that do not use personal data has not been solved yet.

Besides, the general right for data subject to not be object to a decision based solely on automated processing, when such automated processing produces legal effects on this data subject, laid down in article 22 of the GDPR,[30] seems to be a difficult obligation for administrative algorithmic decision. Indeed, what forms will such an obligation for the Administration take in practice? It will be necessary to observe the application of this principle. In France, where a similar principle exists since the late 1970s,[31] this obligation can be respected by the possibility of appealing to a human representative of the Administration,[32] according to the French administrative authority regulating data protection.[33]

After the administrative algorithmic decision, the citizens have rights. Thus, to ensure that administration cannot affect extensively personal rights, recent developments in legislation have given new rights to data subjects. Of course, GDPR increases the right of protection of personal data, and establishes a right to rectification[34] and a right to erasure[35] for data subjects. However, more importantly perhaps, it seems that citizens benefit from a real right to information which has been developed in relation to algorithms using personal data. Thereby, GDPR notably organises the communication of personal data breach to the data subject,[36] or the right to be informed when personal data is transferred to a third-country or to an international organisation.[37] Overall, the data subject has the right to obtain the information based on personal data collected from her or him, as the identity and the contact of the controller, or the processing's purposes.[38]

Unfortunately, such a right of information seems to be related only to processing of personal data, and not all the algorithmic processing. This limit is particularly important in case of administrative algorithmic decision: if a private algorithm can solely affect data subjects, algorithms used by the

[28] French Parliament Loi 2016-1321 pour une République numérique [2016] JO 0235.
[29] European Parliament and Council (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119.
[30] European Parliament and Council (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119, article 22.
[31] French Parliament Loi 78-17 relative à l'informatique, aux fichiers et aux libertés [1978] JO 07/01/78, article 10.
[32] For example, on the contrary of APB, Parcoursup consent to recognise the right of submission to a reprensentative of the French Administration Education.
[33] A. Debet, 'APB enfin remis en cause par la CNIL!' [2017] Communication Commerce électronique n°12, comm. 101.
[34] European Parliament and Council (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119, article 16.
[35] *Ibid*., article 17.
[36] *Ibid*., article 34.
[37] *Ibid*., article 15.
[38] *Ibid*., article 13.

Administration can harm citizens and the general interest. The potential seriousness/danger of public algorithms explains why the legislation needs to go further in this area than the GDPR. For example, French law requires public authorities to publish the main characteristics of their algorithms, when these are the basis of individual decisions.[39] However, this general obligation has many exceptions that reduce its scope.[40]

What could be the potential next developments in the administrative algorithmic decision's legal framework? The European legislation could go further on public algorithms that do not use personal data, but have huge impact on citizens (such as in tax law[41]), for example by ordering more transparency for this category of algorithms. A better regulation of such algorithms would not be justified by a potential harm to personal data, but it could allow citizens to control that Administration's decisions based on algorithms are aimed at the general interest.

Algorithms' collective effects are another legislation's blind spot: thereby, GDPR do not target directly these algorithm's consequences.[42] For example, the recent Cambridge Analytica scandal shows how electoral marketing algorithms can have very important effects on the functioning of democracy itself.[43]

Finally, should we take more into account the specificities of particular sectors of the society in the regulation of algorithmic decision-making? The European Union has already established sector-specific rules for some activities, as algorithmic trading in 2014.[44] If such adaptation according to the regulated domains complicates the law, it is clear that it would offer a customised framework for algorithmic decision-making. Some even stand up for the total prohibition of algorithmic decisions, in very particular fields: at the moment, it is especially the case for the autonomous weapons.[45] Therefore, the object of the algorithmic decision would be a possible limit to it.

Conclusions

The study of administrative algorithmic decision-making enlighten how the legislation starts to consider the use of algorithms by the Administration. Far from prohibiting administrative algorithmic action, the current evolution of the European legislation actually adapts the links between the traditional Administration and this particular area of digitalisation in law. Then, the public algorithmic law would be divided into two branches of rights:[46] several rights for citizens (right of information, protection of personal data) and the regulated right of using algorithms for the Administration, notably to take its decisions.

To conclude, administrative algorithmic decision promises great prospects for the administration's future, in particular a greater speed and agility in decision-making,[47] a potential decrease of expenditures (thanks to the automation of tasks), a reduction of the corruption's risks thanks to a lower intervention of

[39] French Parliament Loi 2016-1321 pour une République numérique [2016] JO 0235, article 6.

[40] The theoretical scope of this general obligation is limited mainly because of the excluded fields (limitations of intellectual property law in particular) and the excluded public authorities (the obligation affects only the largest public authorities and the public authorities carrying out an activity considered as public service), see French Parliament Loi 2016-1321 pour une République numérique [2016] JO 0235, article 6.

[41] 'Les députés demandent la publication des algorithmes de l'impôt sur le revenu' [2016] Lefigaro.fr, http://www.lefigaro.fr/secteur/high-tech/2016/01/21/32001-20160121ARTFIG00255-les-deputes-demandent-la-publication-des-algorithmes-de-l-impot-sur-le-revenu.php or J. Lausson, 'Fraude fiscale des particuliers: Bercy enclenche la traque par algorithme' [2017] Numerama.com, https://www.numerama.com/politique/306112-fraude-fiscale-des-contribuables-bercy-enclenche-la-traque-experimentale-par-algorithme.html.

[42] CNIL, *Ibid*., p. 46.

[43] A. Valdez, 'Everything you need to know about Facebook and Cambridge Analytica' [2018], https://www.wired.com/story/wired-facebook-cambridge-analytica-coverage/.

[44] European Parliament and Council (EU) 2014/65 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU [2014] OJ L173, article 17.

[45] N. Rajan, 'UN Expert Casually Warns That "Killer Robots" Could Become A Reality' [2015] Huffingtonpost.uk, https://www.huffingtonpost.co.uk/2015/10/07/killer-robots-could-become-reality-if-un-talks-continue-to-delay_n_8255496.html.

[46] see J.-B. Duclercq, *Ibid*., p. 1401.

[47] M. Richtel, 'Now, to Find a Parking Spot, Drivers Look on Their Phones' [2011] nytimes.com, https://www.nytimes.com/2011/05/08/technology/08parking.html.

public agents, and, potentially, "*it can make government more equitable*".[48] [49] Meanwhile, administrative algorithmic decision could also be misused, and become counterproductive to the Administration, or, even, be dangerous for citizens.[50]

Bibliography

1. J. Angwin, J. Larson, S. Mattu and L. Kirchner, 'Machine Bias' [2016] Propublica, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.
2. Article 29 data protection working party, 'Guidelines on Automated inidivudal decision-making and Profiling for the purposes of Regulation 2016/679' [2017].
3. Association SOS Education et association Promotion et Défense des Etudiants, Cases 410562, 410640 [2017] CE.
4. Association SOS Education, Promotion et défense des étudiants et Droits des Lycéens, Cases 410561, 410641, 411913 [2017] CE.
5. M. Benesty, 'L'open data et l'open source, des soutiens nécessaires à une justice predictive fiable?' [2017] Journal of Open Access to Law vol. 5 no. 1.
6. D. Boyd and K. Crawford, 'Six Provocations for Big Data A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society' [2011].
7. S. Brentjes, 'Encyclopaedia of Islam' (Leiden: 2017).
8. A. Campolo, M. Sanfilippo, M. Whittaker and K. Crawford, 'IA now Report 2017' [2017].
9. CNIL, 'Comment permettre à l'homme de garder la main? Les enjeux éthiques des algorithmes et de l'intelligence artificielle' [2017].
10. A. Debet, 'APB enfin remis en cause par la CNIL!' [2017] Communication Commerce électronique n°12, comm. 101.
11. CNIL, 'Décision mettant en demeure le ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation' [2017] MED-2017-053.
12. C. Cook, R. Diamond, J. Hall, J. A. List and P. Oyer, 'The Gender Earnings Gap in the Gig Economy: Evidence from over a Million Rideshare Drivers' [2018].
13. J.-B. Duclercq, 'le droit public à l'ère des algorithmes' [2017] Lextenso n°5.
14. European Parliament and Council (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119.
15. French Parliament Loi 2016-1321 pour une République numérique [2016] JO 0235.
16. French Parliament Loi 78-17 relative à l'informatique, aux fichiers et aux libertés [1978] JO 07/01/78.
17. B. Georges, 'Le talon d'Achille de l'intelligence artificielle' [2017] LesEchos.fr, https://www.lesechos.fr/15/05/2017/lesechos.fr/0212088042490_le-talon-d-achille-de-l-intelligence-artificielle.htm.
18. S. Graveleau, 'APB: révélation du code source qui affecte les bacheliers à l'université' [2016], http://www.lemonde.fr/campus/article/2016/10/18/apb-revelation-du-code-source-qui-affecte-les-bacheliers-a-l-universite_5015778_4401467.html.
19. S. Graveleau, 'Parcoursup, la plate-forme qui succède à Admission post-bac, a ouvert' [2018] Le Monde, http://www.lemonde.fr/campus/article/2018/01/15/parcoursup-qui-succede-a-admission-post-bac-ouvre-ce-lundi_5241663_4401467.html?xtmc=parcoursup&xtcr=35.
20. D. W. Hall and J. Pesenti, 'Growing the Artificial Intelligence Industry in the UK' [2017].
21. D. Inglod and S. Soper, 'Amazon Doesn't Consider the Race of Its Customers. Should It?' [2016] Bloomberg, https://www.bloomberg.com/graphics/2016-amazon-same-day/?cmpid=google.
22. La Republicca, 'Scuola, continuano le proteste dei docenti. Giannini: "Ci stiamo occupando della mobilità"'. [2016], http://www.repubblica.it/scuola/2016/08/08/news/scuola_giannini_proteste_docenti_mobilita_-145605988/.

[48] T. Simonite, 'AI Experts Want to End 'Black Box' Algorithms in Government' [2017] Wired.com, https://www.wired.com/story/ai-experts-want-to-end-black-box-algorithms-in-government/.

[49] I. Lapowsky, 'One State's bail reform exposes the Promise and Pitfalls of tech-Driven Justice' [2017] Wired.com, https://www.wired.com/story/bail-reform-tech-justice/.

[50] J. Angwin, J. Larson, S. Mattu and L. Kirchner, 'Machine Bias' [2016] Propublica, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

23. I. Lapowsky, ‘One State’s bail reform exposes the Promise and Pitfalls of tech-Driven Justice’ [2017] Wired.com, https://www.wired.com/story/bail-reform-tech-justice/.
24. J. Lausson, ‘Fraude fiscale des particuliers: Bercy enclenche la traque par algorithme’ [2017] Numerama.com, https://www.numerama.com/politique/306112-fraude-fiscale-des-contribuables-bercy-enclenche-la-traque-experimentale-par-algorithme.html.
25. ’Les députés demandent la publication des algorithmes de l'impôt sur le revenu’ [2016] Lefigaro.fr, http://www.lefigaro.fr/secteur/high-tech/2016/01/21/32001-20160121ARTFIG00255-les-deputes-demandent-la-publication-des-algorithmes-de-l-impot-sur-le-revenu.php.
26. A. Liptak, ‘Sent to Prison by a Software Program’s Secret Algorithms’ [2017], https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html.
27. C. Metz, ‘What the AI Behind AlphaGo Can Teach Us About Being Human’ [2016] Wired.com, https://www.wired.com/2016/05/google-alpha-go-ai/.
28. N. Rajan, ‘UN Expert Casually Warns That "Killer Robots" Could Become A Reality’ [2015] Huffingtonpost.uk, https://www.huffingtonpost.co.uk/2015/10/07/killer-robots-could-become-reality-if-un-talks-continue-to-delay_n_8255496.html.
29. M. Richtel, ‘Now, to Find a Parking Spot, Drivers Look on Their Phones’ [2011] nytimes.com, https://www.nytimes.com/2011/05/08/technology/08parking.html.
30. T. Simonite, ‘AI Experts Want to End ‘Black Box’ Algorithms in Government’ [2017] Wired.com, https://www.wired.com/story/ai-experts-want-to-end-black-box-algorithms-in-government/.
31. A. Valdez, ‘Everything you need to know about Facebook and Cambridge Analytica’ [2018], https://www.wired.com/story/wired-facebook-cambridge-analytica-coverage/.

DIGITALISATION OF B2B TRANSACTIONS: FROM DIGITAL ONBOARDING TO BLOCKCHAIN TECHNOLOGY

Balčiūnė Aurelija[1]

Abstract

Digitalising transactions is not a new challenge, but the legal environment in relation thereof has to evolve. The past few years have shown that law is progressing to adapt to the needs of the market. This paper discusses digitalisation of B2B transactions mainly focusing on digital onboarding of clients, e-commerce and online platforms and using blockchain technologies in B2B transactions. Due to specific legislation applicable to consumers, this paper does not analyse B2C situations, unless the context requires otherwise.

Keywords: B2B, digital onboarding, blockchain, e-commerce, smart contract.

Introduction

The current business and legal environment is changing rapidly. In the past 10-20-year period some or even all lawyers rejected the idea of digitalising the transactions. However, the rise of economy, new technologies and significant growth in Fintech/RegTech, blockchains, cryptocurrencies have made us think forward. What has been considered as unacceptable, now is more than welcome.

Digitalising the transactions, especially B2B transactions in a financial sector, is not a new challenge, but the legal environment in relation thereof has to evolve. The past few years have shown that legal environment is adapting to the needs of the market. This is especially true when we consider digital onboarding of clients. Although Lithuanian legislation had been rather strict with respect to customer due diligence and KYC procedures, in 2016 Lithuanian legislator adapted to the needs of the market players and introduced the possibility of identification of the customers online[2].

Furthermore, the rise of blockchain technologies has made the companies to think of other ways to use such technologies in their activities. For example, in November 2017 Sberbank announced that it had organised the Russian banking industry's first ever pilot blockchain payment transaction[3]. The use of blockchain technologies in payment transactions makes us to think not only about the possible opportunities the blockchain can give, but also possible legal barriers and challenges we might face.

In the view of the above, this paper analyses digitalisation in B2B transactions from the perspective of: (i) digital onboarding of clients; (ii) use of online platforms and other e-commerce tools in B2B transactions; (iii) using blockchain technologies in B2B transactions; and (iv) opportunities and challenges in digitalisation of B2B transactions. Due to specific legislation applicable to consumers, this paper does not analyse B2C situations, unless the context requires otherwise.

1. Digital onboarding of clients

Digital onboarding is blooming. Firstly, it has started with e-commerce tools, later it has reached even one of the most conservative sectors in the market – financial sector. This is especially true when

---

[1] *PhD candidate at Vilnius University, Faculty of Law. Research interests include international private law, contract law, unfair contract terms in B2B transactions.*

[2] This has been done by amending the Law on Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania (in Lithuanian: 'Lietuvos Respublikos pinigų plovimo ir teroristų finansavimo prevencijos įstatymas' [1 December 2016] Valstybės žinios, 1997-07-04, Nr. 64-1502), https://www.e-tar.lt/portal/lt/legalAct/TAR.C44837068B55/fwssaSwABQ (available in Lithuanian only), accessed 1 May 2018.

[3] For more information: 'Sberbank carries out Russia's first payment transaction using blockchain technology' [29 November 2017] Sberbank press release, https://www.sberbank.ru/en/press_center/all/article?newsID=9f676571-5219-4cfb-bbb7-c9c6e1de983a&blockID=1539&regionID=51&lang=en, accessed 1 May 2018.

N26[4] or similar financial market participants are considered, where the client's onboarding and their experience is based on digital solutions. Having this in mind, this part of the paper particularly focuses on the possibilities of digital onboarding in the financial sector.

Adoption of AMLD3[5] and later AMLD4[6] has been one of the drivers for expansion of digital onboarding. In contrast with AMLD3, which allowed digital onboarding, but required application of enhanced customer due diligence (EDD) measures[7], AMLD4 does establish mandatory EDD measures in case of non-face-to-face identification. Notwithstanding the foregoing, AMLD4 indicates that non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures, might pose potentially higher risk, as indicated in Article 18(3) of AMLD4. This suggests that even if digital onboarding is removed from cases of mandatory EDD, this does not exclude that EDD measures would still be required to apply, especially in the cases where no additional safeguards are used (such as electronic signatures suggested by Annex III of AMLD4). This, of course, gives some uncertainty to financial market participants and other obliged entities under AMLD4 as to whether digital onboarding, indeed, simplifies the onboarding or not (especially because of the risk of necessity to apply EDD measures). Furthermore, since AMLD4 does not provide a list of methods for the digital onboarding, it is up to the local legislator to decide which onboarding methods are allowed in each country. Having no harmonized legislation in this area might be a big burden to financial institutions operating in different jurisdictions since their digital onboarding procedures have to be adapted based on legislation of each jurisdiction they operate. In some, even if not in all cases, this might pose certain concerns and doubts as to the resources required to adapt to different legislation.

In Lithuania, digital onboarding has been firstly recognized by law in the end of 2016[8]. Following AMLD3, Lithuanian AML Law established that EDD should be applied in the event the customer has not been physically present for identification purposes. Furthermore, as the directive, Lithuanian AML Law established that, in addition to EDD measures, one or several additional measures should have been applied: (i) ensuring that the customer's identity is established by additional documents, data or information; (ii) supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution; (iii) ensuring that the first payment of the operations is carried out through an account opened in the customer's name with a credit institution. However, at the time of adoption of the Lithuanian AML Law in 2016, no methods for digital onboarding have been approved on the level of law. Only the implementing legal act adopted by the Lithuanian Financial Crime Investigation Service has established certain technical standards applicable to video onboarding[9].

Notwithstanding the foregoing, the situation has changed in mid-2017, when AMLD4 has been transposed into Lithuanian legislation. According to the new law, the following methods of non-face-to-face identification are allowed: (i) using third party data; (ii) using EU electronic identification means issued in EU which meet electronic identification schemes of a high or substantial assurance level (eIDAS Regulation[10]); (iii) when information about the identity of the person is attested by a qualified electronic signature using a qualified certificate for electronic signatures, which meets the requirements

[4] N26 bank operates only digitally and no branch visits are required for the customers to use the bank's services. It is said that N26 currently operates in 17 countries. For more information about the bank, please see 'About N26: Who we are' N26, https://support.n26.com/read/000001253?locale=en, accessed 1 May 2018.

[5] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing [2005] OJ L 309.

[6] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ L 141.

[7] See Article 13(2) of AMLD3.

[8] Although certain methods for digital onboarding have been applied by financial market participants even before adoption of the law.

[9] See technical standards approved by the director of the Financial Crimes Investigation Service on 30 November 2016 (in Lithuanian: Finansinių nusikaltimų tyrimo tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos direktoriaus 2016 m. lapkričio 30 d. įsakymas Nr. V-314 „Dėl Techninių reikalavimų kliento tapatybės nustatymo procesui, kai tapatybė nustatoma nuotoliniu būdu, naudojantis elektroninėmis priemonėmis, leidžiančiomis tiesioginio vaizdo perdavimą, patvirtinimo". TAR, 2016-12-01, Nr. 27955).

[10] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L 257.

of the eIDAS Regulation; (iv) using electronic means allowing live video transmission; or (v) a payment from the customer's bank account to the account of the company is made and a paper copy of the identity document certified in accordance with the applicable requirements is submitted. Therefore, Lithuanian law has established an exhaustive list of methods for non-face-to-face, which *inter alia* includes certain digital onboarding methods.

As AMLD4, new Lithuanian AML Law establishes that non-face-to-face identification might pose potentially higher risk and, thus, EDD measures might be required to apply. Thus, although financial market participants and obliged entities are released from obligation to apply EDD measures in all cases where the client is identified digitally, new regulation does not entirely eliminate the requirement to apply EDD measures (especially where digital onboarding of the customer is not followed by additional safeguard measures, such as electronic signature of similar).

As for digital onboarding when live video transmission is used, the following methods are available: (i) during live video transmission the image of an identity document or corresponding residence permit in the Republic of Lithuania is captured and the customer's identity is determined at least by using advanced electronic signature meeting the requirements under eIDAS Regulation; or (ii) during live video transmission the image of the customer's face and the original of the identity document or corresponding residence permit in the Republic of Lithuania shown by the customer are captured. Although, in theory, such methods look very attractive, they raise some issues in practice. Firstly, many online products allowing digital onboarding allow taking picture of the ID document and a selfie of the face of the customer. However, if only ID document is captured as indicated in method (i) above, such identification has to be followed by using advanced electronic signature (usually by signing KYC questionnaire since the requirement to collect customer's data still exists). If ID document and a selfie is captured during live video (not live image transmission), this does not eliminate the requirement to record the onboarding of the customer (not only the customer is requested to show the face and document in different angles, but also the audio of the onboarding has to be recorded and stored. Moreover, the customer should receive certain KYC questions and answer those questions during such onboarding).

In addition to video onboarding, method (v)[11] is also widely used in Lithuanian market (especially where consumer credit providers are considered). However, although having some benefits, the use of such method is very restricted considering the fact that financial institutions and other obliged entities under Lithuanian AML Law are requested to ask the customer to deliver a copy of the ID document[12] to them in paper by post, courier, by delivering to parcel terminal or delivery in person. Obviously, this complicates and delays the onboarding period and, thus, makes this method very unattractive.

Finally, with the adoption of AMLD4 and eIDAS Regulation, digital onboarding using electronic signatures meeting the requirements of eIDAS Regulation has been also introduced in the Lithuanian AML Law. Although this method increases the possibilities of digital onboarding, certain issues and uncertainties delay the use of such method in practice. These *inter alia* include requirements that (i) prior to establishing the identity of the customer and the beneficial owner, the customer has been duly identified by a third party; (ii) the identity of the customer, being a natural person or a representative of a legal entity, has been established on the basis of the identification documents as required under the law. This basically means that, before identifying the customer using electronic signatures, a financial institution or obliged entity should make sure that the providers of electronic signatures have duly identified their customers based on the document specified herein. Implementing such requirement in practice is rather complicated and might require a lot of resources (both human and timing resources, as well as additional costs). Furthermore, when trusting electronic signatures, financial institutions and obliged entities should basically verify whether such signatures meet the requirements established under eIDAS Regulation. Although there are many companies providing the possibility to sign documents digitally, there is no single database which would ascertain that a particular electronic signature solution meets the requirements of eIDAS Regulation.

[11] A payment from the customer's bank account to the account of the company is made and a paper copy of the identity document certified in accordance with the applicable requirements is submitted.

[12] Such copy being certified by the notary, elder (in Lithuanian: seniūnas) and consular officer of the Republic of Lithuania.

As you have already seen, this part of the paper focuses more on digital onboarding of the customer following AML requirements. However, customer identification under AML rules is only one part of the process. Such process is later followed by additional onboarding procedures based on a product offered by a company. Nevertheless, if customer identification procedures cannot be carried out digitally, full online experience (e.g. as offered by N26) may become impossible or less attractive since already part of the process would require physical presence. As you have also seen no distinction between B2B and B2C transactions have been made in this context. However, one has to admit that the use of digital onboarding in B2C transactions is still searching for its way into consumer's life, whereas digital onboarding of corporate clients (especially foreign clients) is already widely used in the market.

With the rise of this digital age, FinTech/RegTech evolution and iphone society or "millennials", digital onboarding is becoming more and more attractive. However, as already indicated in this part of the paper, digital onboarding still raises certain issues which lead to the continuous use of face-to-face identification in practice. One may hope that the legislation will keep up with the rapidly changing digital world and adapt the regulation to the needs of the market participants.

2. Use of online platforms and other e-commerce tools in B2B transactions

The use of online platforms and other e-commerce tools[13] in B2B transactions has been flourishing over the past years. It is said that B2B e-commerce revenue will be around 6.7 trillion USD by 2020[14]. Therefore, it seems that traders are digitalizing not only onboarding of customers, but they also move their business to e-commerce, which in certain cases may decrease the human and time resources required, as well as move the business into international waters[15].

It is said that the success of e-commerce depends on the ability to execute legally binding transactions online[16]. Indeed, the regulatory environment should focus on making digital transactions legally valid and enforceable[17]. Therefore, legal barriers applicable to e-commerce become significantly important when considering trading digitally. This is especially true where B2B transactions are concerned. In B2C environment businesses are used to strict legal requirements applicable in order to protect consumers. However, where B2B solutions are concerned, companies are interested in liberal regulations recognizing contracts concluded via e-commerce tools, and, especially the validity and enforceability of contracts concluded using electronic signature.

One of the regulatory issues which concerns e-commerce is related to electronic documents and electronic signatures having the same legal status and force as "written documents" and "hand-written signatures"[18]. This suggests that digital transactions which include electronic documentation (contracts) signed by electronic signature should be recognized by the local regulations in the same manner as "written documents" having "hand-written signatures". It is also said that the prevailing local laws should contain provisions that ensure the recognition of electronic signatures as paper-based signatures, as well as provisions on place of origin and permanent establishment (especially relevant in case of cross-border e-commerce), transparency and information requirements, commercial communications, conclusion and validity of electronic contracts[19].

---

[13] For more information regarding online (internet trading) platforms, 'Final Report' (Report of the Expert Group) [2018] B2B Internet trading platforms, http://www.e-thematic.org/download/B2B%20Internet%20trading%20platforms,%20July%202003.pdf, accessed 1 May 2018.

[14] 'What is business to business e commerce? B2B e-commerce examples' [2018] VirtoCommerce, <https://virtocommerce.com/glossary/what-is-b2b-ecommerce, accessed 1 May 2018; B. Robinson, 'B2C and B2B Ecommerce: Whats the difference anyway?' [2017] Business.com, https://www.business.com/articles/b2c-and-b2b-ecommerce-whats-the-difference-anyway/, access on 1 May 2018; 'B2B Ecommerce Market Is Still Maturing' [2016] Emarketer.com, https://www.emarketer.com/Article/B2B-Ecommerce-Market-Still-Maturing/1014311, accessed 1 May 2018.

[15] For more information regarding the role of e-commerce in B2B markets, please see: P. Fauska, N. Kryvinska and C. Strauss, 'The role of e-commerce in B2B markets of goods and services' [2013] Int. J. Services, Economics and Management, Vol. 5, Nos. 1/2, pp. 41–71, https://www.researchgate.net/publication/259333744_The_role_of_e-commerce_in_B2B_markets_of_goods_and_services, accessed 30 April 2018.

[16] 'Securely Executing e-Contracts in International Commercial Trade Transactions', https://www.globaltradeguardian.net/executing-b2b-e-contracts, accessed 1 May 2018.

[17] M. Kumar and M. Sareen, 'Trust and Technology in B2B E-Commerce: Practices and Strategies for Assurance' (IGI Global, 2011) p. 228.

[18] See analysis of this issue supra note 17, p. 228.

[19] See analysis of this issue supra note 17, p. 228.

Directive on Electronic Commerce[20], Misleading and Comparative Advertising Directive[21], eIDAS Regulation and local legislation play an important role with respect to development of e-commerce in B2B transactions. Directive on Electronic Commerce, which has been transposed into Law on Information Society Services of the Republic of Lithuania[22], establishes transparency, information and other requirements for online service providers[23], as well as requirements for forming a contract (including a requirement to the Member States to ensure that their legal system allows contracts to be concluded by electronic means and such requirements do not create obstacles for the use of electronic contracts or result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means, as well as certain requirements applicable with respect to information to be provided and placement of orders)[24][25].

In this respect, electronic signature regulation plays an important role. Law on Electronic Signature of the Republic of Lithuania[26] establishes that a secure-electronic-signature created by a secure-signature-creation-device and based on a qualified-certificate which is valid shall have the same legal force that a hand-written signature in written documents has and shall be admissible as evidence in court; a signature may not be deemed invalid based on any of the following grounds listed below: (i) in electronic form; (ii) not based upon a qualified-certificate; (iii) not based upon a qualified-certificate issued by an accredited certification-service-provider; (iv) not created by a secure signature-creation device[27]. Therefore, as already indicated, electronic signature placed on a document cannot be invalidated solely because of the reason that it is electronic or it is not based on a qualified certificate or similar reasons. At the same time, the law expressly indicates that an electronic signature in each case has the same legal force as a hand-written signature if the counterparties agree on this. Furthermore, eIDAS Regulation may also add some value in developing e-commerce[28]. By providing a harmonised foundation for secure electronic signatures and not interfering into regulation of conclusion and validity of contracts[29], eIDAS Regulation may assist in digitalisation of B2B transactions. Having single regulation for electronic signatures in the European Union may increase cross-border B2B transactions.

Finally, it is said that Misleading and Comparative Advertising Directive, which has been transposed into the Law on Marketing of the Republic of Lithuania[30], is applicable to B2B relations concerning misleading advertising since the directive on unfair commercial practices applicable to B2C relations is in place[31]. Although the Misleading and Comparative Advertising Directive does not directly regulate e-commerce, removal of misleading advertising may also assist in promoting digitalisation of B2B relations, which, as the case may be, may start from the receipt of certain advertising materials.

In the view of the above considerations, one may conclude that the number of digital B2B transactions is increasing. As it is "the internet will accelerate the trend toward the digital economy"[32]. Rather liberal regulation, maybe not as a major factor, but also assists in developing digitalisation of B2B

[20] 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 [2000] OL L 178.

[21] Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising (codified version) [2006] OL L 376.

[22] In Lithuanian: Lietuvos Respublikos informacinės visuomenės paslaugų įstatymas. Valstybės žinios, 2006-06-10, Nr. 65-2380.

[23] Including a requirement to provide detailed information about the business including its name, geographic address, contact details and any trade registration or business authorisation information (see Article 5).

[24] See Articles 9-11.

[25] For more information regarding Directive on Electronic Commerce, please see: A. R. Lodder and A.D. Murray, 'The European Union and E-Commerce' [1 March 2017] EU Regulation of E-Commerce, A Commentary Elgar Commentaries series [2017] 1-14, https://ssrn.com/abstract=2925882, accessed 30 April 2018.

[26] In Lithuanian: Lietuvos Respublikos elektroninio parašo įstatymas. Valstybės žinios, 2000-07-26, Nr. 61-1827.

[27] See Article 8.

[28] Preamble 2 of the eIDAS Regulation seeks to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union.

[29] See Article 2(3).

[30] In Lithuanian: Lietuvos Respublikos reklamos įstatymas. Valstybės žinios, 2000-07-31, Nr. 64-1937.

[31] See the materials on 'Misleading and comparative advertising directive', https://ec.europa.eu/info/law/law-topic/consumers/unfair-commercial-practices-law/misleading-and-comparative-advertising-directive_en, accessed 30 April 2018.

[32] See Section 4.2 Digital Commerce in S. Basu, 'Taxation of Electronic Commerce' [2001] Commentary, The Journal of Information, Law and Technology, http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_2/basu1/, accessed 30 April 2018.

relations. However, regulation has to keep up to the speed of modernisation of B2B transactions and assist in regulation of issues which require regulator's attention[33].

3. Using blockchain technologies in B2B transactions

With the development of society and changing era, the contract law is also advancing. Starting from verbal agreements performed in kind in agrarian society, formal and well standardized agreements dominate nowadays. However, with the rise of the society and high development in social sciences, not only the terms of the agreement are becoming more complicated, but also different forms of agreements find their way in contract law.

Cryptocurrencies not only have changed the way of thinking but have also introduced the possibilities of using technologies in financial and legal matters. When we first think about cryptocurrencies, blockchain technology comes into the mind. However, blockchain may be used not only to facilitate cryptocurrencies[34], but also it already finds its way in other areas[35]. In this way, blockchain has found its place in the legal environment by offering smart contracts. Therefore, this part of the paper focuses on opportunities and challenges offered by smart contracts.

Without going any deeper into the analysis of smart contracts, the definition of smart contracts should be provided as a starting point. Unfortunately, currently there is no harmonized definition of smart contracts. According to Nick Szabo, "smart contract is a computerized transaction algorithm, which performs the terms of the contract"[36]. However, as you can see, this definition is rather generalized and get be used to define the processes carried out by vending machine[37]. To this end, the definition offered by Gideon Greenspan could be used to define blockchain and understand its use in concluding smart contracts: "A smart contract is a piece of code which is stored on an Blockchain, triggered by Blockchain transactions, and which reads and writes data in that Blockchain's database"[38]. This definition basically suggests that blockchain is a core technology based on a code which is used to conclude a smart contract.

Having the aforementioned definition in mind, one has to answer whether blockchain is only a technological tool (or a computer code) which can be basically used for IT purposes or, on the contrary, it is a contract which could be used in legal relations. According to the definitions given with respect to the smart contracts, one cannot exclude that smart contracts do not have the same form as written or verbal agreements. In a classical contract law sense, a smart contract does not provide in detail all the contractual terms (including rights and obligations) as it is done in classic agreements used nowadays[39]. However, due to the fact that: (i) smart contracts are used to govern certain relations between the parties (e.g. for the purpose of circulation of cryptocurrencies or tokens); (ii) despite its nature, conclusion of a

---

[33] In this respect, a new initiative in the area of unfair contracts and trading practices in platform-to-business relations. See Proposal for a regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services. COM (2018) 238 final, 2018/0112 (COD), https://ec.europa.eu/digital-single-market/en/news/regulation-promoting-fairness-and-transparency-business-users-online-intermediation-services, accessed 30 April 2018.

[34] A. Savelyev, 'Contract Law 2.0: «Smart» Contracts As the Beginning of the End of Classic Contract Law' [2016] Higher School of Economics Research Paper No. WP BRP 71/LAW/2016, https://ssrn.com/abstract=2885241 or http://dx.doi.org/10.2139/ssrn.2885241, accessed 1 May 2018.

[35] For example, on 16 March 2018 the Bank of Lithuania (Lithuanian financial supervisory authority) called software developers for proposals to develop a blockchain platform, which would help Lithuanian and international companies gain knowledge and carry out blockchain-oriented research, thus adapting and testing blockchain-based services in the financial sector. More: 'Bank of Lithuania calls for proposals to develop a blockchain platform' [2018] Bank of Lithuania, https://www.lb.lt/en/news/bank-of-lithuania-calls-for-proposals-to-develop-a-blockchain-platform, accessed 1 May 2018.

[36] 'Smart contracts in Essays on Smart Contracts, Commercial Controls and Security' Szabo N 1994, http://szabo.best.vwh.net/smart.contracts.html, as cited in supra note 34, p. 7.

[37] Vending machine example is widely used when analysing N. Szabo's definition. See explanation regarding vending machine effect in supra note 34, pp. 7-8.

[38] G Greenspan 'Beware of the Impossible Smart Contract' [12 April 2016] Blockchain news, http://www.the-blockchain.com/2016/04/12/beware-of-the-impossible-smart-contract, as cited in supra note 34, p. 8.

[39] Smart contracts include a scripting language which is rather limited and is basically determined by programmable logic. Therefore, a smart contract may establish minimum terms (conditions) after successful completion of which transaction is executed. However, since the conditions are providing in scripting language, the execution of contract is automated and does not require human interference. For more information about the construction of smart contracts, see: K.D. Werbach and N. Cornell, 'Contracts Ex Machina' [2017] 67 Duke Law Journal, Forthcoming, https://ssrn.com/abstract=2936294, accessed 1 May 2018.

smart contract requires the will of the party concluding it; (iii) execution of a smart contract creates a certain result; and (iv) having such contract concluded in electronic (digital) form does not eliminate its validity[40], it should be recognized as a certain form of legal arrangement (contract).

However, even if a smart contract is recognized as a contract with all the consequences following execution of a contract, the absence of national legislation[41] with respect to the use of blockchain, in particular where smart contracts are concerned, raises certain issues. Of course, where new technologies come into life, regulatory compliance matters have to be taken into account. Firstly, blockchain technologies operate like computer codes, which means that cross-border transactions are carried out constantly. This suggests that having no harmonized laws may cause certain difficulties in complying with all the local laws affected by a certain transaction[42]. In addition, potential anonymity[43] in blockchain transactions may have legal implications with respect to determination of the counterparty, its capacity and other related matters. Due to these legal challenges, the validity of a smart contract may be questioned. Furthermore, this issue may also be relevant when a potential dispute is in place. Another challenge is related to possible errors in computer codes used by a blockchain. It is yet not clear how the validity of the contracts would be affected in case of possible errors in programming language and how a smart contract could be amended or modified due to such mistakes (due to, e.g. human errors, software issues, cyber-attacks, etc.). Going further, some issues may also arise with respect to governing law and jurisdiction. In general, smart contracts do not deal with governing law and jurisdiction issues and even using the general principles for the governing law and jurisdictions in accordance with Rome and Brussels regulations, some uncertainties may still cause difficulties in solving any possible disputes in a timely manner (this is also relevant where the transaction contains anonymity). Finally, as each contract, a smart contract should bear certain legal consequences. However, the difference from a classical contract here is that a smart contract is automatically executed and irrevocable, therefore, any remedies with respect to execution of the smart contract are basically available only at the moment of execution or post-execution[44]. To this end, it is not clear how, for example, in case of breach of certain terms of the agreement or in case of non-compliance of a smart contract with mandatory provisions of law (including cases, where fraudulent activities are carried out) termination of the contract, restitution and other remedies could be applied.

---

[40] Regarding the validity, please see Section 2 of this paper. Furthermore, detail analysis of these criteria and common features of smart contracts can be found in supra note 34, p. 10-16. Furthermore, analysis as to whether a smart contract is a form of contract can be found in supra note 39, pp. 19-24.

[41] One has to admit that certain legislative initiatives have already been introduced. For instance, in March 2016 the US federal regulator has published the 1st guidance on blockchain technology. Later, in December the US Federal Reserve reported on distributed ledgers. Finally, these 2 reports have been followed by the positive positions of US federal financial regulators (CFTC and SEC). The advance in technologies has also been recognized in the EU. Starting from public reports and continuing to creation of various internal groups and task forces working on technologies, the EU has shown its positive attitude as to the use of blockchain technologies. The same approach has already been followed by some Member States. UK regulator not only has presented a paper on distributed ledger technologies, but also the Bank of England has become a member of the Linux Foundation-led Hyperledger Blockchain initiative. Finally, France has issued to legal bills recognizing blockchains. For further information regarding these initiatives, please see S. Blemus, 'Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide' [2018] Revue Trimestrielle de Droit Financier (Corporate Finance and Capital Markets Law Review) RTDF N°4-2017 - December 2017, pp. 9-12, https://ssrn.com/abstract=3080639 or http://dx.doi.org/10.2139/ssrn.3080639, accessed 1 May 2018; also see H. Kakavand, N. Kost De Sevres and B. Chilton, 'The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies' [2017] pp. 20-24, https://ssrn.com/abstract=2849251 or http://dx.doi.org/10.2139/ssrn.2849251, accessed 1 May 2018.

[42] Regarding regulatory compliance difficulties, please see S. Ammous, 'Blockchain Technology: What is it Good for?' [2016], p. 4, https://ssrn.com/abstract=2832751 or http://dx.doi.org/10.2139/ssrn.2832751, accessed 1 May 2018; also: D.A. Zetzsche, R.P. Buckley and D.W. Arner, 'The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain' [2017] University of Illinois Law Review, 2017-2018, Forthcoming; University of Luxembourg Law Working Paper No. 007/2017; Center for Business & Corporate Law (CBC) Working Paper 002/2017; University of Hong Kong Faculty of Law Research Paper No. 2017/020; UNSW Law Research Paper No. 52; European Banking Institute Working Paper Series 14, pp. 4-5, https://ssrn.com/abstract=3018214 or http://dx.doi.org/10.2139/ssrn.3018214, accessed 1 May 2018; and references indicated therein.

[43] As regards potential anonymity, see P. Catchlove, 'Smart Contracts: A New Era of Contract Use' [2017], https://ssrn.com/abstract=3090226 or http://dx.doi.org/10.2139/ssrn.3090226, accessed 1 May 2018.

[44] See the development of this argument in M. Raskin, 'The Law and Legality of Smart Contracts' [2016] 1 Georgetown Law Technology Review 304 (2017), pp. 321-322, https://ssrn.com/abstract=2959166 or http://dx.doi.org/10.2139/ssrn.2842258, accessed 1 May 2018.

In the view of the above, one may conclude that smart contracts can offer many opportunities, especially where B2B transactions are concerned[45]. It is said that such contracts may be used for crowdfunding[46], insurance contracts, smart properties (e.g. for the use of unlocking the leased car or rented apartment)[47], stock market[48] and even far beyond. Therefore, technology innovation should be followed by legal innovation which should adapt to the needs of the market (where unnecessary, not interfering and, on the contrary, where necessary, providing relevant regulation).

Conclusions

Digitalisation in transactions is clearly a new challenge for contract law. One has to admit that, in B2B transactions corporate entities are interested in liberal regulations recognizing digital onboarding, contracts concluded using e-commerce tools and blockchain technology. However, to ensure the validity and enforceability of digital transactions, contract law has to adapt and support certain changes in commercial practices.

With the rise of this digital age and society, digital onboarding is becoming more and more attractive. However, non-face-to-face identification still raises certain issues which lead to the continuous use of face-to-face identification in practice.

E-commerce tools are commonly used in the market. However, it is important to ensure that the local regulation recognizes the validity and enforceability of contracts concluded using electronic signature.

Smart contracts can offer many opportunities. However, technology innovation should be followed by legal innovation giving some guidance and clarity as to the capacity of counterparties, validity of smart contracts, their enforceability, amendment, termination, restitution and other legal matters.

Bibliography

1. 'Lietuvos Respublikos pinigų plovimo ir teroristų finansavimo prevencijos įstatymas' [1 December 2016] Valstybės žinios, 1997-07-04, Nr. 64-1502, https://www.e-tar.lt/portal/lt/legalAct/TAR.C44837068B55/fwssaSwABQ (available in Lithuanian only), accessed 1 May 2018.
2. N26 bank operates only digitally and no branch visits are required for the customers to use the bank's services. It is said that N26 currently operates in 17 countries. For more information about the bank, please see 'About N26: Who we are' N26, https://support.n26.com/read/000001253?locale=en, accessed 1 May 2018.
3. Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing [2005] OJ L 309.
4. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ L 141.
5. Finansinių nusikaltimų tyrimo tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos direktoriaus 2016 m. lapkričio 30 d. įsakymas Nr. V-314 „Dėl Techninių reikalavimų kliento tapatybės nustatymo procesui, kai tapatybė nustatoma nuotoliniu būdu, naudojantis elektroninėmis

[45] Primarily due to the fact that B2B transactions enjoy more liberal regime and less protection in comparison with B2C transactions.

[46] See also: P. De Filippi, 'Blockchain-Based Crowdfunding: What Impact on Artistic Production and Art Consumption?' [2015] Observatório Itaú Cultural, Issue 19, https://ssrn.com/abstract=2725373, accessed 1 May 2018.

[47] Crowdfunding, insurance and smart properties are analysed in the papers of A. Savelyev, K.D. Werbach, N. Cornell and M. Finck, 'Blockchain Regulation' [2017] German Law Journal, 2018, Forthcoming; Max Planck Institute for Innovation & Competition Research Paper No. 17-13, https://ssrn.com/abstract=3014641 or http://dx.doi.org/10.2139/ssrn.3014641, accessed 1 May 2018.

[48] See, for example, L. Lee, 'New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market' [2016] Hastings Business Law Journal, Volume 12, Issue 2; University of Utah College of Law Research Paper No. 138, https://ssrn.com/abstract=2656501 or http://dx.doi.org/10.2139/ssrn.2656501, accessed 1 May 2018. As for the use in financial markets, see: H. Kakavand, N. Kost De Sevres and B. Chilton in supra note 34, pp. 14-16.

priemonėmis, leidžiančiomis tiesioginio vaizdo perdavimą, patvirtinimo". TAR, 2016-12-01, Nr. 27955.
6. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L 257.
7. 'Final Report' (Report of the Expert Group) [2018] B2B Internet trading platforms, http://www.e-thematic.org/download/B2B%20Internet%20trading%20platforms,%20July%202003.pdf, accessed 1 May 2018.
8. 'What is business to business e commerce? B2B e-commerce examples' [2018] VirtoCommerce. Available at: <https://virtocommerce.com/glossary/what-is-b2b-ecommerce> (accessed 1 May 2018).
9. 'What is business to business e commerce? B2B e-commerce examples' [2018] VirtoCommerce, <https://virtocommerce.com/glossary/what-is-b2b-ecommerce, accessed 1 May 2018.
10. B. Robinson, 'B2C and B2B Ecommerce: Whats the difference anyway?' [2017] Business.com, https://www.business.com/articles/b2c-and-b2b-ecommerce-whats-the-difference-anyway/, access on 1 May 2018.
11. 'B2B Ecommerce Market Is Still Maturing' [2016] Emarketer.com, https://www.emarketer.com/Article/B2B-Ecommerce-Market-Still-Maturing/1014311, accessed 1 May 2018.
12. P. Fauska, N. Kryvinska and C. Strauss, 'The role of e-commerce in B2B markets of goods and services' [2013] Int. J. Services, Economics and Management, Vol. 5, Nos. 1/2, p. 41–71, https://www.researchgate.net/publication/259333744_The_role_of_e-commerce_in_B2B_markets_of_goods_and_services, accessed 30 April 2018.
13. 'Securely Executing e-Contracts in International Commercial Trade Transactions', https://www.globaltradeguardian.net/executing-b2b-e-contracts, accessed 1 May 2018.
14. M. Kumar and M. Sareen, 'Trust and Technology in B2B E-Commerce: Practices and Strategies for Assurance' (IGI Global, 2011) p. 228.
15. 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 [2000] OL L 178.
16. Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising (codified version) [2006] OL L 376.
17. Lietuvos Respublikos informacinės visuomenės paslaugų įstatymas. Valstybės žinios, 2006-06-10, Nr. 65-2380.
18. A. R. Lodder and A.D. Murray, 'The European Union and E-Commerce' [1 March 2017] EU Regulation of E-Commerce, A Commentary Elgar Commentaries series [2017] 1-14, https://ssrn.com/abstract=2925882, accessed 30 April 2018.
19. Lietuvos Respublikos elektroninio parašo įstatymas. Valstybės žinios, 2000-07-26, Nr. 61-1827.
20. Lietuvos Respublikos reklamos įstatymas. Valstybės žinios, 2000-07-31, Nr. 64-1937.
21. 'Misleading and comparative advertising directive', https://ec.europa.eu/info/law/law-topic/consumers/unfair-commercial-practices-law/misleading-and-comparative-advertising-directive_en, accessed 30 April 2018.
22. S. Basu, 'Taxation of Electronic Commerce' [2001] Commentary, The Journal of Information, Law and Technology, http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_2/basu1/, accessed 30 April 2018.
23. Proposal for a regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services. COM (2018) 238 final, 2018/0112 (COD), https://ec.europa.eu/digital-single-market/en/news/regulation-promoting-fairness-and-transparency-business-users-online-intermediation-services, accessed 30 April 2018.
24. 'Sberbank carries out Russia's first payment transaction using blockchain technology' [29 November 2017] Sberbank press release, https://www.sberbank.ru/en/press_center/all/article?newsID=9f676571-5219-4cfb-bbb7-c9c6e1de983a&blockID=1539&regionID=51&lang=en, accessed 1 May 2018
25. A. Savelyev, 'Contract Law 2.0: «Smart» Contracts As the Beginning of the End of Classic Contract Law' [2016] Higher School of Economics Research Paper No. WP BRP 71/LAW/2016,

https://ssrn.com/abstract=2885241 or http://dx.doi.org/10.2139/ssrn.2885241, accessed 1 May 2018.
26. 'Bank of Lithuania calls for proposals to develop a blockchain platform' [2018] Bank of Lithuania, https://www.lb.lt/en/news/bank-of-lithuania-calls-for-proposals-to-develop-a-blockchain-platform, accessed 1 May 2018.
27. 'Smart contracts in Essays on Smart Contracts, Commercial Controls and Security' Szabo N 1994, http://szabo.best.vwh.net/smart.contracts.html, as cited in supra note 34, p. 7
28. G Greenspan 'Beware of the Impossible Smart Contract' [12 April 2016] Blockchain news, http://www.the-blockchain.com/2016/04/12/beware-of-the-impossible-smart-contract.
29. K.D. Werbach and N. Cornell, 'Contracts Ex Machina' [2017] 67 Duke Law Journal, Forthcoming, https://ssrn.com/abstract=2936294, accessed 1 May 2018.
30. S. Blemus, 'Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide' [2018] Revue Trimestrielle de Droit Financier (Corporate Finance and Capital Markets Law Review) RTDF N°4-2017 - December 2017, p. 9-12, https://ssrn.com/abstract=3080639 or http://dx.doi.org/10.2139/ssrn.3080639, accessed 1 May 2018.
31. H. Kakavand, N. Kost De Sevres and B. Chilton, 'The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies' [2017] p. 20-24, https://ssrn.com/abstract=2849251 or http://dx.doi.org/10.2139/ssrn.2849251, accessed 1 May 2018.
32. S. Ammous, 'Blockchain Technology: What is it Good for?' [2016], p. 4, https://ssrn.com/abstract=2832751 or http://dx.doi.org/10.2139/ssrn.2832751, accessed 1 May 2018.
33. D.A. Zetzsche, R.P. Buckley and D.W. Arner, 'The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain' [2017] University of Illinois Law Review, 2017-2018, Forthcoming; University of Luxembourg Law Working Paper No. 007/2017; Center for Business & Corporate Law (CBC) Working Paper 002/2017; University of Hong Kong Faculty of Law Research Paper No. 2017/020; UNSW Law Research Paper No. 52; European Banking Institute Working Paper Series 14, p. 4-5, https://ssrn.com/abstract=3018214 or http://dx.doi.org/10.2139/ssrn.3018214, accessed 1 May 2018.
34. P. Catchlove, 'Smart Contracts: A New Era of Contract Use' [2017], https://ssrn.com/abstract=3090226 or http://dx.doi.org/10.2139/ssrn.3090226, accessed 1 May 2018.
35. M. Raskin, 'The Law and Legality of Smart Contracts' [2016] 1 Georgetown Law Technology Review 304 (2017), p. 321-322, https://ssrn.com/abstract=2959166 or http://dx.doi.org/10.2139/ssrn.2842258, accessed 1 May 2018.
36. P. De Filippi, 'Blockchain-Based Crowdfunding: What Impact on Artistic Production and Art Consumption?' [2015] Observatório Itaú Cultural, Issue 19, https://ssrn.com/abstract=2725373, accessed 1 May 2018.
37. A. Savelyev, K.D. Werbach, N. Cornell and M. Finck, 'Blockchain Regulation' [2017] German Law Journal, 2018, Forthcoming; Max Planck Institute for Innovation & Competition Research Paper No. 17-13, https://ssrn.com/abstract=3014641 or http://dx.doi.org/10.2139/ssrn.3014641, accessed 1 May 2018.
38. L. Lee, 'New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market' [2016] Hastings Business Law Journal, Volume 12, Issue 2; University of Utah College of Law Research Paper No. 138, https://ssrn.com/abstract=2656501 or http://dx.doi.org/10.2139/ssrn.2656501, accessed 1 May 2018.
39. Savelyev, A., 'Contract Law 2.0: «Smart» Contracts As the Beginning of the End of Classic Contract Law' [2016] Higher School of Economics Research Paper No. WP BRP 71/LAW/2016, https://ssrn.com/abstract=2885241 or http://dx.doi.org/10.2139/ssrn.2885241, accessed 1 May 2018.
40. Sberbank press release, dated 29 November 2017, https://www.sberbank.ru/en/press_center/all/article?newsID=9f676571-5219-4cfb-bbb7-c9c6e1de983a&blockID=1539&regionID=51&lang=en, accessed 1 May 2018.

ETERNAL DIGITAL LIFE: POST-MORTEM MANAGEMENT OF DIGITAL ASSETS

Bronušienė Simona[1]

Abstract

The article aims to analyse the future of digital estate planning, outlining the main features of digital asset, the troubles to define it, the property rights in digital assets and possibility to transfer them upon the death of their holder. The main distinction of the inheritance of "virtual property" comparing it with the real or personal one is that most of this property is located in the online platforms owned by the third parties or in the clouds and the transferability of digital assets is linked to the accessibility to digital accounts. The question of accessibility mostly is regulated by private agreements and it differ related to the assets and the online service provider. The other important question explored in digital estate planning is data protection of the deceased, does he or she has a right to privacy and what are possible solutions to deal with the succession of the digital assets.

Key words: digital asset, digital account, ownership, data protection, succession.

Introduction

The internet and computers facilitate nearly every aspect of our personal lives. Our personal records, tax filings, bills, music, communication, books, photos, videos, and even journal entries are stored on our computer or in "the cloud"[2] in digital form. The seemingly ever-expanding usage of digital devices means that individuals increasingly handle many routine aspects of life online. Banking, shopping, and communication are done, at least in part, online by a substantial number of people. We are enjoying our digital life and rare who thinks about the final accord and what will happen to all that good we have created, shared or uploaded during our lives when we die.

Statistics, showing the involvement of the society in digital activities, are impressive. For example, the number of active Facebook users from 1 bilion in 2012 has raised to more than 2 bilion in 2017[3]. In Europe, over 307 million people are on Facebook. From European countries it is mostly used in the UK. Every second five new profiles are created. Every 60 seconds on Facebook 136,000 photos are uploaded what make total 300 million photos per day[4]. People think that "technology has made them feel more connected to each other", that it helps them to keep up with what is going on in the world and that "high tech is so much a part of their lives"[5].

Together with digitalization new expressions come into our daily vocabulary, such as digital life style, digital natives[6], digital twins[7] and digital asset. There is no doubt that in the near future digitalization will cover most aspects of our life. Society is transforming traditional family heirlooms and social accoutrements into digital assets. Digitalization of videos, photo albums, social networking and e-mails make an incredible amount of digital assets. Such fashionable movements as "paperless society" or "go green" also promote the use of digital assets instead of "normal" ones we used to use for ages. A company's value is no longer just linked to employees, physical goods, and property, but now encompasses a vast array of digital assets. These digital assets, including: mailing addresses, online

[1] *PhD student at Vilnius University, Faculty of Law, and at University Paris Nanterre, Faculty of Law. Research interests include international private law and comparative law, particularly international succession and family law. Email: alesimona@gmail.com*

[2] The "cloud" refers to a network of computer servers or related software owned and maintained by a third party and which is accessible through the internet. *See* N. M. Banta, 'Inherit the Cloud: The Role of Private Contracts in Distributing or Deleting Digital Assets at Death' (83 Fordham L. Rev. 2014) pp. 800-801.

[3] See https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

[4] See https://zephoria.com/top-15-valuable-facebook-statistics/

[5] See https://zephoria.com/top-10-valuable-snapchat-statistics/

[6] Digital natives may be defined as a population that satisfy the following criteria: born after the year of 1980; have access to digital technology; and have skills to use digital technology "in relatively advanced ways. *See* E. Harbinja, 'Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could Be the Potential Alternatives' [2013] 10 SCRIPTed 19, p. 21.

[7] Digital twins may be defined as digitally transformed physical goods and tangible services, exact replicas or avatars of the physical product.

stores, photographs, bank accounts, payroll systems, computer software, business plans, music, and videos, are considered the most crucial and valuable company assets. The digitalization of business assets has enabled electronic commerce ("e-commerce") to become a vital business operation and valuable market[8].

This digital evolution should bring some changes to legal regulation too. At the moment most issues of digital legal relations are covered by private agreements, but during the last years it is observed that private regulation is not sufficient to safeguard the interests of all the parties involved, especially of the natural persons, the main actors on digital scene.

In Europe we still keep silence talking about the digital person and his life, which in many cases may differ from the natural one, as well as the moment of death, which could be not the same and digital person may live for ever[9]. Moving from molecules to terabytes changes our environment and the goods we have, use and may devise. At the moment we do not collect physical photo albums, books in the shelters and so on, we collect data, information. So the question arises – what kind of information do we have, where is it located and under which conditions, is it the part of our property which can be transferred upon our death to the heirs and beneficiaries? And finally who is playing the first violin in this digital world – me, digital persons, the user, or the owners of the online platforms, clouds and etc.?

1. What is digital asset?

Currently, there is no universal definition of a digital asset or digital estate. For example, the 10th edition of Balck's Law dictionary does not provide any definition of "digital". But, as it was shown above, digital lifestyle produces more and more digital items. If it is quite clear how the things, a person possessed, are transmitted upon her death, the succession of digital ones is still under the question. Generally, upon a person's death everything she had is transferred to her beneficiaries under the will, if a person has signed it, or to her heirs under the law. The right to pass on property is one of the constitutional rights. Traditionally, the support for this right as sacrosanct includes the following rationales: (1) the right to transfer property at death is natural law; (2) it encourages wealth accumulation and discourages waste; (3) it produces happiness by strengthening families; and (4) it is the most administratively efficient means to dispose of property at death[10]. According to the doctrine of family solidarity, it is presumed that most of the goods, held by the deceased, should be inherited by his family members, children, spouse, parents and others.

The right to transfer the things the person had is one of the main elements of the property right, which, in general, is not defined by the things that we own, but rather, as a bundle of rights in things around us[11]. Generally, property is divided into two types: real and personal. Personal property is further divided into two subcategories: "tangible (car, furniture, jewelry, art, clothing, appliances) and intangible (stocks, bonds, patents, trademarks, copyrights)." During the last decade the new form of property has developed – "virtual property" which would include things such as "a website, a bidding agent, a video game character, or any number of other intangible, digital commodities" and it may be used as a synonymous for digital assets[12].

Different sources provide various definitions of digital assets.

"Digital assets" is broadly defined as any asset that "exists only as a numeric encoding expressed in binary form." For example, information stored on the internet, photographs, account information, videos, electronic documents, software, e-mails, and digital applications are all types of possible digital assets. Essentially, digital assets include any electronically stored information. Digital assets will not include

[8] J. P. Hopkins, 'Afterlife in the Cloud: Managing a Digital Estate' [2013] 5 Hastings Sci. & Tech. L. J., p. 215.
[9] For example, by end of 2012, probably thirty-million Facebook profiles have outlived their owners. *See* J.P. Hopkins, *Ibid*., p. 210.
[10] E. E. Subotnik, 'Copyright and the Living Dead? Succession Law and the Postmortem Term' [2015] 29 HARv. J.L. & TECH. 77.
[11] N. M. Banta, 'Property Interests in Digital Assets: The Rise of Digital Feudalism' [2017] 38 Cardozo L. Rev., p. 1104.
[12] J. Conner, 'Digital Life after Death: The Issue of Planning for a Person's Digital Assets after Death' [2011] 3 Est. Plan. & Cmty. Prop. L.J., p. 304.

electronic or digital devices such as phones or computers, but does include the information stored on these electronic devices[13].

As digitalization covers different aspects of our lives, it may be helpful to think of digital assets in terms of four different categories: personal, financial, business, and social media. Personal assets are files that are "typically stored on a computer or smartphone or uploaded onto a web site," including photographs, videos, or even music playlists. Social media assets, on the other hand, generally entail social interactions with a network of people through various mediums, including websites such as Facebook and Twitter, as well as e-mail accounts. Financial assets may include bank accounts, Amazon accounts, PayPal accounts, accounts with other shopping sites, or online bill payment systems. By contrast, business assets generally include customer addresses and patient information[14]. Other authors split up digital assets into five categories[15]: electronic documents, for example, e-mail, text, Microsoft Word document, Microsoft excel spreadsheet; social media outlets, some examples include Facebook, Twitter, Instagram, Linked-in, Snapchat; financial assets, for example, PayPal, Google Wallet, Amazon, eBay, online bank accounts, YouTube Account that generates ad revenue; business assets, such as digital customer information, databases, trademarks, tradesecrets, websites, domain names; and miscellaneous assets, some examples include blogs, music, videos, online gaming, loyalty programs.

The lack of a clear and common definition of digital assets makes unpredictable the situation of the involved parties. First attempts to specify digital assets by law and to regulate the accessibility to it after the death of its holder were made in USA. At the beginning of 21 century only some States started to govern these issues, later on the uniform act project was proposed as a guideline for the other States to follow. Accordingly, in 2014, the Uniform Law Commission (ULC) issued the Uniform Fiduciary Access to Digital Assets Act (UFADAA), which after reactions of online service providers' was modified issuing the RUFADAA. The RUFADAA defines a digital asset as "an electronic record in which an individual has a right or interests" which "does not include an underlying asset or liability unless the asset or liability is itself an electronic record"[16]. This distinction is important because digital assets have the unique potential to change from an intangible asset to a tangible one. A digital asset, such as a digital photo or email, can change from intangible property to tangible property simply by printing out a copy of it[17]. Such an item upon death of its owner will be transferred according to the common inheritance rules, while the succession of digital ones still poses many challenges. The first of which is if the digital item is an asset which can be transferred as a part of person's estate.

Generally, an asset is defined as „an item that is owned and has value"[18] . According to it, the main questions that should be answered willing to define digital asset are if digital items are owned by their holder and do they have any value.

The value of digital assets mostly depends on the kind of the asset. Although some of them, like personal email accounts, may not have extrinsic monetary value, they may hold significant emotional value. Moreover technological innovations expand the list of digital assets which are becoming more economically valuable[19]. Some studies show that, on average, internet users have roughly $37,438 in digital assets across a variety of digital devices and platforms[20].

[13] J. P. Hopkins, *Ibid*., p. 211.
[14] N. Cahn, 'Postmortem Life On-Line' [2011] 25 Prob. & Prop., pp. 36-37.
[15] E. Sy 'The Revised Uniform Fiduciary Access to Digital Assets Act: Has the Law Caught up with Technology' [2016] 32 Touro L. Rev., p. 650.
[16] J. Ronderos, 'Is Access Enough: Addressing Inheritability of Digital Assets Using the Three-Tier System under the Revised Uniform Fiduciary Access to Digital Assets Act' [2017] 18 Transactions: Tenn. J. Bus. L., p. 1048.
[17] J. Conner, *Ibid*., p. 304.
[18] 'Black's Law Dictionary 140' (2014) 10th ed.
[19] N. M. Banta, 'Inherit the Cloud: The Role of Private Contracts in Distributing or Deleting Digital Assets at Death' (83 Fordham L. Rev. 2014) p. 801.
[20] Accordingly, the assets were broken down into categories, showing personal memories at around $19,000, personal records at $7,000, career information at $4,000, hobbies at $3,000, personal communications at $3,000, and entertainment files at $2,000. See J.P. Hopkins, *Ibid*., p. 221.

The second element of an asset is ownership, which is usually defined as the right to use, transfer, exclude, control, devise, or destroy[21] . The ownership of digital asset mostly depends on the category to which it belongs (personal, social media, financial and business) and the place where it is located.

The distinction of these two elements – ownership and value – is crucial willing to define digital assets, because most of the digital assets are stored online under the agreements with the third parties, called "terms of services" (TOS). In such a way it could be opted, that "digital assets" are more likely to be services, which are not inheritable, than assets. But from the other side TOS contracts provide the access to the account. A person's "digital account" may consist of a variety of personal assets, including e-mail accounts, software licenses, social networking accounts, social media accounts, file sharing accounts, financial management accounts, and domain registration accounts. Simply put, digital assets are the actual files, and digital accounts are the "access rights to files"[22]. This account/asset distinction can be critical; access to the digital account is a service provided by the online platforms under the TOS agreements and usually it is not inheritable, but this service could not be collated to the property rights of digital assets created or otherwise got by the digital account holder and forming the content of his account.

Without a clear definition of the digital asset and property rights in it, the inheritability of the asset is controlled by a private contract between a company that provides a service (access to digital account) or product (like Google, Facebook, Yahoo! or Apple) and an individual who uses the company's services or purchases a digital product[23]. What cannot be left unseen is that private contracts, regulating services, which online platforms do provide, and limiting the access to the deceased' digital account, restrict the deceased' right to transfer his property. That is why it is important to find one universal definition of digital assets in order to predict what and under which conditions may be transferred to the heirs or beneficiaries. As technologies develop much faster than the legislature, the law should be broad enough to incorporate new forms of technology, setting out the main features of digital asset but not determining it strictly.

2. Who owns the digital asset?

The essence of succession is that the deceased cannot transfer more rights to his estate to his heirs or beneficiaries as he had. If the rules of succession of real and personal property are quite clear and stable during the ages, the inheritance of "virtual property" or digital assets is a new field of law, mostly related to contract and property law.

All digital assets must be stored in some physical location be it with the owner, a third party, or on the "cloud". Digital assets located on a digital device owned by the deceased can be transferred in the same manner as all of his or her other assets. While many people store their digital assets on their own digital devices, people are increasingly using online or cloud-based services to store their digital assets. When digital assets are stored on the cloud, the assets are organized by a service provider. In order to take control of a digital asset stored on the cloud, the account name, user name, and password will be needed. To protect the digital assets and keep each individual's assets separate, these service providers require the user to create a unique account identifier[24]. As it was mentioned above, digital account and digital asset held in it are not the same categories of law, because first contains the service – access to the digital account, provided by online platform, and the second – the goods created or obtained by the account holder. That is why accessibility as well as inheritability is the most significant issue regarding digital asset ownership.

Even if ownership and transferability of assets are linked together, when we talk about digital assets it does not mean that all the time they can be transferred. The main obstacle, as it was mentioned above, is the definition of digital assets and its link to the electronic services provided by the third parties. As many of our digital assets are contained in the digital accounts, the conditions of the use, transfer, exclusion, control, devise, or destruction of digital assets are set in the contracts between the online

[21] N. M. Banta, 'Property Interests in Digital Assets: The Rise of Digital Feudalism' [2017] 38 Cardozo L. Rev., p. 1104.
[22] M. Perrone, 'What happens When We Die: Estate Planning of Digital Assets' [2012] 21 CommLaw Conspectus, p. 188.
[23] N. M. Banta, 'Inherit the Cloud: The Role of Private Contracts in Distributing or Deleting Digital Assets at Death' (83 Fordham L. Rev. 2014) p. 802.
[24] J. P. Hopkins, *Ibid*., p. 223.

service providers and account holders and furthermore ownership rights of digital assets held online by service providers might vary depending on the type of asset and service provider. Online service provider gives us a right to create digital account, to connect it, to put there information we want and we need. This contract, often referred to as "terms of service" (TOS) is almost never negotiable and will likely control the transferability of digital assets. Most TOS contracts do not specifically address ownership rights and transferability upon death nether less they state that account user owns all of the material he or she creates, upholds, or receives[25]. Moreover most of the online service providers state that their first priority is to protect the user, who undoubtedly signed a "privacy agreement", which often provides that under no circumstances will the website release the person's personal information[26].

In order to answer what and under which conditions could be succeeded, it should be explained what rights the holder of digital assets has. As the ownership of digital asset mostly depends on the category to which it belongs (personal, social media, financial and business) and the place where it is located, further will be presented the situation of the main types of digital assets.

Personal items: photos, video, text, Microsoft Word document usually are held in the personal computers, phones or other devises and they are created, used and owned by the person who holds them. Difficulties arise with the items that are not created by the holder but are obtained by him. Contracts for music, books, and videos go to great pains to state that the purchaser is buying a license to use digital content and not a fee simple interest in the digital content itself. Because the sale is only of a license to access digital content, the contracts expressly forbid the user from selling, leasing, distributing, renting, broadcasting, licensing, transferring, or conveying the interest to a third party[27]. Such conditions are obvious in order to protect the copyrights of the creator and to combat the copyright piracy. But at the same time it creates the problems with the property rights. For example, my dad had vinyl collection. When he passed away my siblings and I divided it. At the same time my dad had a big music library collection on Amazon (digital assets) which according to the TOS contract gives only non-exclusive, non-transferable right to use purchased music. Account holder of digital media has not absolute right to possession because the platform also possesses digital files. Even if account holder keeps the control over excluding others from the account but his right to use, like the right to possess, is dependent on the proper functioning of the platform. As it was mentioned before, account holder does not obtain an item but only a license to it and there is no mechanism to transfer the digital media nor to make a request for it stored in the deceased account holder's account. The expanding digital ®evolution replace physical, tangible goods that were freely devisable by digital ones. They hold a great deal of monetary values to an estate, that is why it should be revised if the purchase of the license but not of the digital media as such is the appropriate decision in order to regulate these new relations and to ensure the development of property rights.

Social media items: e-mail and social networking platforms consistently protect a user's property interests in the content she creates, uploads, or stores on the platforms. These contracts assume that a property interest exists in the content of an account. The nature of e-mail and social networking platforms lends itself to a wide range of uses by account holders. E-mail and social media are digital platforms designed to share and transfer the contents of an account with just a few clicks of a button. An e-mail account and social networking user can transmit data, personal notes, pictures, videos, status updates, recipes, book reviews, documents, and news. E-mail and social networking account holders have possession of their accounts because they have control over the account and they intend to own their accounts. Google, Yahoo, Microsoft in general in their contracts state that they do not claim ownership of the content created and that the holder of the account retain ownership of any intellectual rights that he or she hold in that content. Nevertheless, there should be made a difference between the transferability of the content of the accounts and transferability of individual's access to the account which is not designated to be transferred to others.

[25] *Ibid*., p. 225.
[26] J. Conner, *Ibid*., p. 305.
[27] N. M. Banta, 'Property Interests in Digital Assets: The Rise of Digital Feudalism' [2017] 38 Cardozo L. Rev., p. 1106.

The very name "*e-mail*" is an abbreviation for electronic mail. As a digital transformation of a physical thing, individuals have certain expectations about their e-mail accounts that derive from experience with physical mail. However e-mail could not be transferred as easy as the written letters. It can be illustrated by well-known old case of American solder Lance Cpl. Justin Ellsworth. The case of Justin Ellsworth showed that the owner of the online platform, Yahoo in this case, cannot give even the access to the account of the deceased if family member or other loved ones do not know the identifying information – username and password. Even if the court has allowed to give an access to the account, Yahoo provided only the list of the letters but not the content of them. During the previous wars, if a soldier died, his personal effects were put together and sent to his family, including any letters he had in his possession. These could've been letters that he sent or received. There was no internet, no email, the soldiers routinely on the post office mailed letters home to their families the old fashioned way pen to paper and anxiously awaited letters from the home. Today, in the digital age, letters have become emails, pen and paper have become laptop computers and PDA's and you don't have to depend upon the post office to get that letter to or from the home front. The post office has been replaced by companies who, if you believe Yahoo, become the owner of the message you send through them. Can the post office keep your letter? No. Do you have to sign an agreement with the post office that says they own your mail and if for some reason you can't take delivery anymore that they can just destroy it? No. Even if this famous battle has finished and the parents of the young solder could read the last e-mails of their son and make a memorial, but the problem of the ownership of e-mail and access to it still exist[28].

Social networking platforms such as Facebook, Twitter, LinkedIn give similar protections to the content and information posted on their site by stating that users "retain" ownership and rights over the content they submit[29]. However social networks are a bit different from e-mail because they are much more public. Even so the account holder still has a right to exclude someone from viewing his posts or to choose to post publically or privately, but it is not applied to social network site, which cannot be excluded from accessing our post.

Instagram's policy on accounts of the deceased aligns closely to that of its parent company, Facebook. Users' accounts can either be memorialized or removed. However, there exists one big difference between Facebook and Instagram – while Facebook now allows users to choose which of these options they prefer before they die – Instagram does not. Thus the decision of what happens to your Instagram (and your picture-perfect selfies) is out of your hands. If you see an Instagram account of a deceased person (or you happen to be that deceased person), the account can be reported to Instagram for memorialization. Immediate family members are also able to request the account be deleted.

Financial digital items such as online bank accounts, PayPal account or Google Wallet give the right to access the content which is owned by the holder of the account. However contracts of digital financial items forbid to transmit the personal information, identifying the user, to the third parties in order to protect and to secure the content. So even if the owner of the financial digital items leaves his username and password to the beneficiaries, these are not allowed to access the content without the permission of the competent institution.

Different situation is with the *digital currency* which is not safeguarded by the third-party intermediary, such as a bank or PayPal. At the moment more and more popular become digital coins, such as bitcoins. Anonymity is very important for those who use the digital currency that is why nobody knows who in fact uses it. The main factor is to be certain that other people will not have access to your money. But other ones may use your digital wallet if they have an access to it. So the main issue is how and to whom to leave the keys of your cryptocurrency wallet.

Also very important issue is *digital liabilities*. Each of us have various passions, for example, gym memberships, computer games, films, magazines online and so on. How to deal with them? Of cause, all these monthly payments are known for your account holder, usually some financial institution, but at the same time it may take some time till the heirs or executors will set up all these subjects, so during this time quite a big sum of money of the deceased person may be lost for nothing.

[28] It is very sensitive especially in the case of the suicide persons when the living ones wish to know the reasons of such a commitment.
[29] N. M. Banta, 'Property Interests in Digital Assets: The Rise of Digital Feudalism' [2017] 38 Cardozo L. Rev., pp. 1105-1106.

The ownership of **business digital items** also belongs from the kind of it and the place where they are held and by whom. Data bases, custom information which is created by the company belongs to the company but if these data are used publically or if it is not protected from downloading or it is not named as the competitive information of the company that cannot be disclosed to the third parties for certain period of time, it could be difficult to prove the authentic property rights of it.

At the end, it is obvious that to transfer digital assets may be difficult, first of all because most of them are located in the digital accounts. Access to it is regulated by private agreements, which recognize log in as private information which cannot be freely reached by the third parties such as the heirs or beneficiaries. That means that the right to devise digital assets and to decide to whom and what should go after the death of the account holder is limited by the online service providers. Willing to avoid this, the account holder and the owner of the digital assets should properly prepare his virtual property to be transmitted.

3. Did the deceased prepare for a digital asset transfer upon death?

Usually we do not think about our death and that is the reason why we are not preparing to pass away. We are leaving not only all the goods we have created or obtained during our life but also unsolved problems and answered questions for others, our loved ones, to deal with. As it was shown before, the digital assets most often have not a monetary, but personal, emotional and historical value for the future generations. The questions related to their inheritance are still unclear, left for individual regulation of the private parties and the decisions of the courts according to the individual circumstances of each particular case. In order to obtain the digital assets usually first of all the heir, beneficiary or fiduciary has to access to digital account where the digital assets are held. The most relevant issues for access are: (1) privacy for decedents and (2) preventing liability for personal representatives when they access a decedent's online account[30].

3.1. Does a deceased person has a right to privacy?

Deceased person's privacy is discussed broadly in the context of their personal data, and whether this data should be protected through data protection legislation. One of the most significant arguments against the legal recognition of post-mortem privacy is the lack of real harm to the user, that is, the deceased cannot be harmed or hurt[31]. However users do have interests in what happens after their death, in the digital realm this interest is greater than in the offline world, due to the prominence and volume of personal data disclosed online, and the importance of digital assets in creating one's online identity[32]. Social networks pose a significant threat of post-mortem identity theft because the death of an individual leaves his or her online presence vulnerable to hackers who could change, steal, or remove the tangible or digital property of the decedent.[33] Social network account holders, who passed away, are particularly vulnerable to identity theft, because they have no way to monitor or combat attacks by cybercriminals.

As it was mentioned above the access to digital accounts is regulated by private agreements which preview this identifying information as the personal one of the account holder. So the question arises, if a deceased person has a right to privacy and could post-mortem personal data be defined.

On 14 April 2016 the EU Parliament finally approved General Data Protection Regulation (GDPR) No 2016/679, which replaces the Data Protection Directive 95/46/EC and which was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizen's data privacy and to reshape the way organizations across the region approach data privacy[34].

---

[30] J. Ronderos, *Ibid*., p. 1036.

[31] H. Beverley-Smith, 'The Commercial Appropriation of Personality' (Cambridge: Cambridge University Press 2002) p. 124.

[32] L. Edwards and E. Harbinja, 'What Happens to My Facebook Profile When I Die?: Legal Issues Around Transmission of Digital Assets on Death', in Digital Legacy and Interaction: Post-Mortem Issues (Springer: Human–Computer Interaction Series 2013) pp. 115-144.

[33] C. Ray, 'Till Death Do Us Part: A Proposal for Handling Digital Assets after Death' [2013] 47 Real Prop. Tr. & Est. L.J., p. 587.

[34] *See* https://www.eugdpr.org/

Everyone will agree that personal data indeed does not change because of the fact that its holder passed away, so it contains any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[35]. Despite this broad definition of personal data, deceased person is not a data subject according to GDPR because this regulation does not apply to the personal data of deceased persons[36]. The same exclusion was foreseen in the national laws of data protection of the most European countries[37]. Data Protection Directive also did not mentioned deceased's data in any context. But Directive as well as GDPR leaves discretion in implementation to EU member states to extend this protection and to provide for rules regarding the processing of personal data of deceased persons. However most of the EU member states did not utilize the possibility of extending the definitions of personal data and data subjects in their legislation[38].

Personal data protection is one of the *human rights* – the right to inviolability of one's private life. The question is – do the human rights survive their holder? In general human rights apply only to living persons and the right to privacy dies with individual[39]. The main argument for this is that dead person cannot give consent to use or changes in his personal data or contribute to any balancing of interests which may be required. But some states, for example, Estonia, has found the way to regulate this issue stating that the consent of a data subject shall be valid during the life of the data subject and thirty years after the death of the data subject, unless data subject has decided otherwise[40]. As it was mentioned before it is previewed that deceased person has no interests in his privacy protection. But it is hard to agree with such opinion because deceased person, especially in this digital era, has a lot of personal data online and it could be harmful for him, for his reputation, good name if some of these personal data (for example, some love letters) are disclosed in improper way. It even could bring a big financial loss for him, or, to be more precisely, for his estate and the interests of his beneficiaries[41].

Talking about the digital assets planning and possibilities to inherit them it is clear that a lot of digital assets contain personal data. Personal data is recognized as the new "oil" of 21st century and it will emerge as a new asset class touching all aspects of society[42]. That is why it is very useful to look at the personal data not only from the human rights or torts perspective but also to evaluate them as the property rights. It should be mentioned that *propertisation* of personal data is a new trend in the field of privacy policy and data protection[43]. General features of the new regime that resemble a property model, could be found in GDPR too. For example, GDPR proposes two innovations: right to be forgotten and right to data portability.

---

[35] Article 4 of GDPR.

[36] Recital 27 of GDPR.

[37] For example, Lithuanian law on legal protection of personal data prescribes that it is not applied to the personal data of the deceased persons. The new proposal of this law stays silent about the protection of personal data of deceased persons but as it should be applied in convenience with the GDPR, which is not applied to the personal data of deceased persons, it is obvious that the same exclusions is left.

[38] E. Harbinja, 'Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could Be the Potential Alternatives' [2013] 10 SCRIPTed 19, p. 27.

[39] According to the European Court of Human Rights case law, Article 8 grants protection only to the living. In numerous cases, the Court has refused to recognise this right to the deceased, unless their privacy is connected to the privacy of the living individuals (see for example, *Estate of Kresten Filtenborg Mortensen v.Denmark* (dec.), no. 1338/03).

[40] Par. 6 Article 12 of Estonian Personal data protection act, *see* https://www.riigiteataja.ee/en/eli/509072014018/consolide.

[41] For example, in the German Marlene Dietricht case the claimant, the only child and the hier of the famous actress Marlene Dietricht, was claiming from the defendant, the company which after the death of the actress produced a musical on the life of Marlene Dietrich "Tell me where the flowers are", injunctive relief, a declaration of his duty to compensate for harm and provision of information in respect of the use of the picture, name and signature of Marlene Dietrich, on the basis of her own rights and her legal status as executrix for the estate of her mother. She considers that the claims she is making arise from infringement of the posthumous personality rights of her mother. The court decided that The components of the right of personality which are of financial value remain after the death of the holder of the right of personality, at any rate as long as the non-material interests are still protected. The corresponding powers pass to the heir of the holder of the personality right and can be exercised by him in accordance with the express or presumed will of the deceased, https://law.utexas.edu/transnational/foreign-law-translations/german/case.php?id=726.

[42] 'Personal Data: The Emergence of a New Asset Class' [2011] World Economic Forum, file:///C:/Users/alesi/Desktop/DIGITAL%20succession/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

[43] E. Harbinja, *Ibid*., pp. 29-31.

Right to be forgotten in GDPR is not the same as it was in Data Protection Directive because it consist first of all of the right to erasure of personal data which was extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data[44]. It will be interesting to see if and how the judicial practice change[45].

Right to data portability means that he data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller[46]. It adds a significant new value to the data protection regime and could empower individuals and provide for a better control over their personal data, as they would be able to leave the provider/platform that does not satisfy their privacy requirements, for instance, or just shift to a provider with better services[47].

Comparing these data protection novelties with the technics of post-mortem digital estate management we can stress some common points: 1) right to erasure of personal data is foreseen by private online services agreements where the account user may identify that after his death he requires his account to be erased. However if there is no contract, then situation becomes more complicated because there are no legal regulation concerning these issues and the terms of services agreements regulate it differently. 2) The same is with the right to data portability, because data protection legal acts are not applicable to the personal data of the deceased and terms of services agreements usually strictly prescribes that the personal data cannot be transferred to any third person upon the death of the account holder. So even if the data subject being alive has indicated that after his death he would like his personal data to be transmitted to another platform, for example, the online cemetery of the digital persons, it could not be done. And it is difficult to find convincing arguments why because personal data hold a lot of features of property rights and according to the recent regulation it could be managed in many ways as any other material asset.

According to what is mentioned above, it could be concluded that a deceased person do has a right to privacy. As it is not possible for a deceased person to manage her personal data and access to it, it should be previewed the ways she could give access to others to the personal information contained online.

3.2. How personal representatives could access the digital account?

In most European countries the heirs “step into the shoes” of the deceased. There are no specific rules for digital inheritance and digital assets are therefore inherited in the same manner as any other type of asset. But if the contract of online services stipulates what happens to the account and the digital assets after the death of the user, the heir should act according to it. So, as it was mentioned above, the transfer of digital assets in most cases is left to the private disposition.

First attempt to regulate the accessibility to digital assets after the death of its holder where made in USA. At the beginning, the Uniform Fiduciary Access to Digital Assets Act (UFADAA) proposed to give personal representatives implicit authority to access a decedent's online accounts. In other words, the UFADAA presumed that the decedent would have wanted the personal representative to access and manage his or her online accounts. Naturally, online service providers feared that this presumption of authorization would undermine a decedent's privacy after death because the decedent does not have to authorize the access of electronic communications (e.g., emails, social media accounts, etc.). In the new drafted RUFADAA it was foreseen that if users consented to disclosure of electronic communications, then the online service provider would disclose that information to a personal representative. Without this

[44] Article 17 and recital 65, 66 of GDPR.

[45] For example, On March 9, 2017, the Court of Justice of the EU (CJEU) in a case C-398/15 *Manni* handed down a ruling limiting the reach of its prior “right to be forgotten” jurisprudence (case C-131/12 *Costeja/Google Spain*), by holding that the right does not prevail over society’s interest in access to official public records of company details required by law.

[46] Article 20 and recital 68 of GDPR.

[47] E. Harbinja, *Ibid*., p. 35.

consent of the decedent, personal representatives can only receive a catalogue of the electronic communications of a deceased user.

The RUFADAA created a three-tier system for a decedent to authorize an executor to access his or her online accounts. Specifically, a decedent may authorize a fiduciary to access the online accounts via an online tool agreement, which overrides any will or TOS agreement. Otherwise, a decedent may authorize an executor to access the accounts under a will, thereby overriding a TOS agreement. Absent authorization by an online tool agreement or will, the TOS agreement controls access to the online account[48]. At the moment this three-tier system is the only widely recognized tool used by different online service providers, private estate planners and public.

Some authors argue that *private contracts*, not wills, are the most efficient manner to transfer property at death. Simply put, individuals could transfer digital assets at death under a private agreement between the online service provider and user[49]. A TOS agreement is distinct from an online tool agreement under the RUFADAA because an online tool only controls the designation of an individual that may access a person's account at death, unlike a TOS agreement which "controls the relationship between a user and a custodian." For example, Facebook, a social media platform, provides a legacy contact agreement (i.e., an online tool) that allows a user to designate an individual to manage the user's account upon his or her death.

To leave digital assets by *will* is not always the best option because, as it was mentioned above, digital assets usually are held in the online accounts which are governed by the TOS agreements. TOS agreements usually give only the access to the accounts or the license to use digital assets but not digital assets as such. License to use a website expires upon a death and wills tend only to deal with assets that survive death and may not include online accounts that a person has been granted a license to use. For this reason, if the license granted to persons to use the websites does in fact expire upon death, whoever receives the usernames and passwords has no legal right to use or access the information contained in the accounts.

Also it should be clearly distinguished what you are leaving by a will: digital assets or access to digital assets. If you are leaving digital assets that means that they should be well inventoried. But the internet moves quicker that we do so probably making a will it is not possible to mention all the digital assets that we will have at the time of our death. So most often we are leaving the access to our digital assets that means username and password of digital account. Each of us have various digital accounts and various usernames and passwords, which we even don't remember very well. Also we are obliged to change password of our accounts in some timeframes because of security reasons. So even if we are writing the identifying information in the will there are no guaranties that it will be not changed upon our death. Is it possible to change a will all the time? Perhaps that not. It is too expensive to go each time to the notary. Besides it should be noticed that will is a public document so the identifying information – your username and password will be disclosed not only for those to whom you wish to leave your digital assets but also for the other beneficiaries.

At the moment there are more and more private suggestion for digital estate planning. One of them is *"electronic will"*. It could be made, changed very quickly, even not moving from your chair, just by several online clicks. But people are urged to remember that in most countries a will requires certain formalities and the absence of these formalities can render one's good intentions legally invalid[50].

Besides, wills can be used to create a special *"digital executor"* or "social-media executor"[51], as someone who would have the explicit authority and duty to manage the estate's digital assets[52].

An additional option is to provide an *informal letter* to your beneficiary, that lists important user names, passwords, security codes, and other information needed to access online accounts. This letter can also provide specific instructions as to how the executor should handle the digital assets.

---

[48] J. Ronderos, *Ibid*., p. 1038.

[49] N. M. Banta, 'Inherit the Cloud: The Role of Private Contracts in Distributing or Deleting Digital Assets at Death' (83 Fordham L. Rev. 2014) p. 853.

[50] M. Perrone, *Ibid*., p. 203.

[51] A. Berlee, 'Digital Inheritance in the Netherlands' [June 2017] EuCML, p. 259.

[52] J.P. Hopkins, *Ibid*., p. 234.

A *"password vault"* is another tool that can be used to ensure that the proper usernames and passwords are passed on for any Internet accounts. Password vaults are available for download via several websites. The crux of these vaults is that a person can store several usernames and passwords into the vault, which is protected by one single "master password." Thus, the testator, *de cujus* would only need to supply his family with the master password, and then his family would have access to all important usernames and passwords regardless of how often the testator changed them[53].

Even a variety of digital estate planning services have developed, especially in USA, to deal with the new challenges facing digital asset management and disbursement, privacy, security, digital ownership and longevity concerns remain unanswered by online digital estate services. Moreover as digital estate planning is some kind of startup services there is always uncertainty with the business continuity. If the company goes out, how you or heirs, beneficiaries could demand to continue online estate planning, for example, keeping password vault or to transmit online testament. All these issues show that it is not enough to leave the digital estate planning to private regulation. Some governmental solutions should be proposed too.

Conclusions

Digital assets are becoming pervasive in everyday life and it is more and more important to deal with them after death. The legal questions surrounding digital inheritance span several areas of law: property, contract, human rights and data protection. First of all, it should be distinguished the main features of digital asset in order to define it. The digital assets are overviewed specifying four main categories of them: personal, social media, financial and business items. The definition of digital assets is helpful trying to determine what kind of rights do we have in them. As most of these digital assets are located in the online platforms owned by third parties or in the clouds, the property rights of digital assets are dependent on the accessibility to the digital account, which is usually regulated by private agreements. The lack of the governmental attention to regulate this field of law leaves the fate of digital assets in the hands of online service provider but not of their owner. This evokes the need of coherence between succession law and the other fields of law. Also it poses trouble in deceased identity protection, because most of the digital assets, held online, contain personal information. However, according to the newest regulation, deceased person is not a data subject, because right to privacy “dies” together with her holder. Despite this, it was analyzed the situation of digital assets in the field of data protection and presented several solutions for digital estate planning.

Bibliography

1. N. M. Banta, ‘Inherit the Cloud: The Role of Private Contracts in Distributing or Deleting Digital Assets at Death’ (83 Fordham L. Rev. 2014).
2. N. M. Banta, ‘Property Interests in Digital Assets: The Rise of Digital Feudalism’ [2017] 38 Cardozo L. Rev.
3. A. Berlee, ‘Digital Inheritance in the Netherlands’ [June 2017] EuCML.
4. H. Beverley-Smith, ‘The Commercial Appropriation of Personality’ (Cambridge: Cambridge University Press 2002).
5. ‘Black’s Law Dictionary 140’ (2014) 10th ed.
6. N. Cahn, ‘Postmortem Life On-Line’ [2011] 25 Prob. & Prop.
7. J. Conner, ‘Digital Life after Death: The Issue of Planning for a Person's Digital Assets after Death’ [2011] 3 Est. Plan. & Cmty. Prop. L.J.
8. L. Edwards and E. Harbinja, ‘What Happens to My Facebook Profile When I Die?: Legal Issues Around Transmission of Digital Assets on Death’, in Digital Legacy and Interaction: Post-Mortem Issues (Springer: Human–Computer Interaction Series 2013).
9. Estonian Personal data protection act, see https://www.riigiteataja.ee/en/eli/509072014018/consolide
10. General Data Protection Regulation (GDPR) No 2016/679.

[53] J. Conner, *Ibid*., p. 317.

11. E. Harbinja, 'Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could Be the Potential Alternatives' [2013] 10 SCRIPTed 19.
12. J. P. Hopkins, 'Afterlife in the Cloud: Managing a Digital Estate' [2013] 5 Hastings Sci. & Tech. L.J.
13. Lithuanian Personal data protection act.
14. 'Personal Data: The Emergence of a New Asset Class' [2011] World Economic Forum, file:///C:/Users/alesi/Desktop/DIGITAL%20succession/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf.
15. M. Perrone, 'What happens When We Die: Estate Planning of Digital Assets' [2012] 21 CommLaw Conspectus.
16. C. Ray, 'Till Death Do Us Part: A Proposal for Handling Digital Assets after Death' [2013] 47 Real Prop. Tr. & Est. L.J.
17. J. Ronderos, 'Is Access Enough: Addressing Inheritability of Digital Assets Using the Three-Tier System under the Revised Uniform Fiduciary Access to Digital Assets Act' [2017] 18 Transactions: Tenn. J. Bus. L.
18. E. Sy 'The Revised Uniform Fiduciary Access to Digital Assets Act: Has the Law Caught up with Technology' [2016] 32 Touro L. Rev.
19. E. E. Subotnik, 'Copyright and the Living Dead?: Succession Law and the Postmortem Term' [2015] 29 HARv. J.L. & TECH.

REGULATION OF SOCIAL-BOTS AND FREEDOM OF COMMUNICATION

Çıkar Ruşen[1]

Abstract

The rapid change in communications technology has profoundly altered the conditions under which we communicate. Smartphones and social media services are dominating the field of today's communication. Moreover, as computer programmes are learning to imitate human behaviour matters become increasingly complex.

This Paper analyses the emergence of social bots from the Human Rights Law perspective. Unlike the topic is commonly viewed it will not primarily ask about how to protect citizens from non-human defamation and from harms caused to the function of free speech in democratic societies through fabricated information. Instead, it will switch the perspective and analyse if and in which cases expression, that is transmitted and composed by machines, is protected by the guarantees of free communication as laid down in Art. 10 ECHR on a regional and Art. 19 ICCPR on a universal level. It will be shown that "not all bots are created equal". The difference in programming between "scripted" and artificial intelligence based chat bots, between bots that follow a given path and those that compose messages from scratch, is significant for their legal classification and the possible protection of their programmer's or propagator's freedoms under the existing Human Rights Law regimes.

More abstractly, this Note will raise the question of whether traditional views on communication freedoms can be maintained. While it is far-fetched (but however popular) to state that the freedoms of communication are "outdated" in times of social media and artificial intelligence, the real task begins when it comes to examining the exact stress points of existing legal concepts. In order to achieve this task, the analysis will not shy away from diving into technical details of the algorithms that make up social bots and—more generally—self-learning machines (Artificial Neural Networks—ANN and Deep Learning), as understanding the details is crucial for the legal assessment of certain regulation options.

Keywords: Social Bot; Artificial Neural Networks; Twitter; Communication; ECHR; ICCPR.

Introduction

The change of communications technology is shaping the way we communicate and ultimately our society. The internet in general, social media services and smart mobile devices already had a major impact. With artificial intelligence systems being on the rise thanks to recent developments in Artificial Neural Network technology and Natural Language Processing[2], new and sophisticated forms of machine-speech come into play. The recent emergence[3] of chat bots on social media platforms and the automated generation of entire news articles[4] raises questions concerning the freedom of expression and its meaning in a changing environment of communication.

In recent news coverage and even scientific literature[5] the rise of algorithmically generated text is oftentimes linked to malicious intent, the infiltration of political discourse and the spreading of misinformation. Popular examples, to name a few, are the U.S. presidential election in 2016, where social

---

[1] *PhD Student in Law, Goethe University Frankfurt, Department of Public Law. The Author's research focuses on information and communications law, international economic law and constitutional law.*

[2] See I. Goodfellow, Y. Bengio, A. Courville,'Deep Learning' (Cambridge, MA: MIT Press 2017) pp. 451-465 for a general (computer science focused) introduction to the topic.

[3] Reports on social bot activity have increased since about 2010, C. Grimme, M. Preuss, L. Adam et al., 'Social Bots: Human Like by Means of Human Control?' [2017] 5 Big Data, p. 279.

[4] Automated Insights Inc. is a company that uses Natural Language Processing to generate news articles. It is inter alia working in collaboration with Associated Press (AP). See Finley, 'This News Writing Bot is Now Free For Everyone', Wired [20 October 2015], https://www.wired.com/2015/10/this-news-writing-bot-is-now-free-for-everyone/; Automated Insights, https://automatedinsights.com/media-coverage with further examples of news coverage on the topic; J. Villasendor, 'Technology and the Role of the Internet in Constitutionally Protected Expression' [2016] 39 Harvard JLPP, pp. 631-641.

[5] E. Ferrera, O. Varol, C. Davis et al., 'The Rise of Social Bots' [2016] 59 Communications of the ACM, p. 96.

bots sent nearly 19 % of the Twitter posts related to the election[6], the Brexit campaign[7] and the conflict in Eastern Ukraine and Crimea[8]. However, in a significant amount of cases social bots are benevolent or even useful[9]. The common meaning of the term chat bot or social bot encompasses different fields of use. Therefore, the first part of this Article will analyse the underlying technology behind machine speech—as far as this is possible without a deeper understanding of computer engineering and mathematics. The description and factual analysis of the different models that can be deployed for Natural Language Processing will be useful for raising the question whether (and in what sense) machine speech is protected by the freedom of expression as laid down in Art. 10 ECHR and Art. 19 ICCPR. So far, this question has drawn considerable attention on the domestic level, especially in the U.S. regarding Google's search engine results and their first amendment protection[10] and most recently regarding bots on social media and newspaper websites[11]. The international debate does not seem to have caught up on the meaning of algorithmically generated speech and its meaning for the protection of free expression by International Human Rights Law yet[12]. Therefore, questions concerning other Human Rights provisions such as property-protection, the right to private life (Art. 8 ECHR) that might also be activated in the context of the use of social bots lie beyond the scope of this analysis. Another restriction to this Paper is that it will only deal with the use of bots by private entities and not by the state.

Finally, the topic must be put into the greater context of changes in communication and social order in general as well as to paradigm changes in International Law, since the emergence of social bots is only one element of a greater development. By doing so, it will be shown that the concept of freedom of expression is far from being called outdated as long as adjustments in the interpretation of the norms in the light of current developments are regarded as an integral element of the normativity of International Human Rights Law norms.

1. Understanding Social Bots

1.1. Brief Introduction to Machine Learning and Natural Language Processing[13]

Natural Language Processing (or Computational Linguistics, depending on the subject field[14]) is defined as the use of human language by a computer[15]. In contrast to a programming language, which is designed in order to allow machines to read clear instructions, natural languages such as English are deeply ambiguous and had therefore been difficult to mimic by computers. Algorithms designed to hold a conversation with humans were a vision of Alan Turing in the 1950s[16], who was one of the most influential computer scientists of his times. Classical applications relied on the definition of probability distributions

[6] A. Bessi, E. Ferrera, 'Social bots distort the 2016 U.S. Presidential election' online discussion [7 November 2016] 21 First Monday, http://firstmonday.org/ojs/index.php/fm/article/view/7090/5653.

[7] P. N. Howard and B. Kollanyi, 'Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum' [2016] Comprop Research Note 2016.1, https://arxiv.org/abs/1606.06356 [cs.SI].

[8] R. Menn, 'Die Macht der Social Bots' [22 October 2016] Deutschlandfunk, http://www.deutschlandfunk.de/wahlkampf-die-macht-der-socialbots.1818.de.html?dram:article_id=369303.

[9] V. Volkmann, 'Hate Speech durch Social Bots, Strafrechtliche Zurechnung von Volksverhetzungen gem. § 130 Abs. 1 StGB' [2018] Multi Media und Recht, p. 58-59; E. Ferrera et al., *Ibid*., p. 96.

[10] See amongst many S. M. Benjamin, 'Algorithms and Speech' [2013] 161 U. Pa. L. Rev. 1145; T. Wu, 'Machine Speech' [2013] 161 U. Pa. L. Rev. 1495; on both M. Kaminski, 'From Google to Tolstoy Bot: Should the first Amendment Protect Speech Generated by Algorithms?' [2 September 2014] 128 J. Thinks We Like, https://cyber.jotwell.com/from-google-to-tolstoy-bot-should-the-first-amendment-protect-speech-generated-by-algorithms/; in German legal debate the topic has at least been touched upon, see German Federal Court [14 May 2013], Autocomplete, VI ZR 269/12, para. 22.

[11] J. Villasendor, *Ibid*.; L. Witt, 'Preventing the Rogue Bot Journalist: Protection from Non-Human Defamation' [2017] 15 Colorado Tech. L. J., p. 517.

[12] Except for N. Maréchal, 'When bots Tweet: Toward a Normative Framework for Bots on Social Networking Sites' [2016] 10 International Journal of Communication, p. 5022.

[13] Note: Part of the Author's knowledge on the underlying technologies of social bots is based on an online course on Natural Language Processing by the Stanford University School of Engineering which is available on YouTube (link to the playlist: https://www.youtube.com/watch?v=OQQ-W_63UgQ&list=PL3FW7Lu3i5Jsnh1rnUwq_TcylNr7EkRe6).

[14] See C. D. Manning, 'Computational Linguistics and Deep Learning' [2015] 41 Computational Linguistics, p. 701.

[15] I. Goodfellow et al., *Ibid*., p. 448.

[16] E. Ferrera et al., *Ibid*., p. 96; see also J. Reichwald and D. Pfisterer, 'Autonomie und Intelligenz im Internet der Dinge, Möglichkeiten und Grenzen autonomer Handlungen', [2016] Computer und Recht, p. 208-209.

of words and their co-occurrence in the context of other words[17]. Models that are even more primitive but however still in use today deploy simple scripts, which are only composed of outputs to specific (anticipated) user input and which thereby are deterministic[18].

Neural Networks, which are also the basis for recent ground-breaking developments in different fields of artificial intelligence applications such as automated driving, face recognition and legal-tech, can be applied to previous Natural Language Processing models to achieve much higher performances in the mimicking of human speech[19]. Neural Networks are computational models inspired by the biological brain, which utilise learning (or optimisation) algorithms such as backpropagation[20]. Without the need of further listing technical terms, a few facts and concepts are worth noting on natural language models and especially Neural Language Models in the context of a legal analysis of social bots:

First: the possibilities of combining or concatenating different models and architectures of Natural Language Processing for different tasks and domains are numerous[21]. There is not only one common way of programming. Second: For machine learning, the way the models operate—and ultimately the machines communicate—depends on the specific composition of the training data that the algorithms use for optimisation. One vivid example of this is the chat bot "Tay" which was launched by Microsoft as an experiment in learning through interaction with different users. It was shut down after less than 24 hours because some Twitter users taught it to post racist and inflammatory political statements[22]. Third: Neural Networks and Deep Learning algorithms are constructed in a way that the models themselves "decide" on what has to be adjusted to maximise performance under the given training dataset[23]. In some sense, many of the more advanced Natural Language Processing algorithms operate as black-boxes even from the viewpoint of their programmers[24], because tracing back which "neuron" fired in which instance is almost impossible.

1.2. Different Implementations, Different Purposes, Different Definitions

Social bots can be implemented in different ways on different platforms. One simple way is the implementation of a (purely) reactive bot via the Twitter Stream Application Programming Interface (API). The bot listens to the ongoing Twitter activity and reacts to specific posts or topics[25]. One simple way of reacting then is simply to retweet certain tweets that contain specific keywords (e.g. "refugees")[26]. More developed bots produce content autonomously based on artificial intelligence, leave a trace of human like metadata and create a network of friends to spread information[27]. Currently, the more simple bots are dominating social media sites[28]. The standard approach is called hybridisation, where a human designer and a simple social bot work together in a way in which tedious tasks were automated and complicated tasks such as the creation of content is left to a human user[29].

Depending on the specific application of a bot, different terms and definition are used. There is, for example, a distinction made between the term chat bot and social bot, where social bot is defined as a

---

[17] I. Goodfellow et al., *Ibid*., pp. 448-451.

[18] 'Brands and Bots – what you need to know' [18 April 2016] Fourth Source, http://www.fourthsource.com/branding/brands-bots-need-know-20801; see also L. Reichwald and D. Pfisterer, *Ibid*., p. 210.

[19] I. Goodfellow et al., *Ibid*, p. 449.

[20] *Ibid*., pp. 13-14, 197-217.

[21] *Ibid*., pp. 449-460.

[22] E. Hunt, 'Tay, Microsoft's AI chatbot, gets a crash course in racism from Twitter' [24 March 2016] The Guardian, https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter?CMP=twt_a-technology_b-gdntech.

[23] M. Hildebrandt, 'Smart Technologies and the End(s) of Law' (Cheltenham: Edward Elgar Publishing 2016), p. 24-26.

[24] W. Hoffmann-Riem, 'Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht' [2017] 142 Archiv des öffentlichen Rechts, p. 1, 29; see M. Hildebrandt, 'Learning as a Machine: Crossovers between Humans and Machines' [2017] 4 Journal of Learning Analytics, pp. 6, 10-15.

[25] C. Grimme *et al*., *Ibid*., p. 282-283; J. Villasendor, *Ibid*., p. 640.

[26] J. Villasendor, *Ibid*., p. 640.

[27] C. Grimme *et al., Ibid*., p. 283.

[28] 'Social Bots, Thesenpapier zum öffentlichen Fachgespräch Social Bots – Diskussion und Validierung von Zwischenergebnissen am 26. Januar 2017 beim Deutschen Bundestag' [January 2017] Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB), p. 4.

[29] C. Grimme *et al., Ibid*., p. 286.

specific type of chat bot which is used on a social media site[30]. Another class of bots are being described by the term "political bots" which refers to bots that are designed by politically motivated groups to communicate their opinions and mind sets on political topics[31]. In legal scholarly literature some authors suggest that the term social bot should be restricted to bots that are used to manipulate public opinion and disruption of communication[32]. This restriction to malicious or manipulative intent seems to be problematic and is at least not much of use. Set in a different context, "manipulation" can sometimes be rephrased as dissemination of an important topic. Think of a case in which human rights law activists and opponents of a regime are using social bots in order to drag public attention towards cases of human rights abuse and political persecution. The "deceiving" of the public about the initial relevance of a topic by social bots might also mean that bots prevented the stifling of a relevant message[33].

The common denominator for most cases and implementations of chat bots is the dissemination of a message or at least an idea, which can sometimes be certain and in some cases arbitrary from implementers viewpoint—this depends as shown on the degree of machine autonomy—through social media sites or the web in general. Bots enable a more permanent flow of information or ideas in the internet by ensuring that a topic stays relevant over a longer period of time. The intentions of the implementer or programmer might differ. The purposes of the implementation could range from commercial to political reasons. There is at least for the purpose of dealing with Human Rights Law questions, not much use to prima facie limitation of the term with respect to its actual common meaning.

2. Protection of Social Bots under Human Rights Law Regimes?

The question of whether machine speech is protected by Human Rights Law can be interpreted in two ways. One interpretation is to reason about the personhood of machines and the possibility of machines being the subject of protection. Some scholars and even the European Union[34] have already sparked this debate[35]. It would go far beyond the scope of this analysis to answer these sort of questions—predominantly it is propounded that machines should not have rights comparable to a human being[36]. Here the second interpretation will be addressed, namely the question after the protection of the people ("steersmen") behind the machines (the implementers or programmers).

2.1. Scope of Protection

Art. 10 para. 1 ECHR guarantees freedom of expression to "everyone", which means that it applies to both natural and legal persons that might be using the bot (legal persons might be newspapers or other media outlet that are using robot journalist, see above). It protects expression regardless of the form (it contains the freedom which covers the press as printed newspapers, magazines or electronic mass media[37]) and it applies to the means of dissemination and not just the content, "since any restriction

[30] 'Social Bots, TA-Vorstudie' [April 2017] Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB), p. 11; see Y. Boshmaf, I. Muslukhov, K. Beznosov et al., 'The Socialbot Network. When bots socialize for fame and money' [2011] Proceedings of the 27th Annual Computer Security Applications Conference, p. 93.

[31] C. Grimme *et al., Ibid*., p. 281.

[32] S. C. Woolley, 'Automating power: Social bot interference in global politics' [4 April 2016] 4 First Monday, http://firstmonday.org/article/view/6161/5300; S. Hegelich, 'Invasion der Meinungsroboter' [September 2016] Analysen & Argumente: Konrad Adenauer Stiftung, pp.1-9.

[33] E. Velázquez, M. Yazdani and P. Suárez-Serrato, 'Socialbots supporting human rights' [31 October 2017], https://arxiv.org/abs/1710.11346 [cs.CY].

[34] See Opinion of the European Economic and Social Committee on 'Artificial intelligence' – The consequences of artificial intelligence on the digital single market, production, consumption, employment and society (own-initiative opinion) [2017] on 526th EESC Plenary Session of May and 1 June 2017, OJ 2017/C 288/1, para. 1.6, 1.12, 3.33; N. Nevejans, 'European Civil Law Rules in Robotics' [2016], study requested by the European Parliaments Committee on Legal Affairs and published by the Policy Department C: for Citizens' Rights and Legal Affairs, p. 14.

[35] See T. Wu, *Ibid*., p. 1500; J. Boyle, 'Endowed by their Creator? The Future of Constitutional Personhood' [9 March 2011] Brookings Institute Governance Studies: 'The Future of the Constitution', https://www.brookings.edu/research/endowed-by-their-creator-the-future-of-constitutional-personhood/; L. B. Solum, 'Legal Personhood for Artificial Intelligences' [1992] 70 North Carolina Law Review, p. 1231.

[36] See for the European Union supra note 34.

[37] C. Grabenwarter, 'European Convention on Human Rights – Commentary' (Munich: C. H. Beck 2014), Art. 10 para. 2.

imposed on the latter necessarily interferes with the right to receive and impart information"[38,39]. Regarding the internet, the ECtHR has noted that it has become "one of the principal means by which individuals exercise their right to freedom of expression and information, providing as it does essential tools for participation on activities and discussions concerning political issues and issues of general interest"[40]. "In light of its accessibility and its capacity to store and communicate vast amounts of information, the internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information generally"[41].

In German legal literature regarding the scope of protection of Art. 5 of the Basic Law for the Republic of Germany, it has been proposed that the use of a social bot can be regarded as a decision on the means of dissemination, which is protected[42]. In a sense, a social bot could be regarded as a sort of messenger service or a tool, which is designed to send a message in the future[43]. However, one problem might lie in the fact that the message posted by the bot is from the viewpoint of the "steersmen" anticipated (in the case of reposting as well as in the case of generating content by the machine). It could be asked whether the programming of an algorithm with a certain bias or tendency constitutes an expression at all[44]. Another problem is the fact that the actual speaker hides anonymously behind the machine and is deceiving the public about the fact that he has written the message[45].

In general, this idea could be applied regarding Art. 10 para. 1 ECHR as well. As long as the bot can be regarded as a mere messenger or a sort of a typewriter its use would be protected as a modality of dissemination within the internet, which itself is a dissemination tool. However, as shown above "not all bots are created equal"[46]. Because of the various ways to manufacture a social bot, it is not possible to make a prima facie distinction of the different degrees of relation between the bot and its implementer or programmer. A coarse scaling is the distinction between Deep Learning bots and simple bots (in hybrid) use, but a Deep Learning bot is not necessarily fully autonomous and unconnected to the user behind it. Protection might depend e.g. on the specific training corpus for the bot and whether the training data had some bias to it. Whether the tendency or bias to make certain statements suffices to be regarded as protected expression, is yet questionable. Here, the protection would have to be evaluated on a case-to-case basis, which would require factual knowledge about the way the bot is programmed, which again would require expertise by computer engineers.

In some cases, when the bot is programmed in a way that it acts "neutral" and fully autonomous to specific topics or opinions , the use of a social bot may go without any expression by the "steersmen" because no message was ever intended to be made (not concrete, nor abstractly, as a tendency of the machine towards certain content). What would be left is the mere manufacturing of a bot, which might be protected as a form of property or by the freedom to a private life but not as an expression. What counts is the intention of the creator or implementer of the machine to express something "through" the bot. Even though highly developed algorithms might still be regarded as social constructs[47], the messages generated by them might not be regarded as protected expression. What is difficult however is to find out about the intentions of the "steersman" behind a certain bot when the "steersman" stays hidden and the algorithm remains opaque and too complex to grasp.

Regarding the problem of anonymity on the internet, the ECtHR has laid down some important guidelines in its Judgment of the case Delfi AS. v. Estonia[48]. In brief, the Court—rightly—argued that the

[38] ECtHR, Ahmet Yildirim v. Turkey, application no. 3111/10 (Dec. 18, 2012; final Mar. 18, 2013), para. 50.
[39] W. Schabas, 'The European Convention on Human Rights, A Commentary' (Oxford: Oxford University Press 2015), Art. 10, p. 456.
[40] ECtHR, Ahmet Yildirim v. Turkey, application no. 3111/10 (Dec. 18, 2012), para. 54.
[41] ECtHR, Times Newspapers Ltd. v. the United Kingdom (Nos. 1 and 2), applications nos. 3002/03 and 23676/03 (Mar. 10, 2009; final June 10, 2009), para. 27.
[42] J. Milkner, 'Social Bots im Meinungskampf, Wie Maschinen die öffentliche Meinung beeinflussen und was wir dagegen unternehmen können' [2017] Zeitschrift für Urheber- und Medienrecht, pp. 216-217.
[43] A. Steinbach, 'Social Bots im Wahlkampf' [2017] Zeitschrift für Rechtspolitik, pp. 101-102.
[44] J. Milkner, *Ibid*., p. 217.
[45] A. Steinbach, *Ibid*., p. 102; J. Milkner, *Ibid*., p. 218.
[46] S. De Paoli, 'Not All the Bots Are Created Equal: The Ordering Turing Test for the Labeling of Bots in MMORPGs' [2017] 3 Social Media + Society, p. 1.
[47] W. Hoffmann-Riem, *Ibid*., p. 29.
[48] ECtHR, application no. 64569/09 (June 16, 2015).

need for anonymity in the internet should be acknowledged. It found that "[a]nonymity has long been a means of avoiding reprisals or unwanted attention. As such, it is capable of promoting the free flow of ideas and information in an important manner, including, notably, on the Internet. At the same time, the Court does not lose sight of the ease, scope and speed of the dissemination of information on the Internet, and the persistence of information once disclosed, which may considerably aggravate the effects of unlawful speech on the Internet compared to traditional media"[49]. Further, the Court noted that "anonymity on the Internet, although an important value, must be balanced against other rights and interests"[50]. Judge Zupančič on the other hand argued in his dissenting opinion that "it is completely unacceptable that an Internet portal or any other kind of mass media should be permitted to publish any kind of anonymous comments. We seem to have forgotten that 'letters to the editor', not so long ago, were double-checked as to the identity of the author before they were ever deemed publishable"[51].

With the acknowledgement of anonymity, it is when applied to the use of social bots clear that the fact of "hiding" behind a bot does not hinder the general protection of the original communicator. Thereby the deception-element about the fact that not a person has physically typed in the message is only a side effect of the anonymity that the communicator (as long as there is a relevant expression, see above) has chosen. The reference to the "letters to the editor" and the critique of Judge Zupančič that goes with it lacks differentiation and does not consider the needs of communication in the realm of the internet.

However, the anonymity, the degree of relation between bot and original communicator, and the dangers of unlawful speech play a role for the justification of the regulation of social bots by the Member States.

For the protection of chat bots within the scope of Art. 19 para. 2 ICCPR, analogous arguments can be made. Just as within the scope of Art. 10 ECHR all the forms of communication including internet-communication are protected[52].

2.2. Permissible Restrictions and Regulatory Options

The most popular regulation options for the use of social bots that are being discussed range from the complete ban on the use of social bots, through labelling and the requirement of algorithm-transparency to a system of ensuring "social compatibility"[53].

In search for appropriate measures, some aspects should be considered. As noted, one fact to be recognised is that many of the Natural Language Processing algorithms especially the Neural Language Models are manufactured in some sense as black boxes[54]. Regarding the calls for algorithm-transparency it becomes clear that such a requirement would run up to its limits quickly. One might think about making requirements for the transparency of training data in order to detect whether the machine is programmed to have a certain tendency. Even then, it should be contemplated that most of the training data is based on large datasets containing billions of words and sentences, so that unfiltered disclosure of training data would not help improve the situation.

Considering the justification of regulation of social bots in a generalised manner, regulation would aim at the abstract dangers of unlawful speech or hate speech and the dangers of an aggravation of the effects of unlawful speech that are related to the use of social bots as means of dissemination. Thereby the regulation of social bots could be justified, if it is prescribed by law, as necessary in a democratic society in the interest of the protection of reputation or rights of others. In overview, the labelling of chat bots seems to be a good choice, because it would not interfere with the desired dissemination of a message as well as with the interest to remain anonymous on the internet. Because of the anonymity of

[49] *Ibid*., para. 147.
[50] *Ibid*., para. 149.
[51] *Ibid*., Concurring Opinion of Judge Zupančič, pp. 65, 66-67.
[52] M. Nowak, 'U.N. Covenant on Civil and Political Rights, CCPR Commentary' (Kehl: N. P. Engel 2nd revised ed.2005), Art. 19 para. 16; Human Rights Committee, General comment No. 34 on Article 19 (Freedoms of opinion and expression) of the International Covenant on Civil and Political Rights, CCPR/C/GC/34 (12 September 2011), para. 12.
[53] 'Social Bots, TA-Vorstudie' [April 2017] Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB), pp. 50, 63; A. Steinbach, *Ibid*., p. 103.
[54] See supra note 24.

the original communicators in most of the cases, regulation would have to be directed at the intermediaries of communication, especially to the social media platforms. A generalised ban on social bots on the other hand would overshoot its ends. As shown above, while many think of social bots as manipulative agents and a threat to democratic societies, they might also help supporting democratic ideas and human rights[55].

In a case-to-case analysis, the legal assessment of a specific measure would of course further depend on the content and context of the message that is produced by the bot. To name a few examples in the case of robot journalism by bots that are occupied by the press, its special role must be taken into account[56]. In the case of hate speech, the produced message might either not be protected at all (as it would be within the scope of Art. 17 ECHR) or it would lead to a greater margin of appreciation for the Member State to interfere with the rights of the original communicator behind the messages that are produced by the bot[57].

In its general comments on Art. 19 ICCPR the Human Rights Committee shows that it tends to a dissemination-friendly regulation of the internet which is aware of current needs and communications practises:

"Any restrictions on the operation of websites, blogs or any other Internet-based, electronic or other such information dissemination system, including systems to support such communication, such as Internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3. It is also inconsistent with paragraph 3 to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government[58]". And further: "States parties should take account of the extent to which developments in information and communication technologies, such as Internet and mobile based electronic information dissemination systems, have substantially changed communication practices around the world. There is now a global network for exchanging ideas and opinions that does not necessarily rely on the traditional mass media intermediaries. States parties should take all necessary steps to foster the independence of these new media and to ensure access of individuals thereto"[59].

In conclusion, generalised regulations on social bots should consider the need for the dissemination of messages with the help of social bots as well as for anonymity on the internet. A generalised ban on the use of social bots or generalised requirements for the disclosure of the identities of the persons who are using bots go too far. State regulations should be directed towards information intermediaries as in most cases the original communicators behind the bots would remain unknown whereas the intermediaries are identifiable and have the capability to detect and filter the use of social bots[60]. And in fact, in reply to the critique, many platforms have already adapted their terms of use and have set new community rules for the use of social bots[61]. However, it is questionable whether this is sufficient.

The approach to (further) oblige social media intermediaries is a reflection of the fact that private actors such as information intermediaries are ever crowding in to new public functions (or into new tasks of public interest) and seem to be in fact most capable of fulfilling these new tasks. These developments not only stand for a transformation of the ways of communication, but also of the public sphere in general.

[55] E. Velázquez et al., *Ibid*., p. 33.
[56] C. Grabenwarter, *Ibid*., Art. 10 para. 11; 46.
[57] N. Wenzel, 'Opinion and Expression, Freedom of, International Protection' [2014] Max Planck Encyclopedia of Public International Law (MPEPIL Online), para. 25.
[58] Human Rights Committee, General comment No. 34 on Article 19 (Freedoms of opinion and expression) of the International Covenant on Civil and Political Rights, CCPR/C/GC/34 (12 September 2011), para 43.
[59] *Ibid*., para. 15.
[60] J. M. Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' [2018] 51 U.C.D.L. Rev., pp. 1149, 1175.
[61] N. Maréchal, *Ibid*., p. 5025-5027.

3. Transformation of Communication and the Public Sphere

3.1. Changes to Communication and "Transformation of the Public Sphere"

Discussions about the Information Society and its implications for the law reach back to the early days of the internet 20 years ago, which was not comparable to what it is today. This might be seen as a reason to call out a new phase of development—the "Algorithmic Society"[62]. While in public discourse about future and development there always is a tendency to call out new "eras", it is plainly evident that changes to practical conditions of speech have occurred as well as to entities and actors that control, limit and censor speech[63]. With the use of big data and algorithms by private entities, power shifts into new structures. As behind the algorithm is always a group of persons that are controlling the technology, these new technologies help to mediate power between humans and other humans[64].

The new ways of communication through social media can be characterised with a few key features. Social media allows for the distribution of user-generated content, which means that users become producers of media content rather than mere consumers. This leads to a situation of many-to-many communication which differs from the classic role of media[65]. This phenomenon has already been recognised by the ECtHR in Cengiz and others v. Turkey as "citizen journalism" [66]. Unlike with press lead journalism, in the current state of "citizen journalism", it is possible for everyone to interfere with the authenticity of a message or to produce and distribute fabricated information (partly with the help of bots), while no institution is responsible for the quality of the news or messages that is being produced. In all this turmoil, social media intermediaries and other platforms act as mere newsstands, while in fact through their filtering capabilities and instruments of private governance[67], that crosscut national boundaries[68], they should be regarded as gatekeepers[69].

With the power of intermediaries to set community rules and to filter and sort out speech, speech governance shifts from a bipolar to a triangular (or in fact multipolar and complicated) relationship of state actors (nation states, international organisations such as the EU), end users and infrastructure providers (social media and other platforms)[70]. States are no longer the only guarantors of public order[71]. Social media sites and other information intermediaries form a new public sphere in which they act as rule setters for communication (not to call them sovereigns)[72]. They become the maintainers of a new infrastructure of free expression[73], owners of public fora[74], in the light of which the liberal premise of public private dichotomy seems no longer to be maintainable[75]. As a flipside to this, the ways for the state to regulate

[62] J. M. Balkin, *Ibid*., p. 1151.
[63] *Ibid*., p. 1153.
[64] *Ibid*., pp. 1157-1158.
[65] J. A. Tucker, Y. Theocharis and M. E. Roberts, 'From Liberation to Turmoil: Social Media and Democracy' [2017] 28 Journal of Democracy, pp. 46, 48-49.
[66] ECtHR, Cengiz and others v. Turkey, applications nos. 48226/10 and 14027/11 (1 December 2015; final 1 March 2016), para. 52.
[67] See J. M. Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' [2018] 51 U.C.D.L. Rev., p. 1182.
[68] *Ibid*.
[69] J. Drexl, 'Bedrohung der Meinungsvielfalt durch Algorithmen, Wie weit reichen die Mittel der Medienregulierung?' [2017] Zeitschrift für Urheber- und Medienrecht, p. 529, 536; J. M. Balkin, 'Old-School/New-School Speech Regulation' [2014] 127 Harv. L. Rev., pp. 2296, 2304.
[70] J. M. Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' [2018] 51 U.C.D.L. Rev., p. 1186.
[71] G. Buchholz, 'Demokratie und Teilhabe in der digitalen Zeit' [2017] Die öffentliche Verwaltung, pp. 1009-1010.
[72] N. Maréchal, *Ibid*., p. 5024.
[73] J. M. Balkin, 'Old-School/New-School Speech Regulation' [2014] 127 Harv. L. Rev., p. 2300.
[74] In the U.S. debate, it has been propounded that the first amendment public forum doctrine should be applied on the information intermediaries such as Google, Twitter and Facebook. See: F. M. Sparr, 'Expanding the Public Forum Doctrine in Cyberspace: Some Lessons from Jersey' [2006] 6 Communication Law Review, p. 26; D. C. Nunziato, 'The Death of the Public Forum in Cyberspace' [2005] 20 BTLJ, p. 1115; J. M. Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' [2018] 51 U.C.D.L. Rev., p. 1194.
[75] S. M. Feldman, 'Postmodern Free Expression: A Philosophical Rationale for the Digital Age' [2017] 100 MULR, pp. 1123, 1155.

speech shift towards more cooperative approaches and towards models of Public-Private Governance[76]. In the words of Jürgen Habermas, the structures of the public sphere transforms[77].

3.2. The Specific Changes to Modern Communication Caused by Social Bots

In the analysis of changes to communication that go specifically with the use of social bots it can be established that many of the existing internet- and social media-related changes (and dangers, when regarded abstractly) are further amplified. The effects of echo-chambers, filter-bubbles and confirmation biases[78] are potentiated with social bots pushing specific topics more than others. They induce what can be called as "spirals of silence" ("Schweigespirale"[79]), because they create the impression that most of the public is clearly tending towards a specific opinion whereas many people have the opposite opinion or a much more nuanced view on a given topic. This in turn discourages many from stating their opinion in the fear of social exclusion[80]. By the potentials for manipulation they pose a threat to the autonomy of communication[81] and cause disturbances to the "marketplace of ideas"[82]. However, as mentioned, in certain cases the dangers of social bots could also be rephrased as benefits. In addition, social bots make it increasingly difficult to find a distinction between publisher and typewriter, between speech product and communication tool[83]. As the convergence of different types of media[84], social bots lead to a convergence of communicator and communication-tool.

4. Transformation of Human Rights Law and International Law—Towards a Functional Approach

To tackle the challenges that are related to the changes of communication, responds from the law are required. Some might ask for a law reform. A change to the text of the provisions in question of course would not solve the problems. Transformation with respect to Human Rights norms can only mean that the reading of the provisions might be adjusted to the changing situation. The question to be answered is whether the rationales on which freedoms of communication traditionally relied on shifted because the social setting have changed[85]. The appropriate degree of adjustment on the reading of free expression provisions depends on their initial rationale. This is part of what constitutes their normativity[86]. To be more specific, the adaptations to be made to the freedoms of communication call for a stronger positive (or objective) nature of the obligation in question[87] and towards a stronger horizontal effect[88]. And many recent academic debates and judgements (domestically and internationally) tend to point in this direction.

One significant example of a development towards more positive obligations is (in relations between private entities), again, the Judgement in the Case of Delfi AS. v. Estonia, in which the Court found that it "concerns the 'duties and responsibilities' of Internet news portals, under Article 10 § 2 of the Convention, when they provide for economic purposes a platform for user-generated comments on

---

[76] J. M. Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' [2018] 51 U.C.D.L. Rev., pp. 1173, 1193-1198.

[77] J. Habermas, 'Structural Transformation of the Public Sphere' (Cambridge: MIT Press 1991); see also N. Maréchal, *Ibid*., p. 5024; G. Buchholtz, *Ibid*., p. 1010.

[78] J. Drexl, *Ibid*., p. 529-530, 534; see also E. Pariser, 'The Filter Bubble: What the Internet is Hiding from You (London: Penguin 2011).

[79] 'Social Bots, TA-Vorstudie' [April 2017] Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB), p. 59; E. Neoelle-Neumann, 'Die Schweigespirale: Öffentliche Meinung – unsere soziale Haut' (Munich: Langen Müller 6. ed., 2001).

[80] W. Hoffmann-Riem, *Ibid*., p. 15.

[81] S. M. Benjamin, *Ibid*., p. 1454.

[82] See ECtHR, Mouvement Raëlien Suisse v. Switzerland, application no. 16354/06 (July 13, 2012), Dissenting Opinion of Judge Pinto de Albuquerque p. 46, 50 note 15; see further J. Gordon, 'John Stuart Mill and the Marketplace of Ideas' [1997] 23 Social Theory and Practice, p. 235.

[83] See T. Wu, *Ibid*., pp. 1504-1505.

[84] T. Flew, 'Media convergence' [17 August 2017] Encyclopædia Britannica, https://www.britannica.com/topic/media-convergence.

[85] S. M. Feldman, *Ibid*., p. 1125.

[86] See K. Hesse, 'Die normative Kraft der Verfassung, Freiburger Antrittsvorlesung' (Tübingen: Mohr Siebeck 1959). This should not be understood as a proposal to apply German constitutional theory to International Human Rights Law, the constitutionality of International Law in general is, as known, heatedly debated (see below).

[87] In general, W. Schabas, *Ibid*., Art. 10 pp. 453-454; C. Grabenwarter, *Ibid*., Art. 10 para. 63–64; 66.

[88] See W. Hoffmann-Riem, *Ibid*., p. 40.

previously published content and some users—whether identified or anonymous—engage in clearly unlawful speech, which infringes the personality rights of others and amounts to hate speech and incitement to violence against them"[89]. Nevertheless "because of the particular nature of the Internet, the 'duties and responsibilities' that are to be conferred on an Internet news portal for the purposes of Article 10 may differ to some degree from those of a traditional publisher, as regards third-party content"[90]. Reaching further, it was argued by Judge Pinto de Albuquerque in a previously dissenting opinion that: "If streets and parks of a city are the historical quintessential public fora, the Internet is today's global marketplace of ideas"[91]. The general hope for the future seems to be that what happened to newspapers in the early twentieth century, in which not only the norms but also the self-perception of the press changed, reoccurs in the case of large international owners of communication infrastructure and social media[92].

These tendencies could be summed up under aspiration for a functional rather than formalist account of obligations related to free expression, which enables to include other entities such as private actors[93], when those carry public functions[94]. The requirement for labelling social bots for example then becomes a question of quality of the provided infrastructure which falls under the responsibilities of the social media service.

Going even further, the need for regulation of multinational intermediaries of information with the help of objective principles, other paradigm shifts of International Law that are on the merge, could have a chance to solidify. This includes the constitutionalisation of International Law[95] and the Publicness of International Law whereas public in this context means the claim for law to stand in the name for the whole society[96].

Conclusions

With the ever faster evolving change of society, developments of technology and the changing nature of communication some voices require that the law is capable of grasping the complexity of today's society. But ever complex laws are not a solution to the problem. Especially for Human Rights Law, it is necessary to contain its abstract and general nature.

The transformations of law generally have (and need to have) a longer scale than the changes to communication habits and media-phenomena in order to be normative. It is hard to make any predictions about the relevance of social media, chat bots, search engines or any kind of internet-related development in the future.

Law-making, thought as finding general principles within the law and in the light of new developments requires as a necessary condition some sense of what the characteristics of the current development are. For internet phenomena like social media services, chat bots and the like this requires understanding on the one hand what the defaults of communication are[97] and on the other hand, what it is that is generally changing in the ways of our communication. This requires some knowledge of technical and factual features of recent developments to a reasonable extent at least. More than ever it becomes

[89] ECtHR, Delfi AS. v. Estonia, application no. 64569/09 (June 16, 2015), para. 115.
[90] *Ibid*., para. 113.
[91] ECtHR, Mouvement Raëlien Suisse v. Switzerland, application no. 16354/06 (July 13, 2012), Dissenting Opinion of Judge Pinto de Albuquerque pp. 46, 54.
[92] J. M. Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' [2018] 51 U.C.D.L. Rev., p. 1209.
[93] See also N. Maréchal, supra note 12, 5024 pointing towards the United Nations Guiding Principles on Business and Human Rights, HR/PUB/11/04, 2011 (Ruggie Principles).
[94] Regarding the Right to Information see A. Peters, 'Towards Transparency as a Global Norm' in A. Bianchi, A. Peters (ed.), 'Transparency in International Law' (Cambridge: Cambridge University Press 2013) p. 534, 593; see Human Rights Committee, General comment No. 34 on Article 19 (Freedoms of opinion and expression) of the International Covenant on Civil and Political Rights, CCPR/C/GC/34 (12 September 2011), para. 18.
[95] W. Hoffmann-Riem, *Ibid*., p. 41; see also I. Pernice, 'Global Constitutionalism and the Internet: Taking People Seriously', in: R. Hofmann, J Kadelbach (ed.), 'Law Beyond the State' (Frankfurt: Campus 2016) p. 151.
[96] See A. Peters, *Ibid*., pp. 600-604 regarding transparency.
[97] M. Hildebrandt, *Ibid*., p. 226.

for the legal scholar important to think and work interdisciplinary (analogues to the convergences of media and public mentioned above one might also speak of the convergence of scientific disciplines).

The recent developments in society and in the necessities of legal thinking that follow from it may empower emerging paradigm shifts in many domestic laws and in International Law to solidify. Many of the recent developments point towards a more functional account, towards more objective and positive rights and obligations (notwithstanding the remaining importance of defence against the state) and towards more "duties and responsibilities" for some actors that undertake tasks of general public interest.

Applied on the problem of the emergence of social bots and the threats to free expression that are linked to it, it becomes clear that only the owners of the new public fora, those who take up a function of general public interest should be the addressees of "duties and responsibilities" to guarantee a qualitative communication infrastructure.

Bibliography

1. J. M. Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' [2018] 51 U.C.D.L. Rev. 1149.
2. J. M. Balkin, 'Old-School/New-School Speech Regulation' [2014] 127 Harv. L. Rev. 2296.
3. S. M. Benjamin, 'Algorithms and Speech' [2013] 161 U. Pa. L. Rev. 1145.
4. A. Bessi, E. Ferrera, 'Social bots distort the 2016 U.S. Presidential election' online discussion [7 November 2016] 21 First Monday, http://firstmonday.org/ojs/index.php/fm/article/view/7090/5653.
5. J. Boyle, 'Endowed by their Creator? The Future of Constitutional Personhood' [9 March 2011] Brookings Institute Governance Studies: 'The Future of the Constitution', https://www.brookings.edu/research/endowed-by-their-creator-the-future-of-constitutional-personhood/.
6. 'Brands and Bots – what you need to know' [18 April 2016] Fourth Source, http://www.fourthsource.com/branding/brands-bots-need-know-20801.
7. G. Buchholz, 'Demokratie und Teilhabe in der digitalen Zeit' [2017] Die öffentliche Verwaltung.
8. S. De Paoli, 'Not All the Bots Are Created Equal: The Ordering Turing Test for the Labeling of Bots in MMORPGs' [2017] 3 Social Media + Society.
9. J. Drexl, 'Bedrohung der Meinungsvielfalt durch Algorithmen, Wie weit reichen die Mittel der Medienregulierung?' [2017] Zeitschrift für Urheber- und Medienrecht, p. 529, 536; J. M. Balkin, 'Old-School/New-School Speech Regulation' [2014] 127 Harv. L. Rev.
10. ECtHR, Ahmet Yildirim v. Turkey, application no. 3111/10 (Dec. 18, 2012; final Mar. 18, 2013).
11. ECtHR, application no. 64569/09 (June 16, 2015).
12. ECtHR, Cengiz and others v. Turkey, applications nos. 48226/10 and 14027/11 (1 December 2015; final 1 March 2016).
13. ECtHR, Delfi AS. v. Estonia, application no. 64569/09 (June 16, 2015).
14. ECtHR, Mouvement Raëlien Suisse v. Switzerland, application no. 16354/06 (July 13, 2012), Dissenting Opinion of Judge Pinto de Albuquerque.
15. ECtHR, Times Newspapers Ltd. v. the United Kingdom (Nos. 1 and 2), applications nos. 3002/03 and 23676/03 (Mar. 10, 2009; final June 10, 2009).
16. S. M. Feldman, 'Postmodern Free Expression: A Philosophical Rationale for the Digital Age' [2017] 100 MULR.
17. Finley, 'This News Writing Bot is Now Free For Everyone', Wired [20 October 2015], https://www.wired.com/2015/10/this-news-writing-bot-is-now-free-for-everyone/.
18. E. Ferrera, O. Varol, C. Davis et al., 'The Rise of Social Bots' [2016] 59 Communications of the ACM.
19. T. Flew, 'Media convergence' [17 August 2017] Encyclopædia Britannica, https://www.britannica.com/topic/media-convergence.
20. I. Goodfellow, Y. Bengio, A. Courville,'Deep Learning' (Cambridge, MA: MIT Press 2017)
21. J. Gordon, 'John Stuart Mill and the Marketplace of Ideas' [1997] 23 Social Theory and Practice.
22. C. Grabenwarter, 'European Convention on Human Rights – Commentary' (Munich: C. H. Beck 2014), Art. 10 para. 2.
23. C. Grimme, M. Preuss, L. Adam et al., 'Social Bots: Human Like by Means of Human Control?' [2017] 5 Big Data.

24. J. Habermas, 'Structural Transformation of the Public Sphere' (Cambridge: MIT Press 1991).
25. S. Hegelich, 'Invasion der Meinungsroboter' [September 2016] Analysen & Argumente: Konrad Adenauer Stiftung.
26. K. Hesse, 'Die normative Kraft der Verfassung, Freiburger Antrittsvorlesung' (Tübingen: Mohr Siebeck 1959).
27. M. Hildebrandt, 'Learning as a Machine: Crossovers between Humans and Machines' [2017] 4 Journal of Learning Analytics.
28. M. Hildebrandt, 'Smart Technologies and the End(s) of Law' (Cheltenham: Edward Elgar Publishing 2016).
29. W. Hoffmann-Riem, 'Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht' [2017] 142 Archiv des öffentlichen Rechts.
30. P. N. Howard and B. Kollanyi, 'Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum' [2016] Comprop Research Note 2016.1, https://arxiv.org/abs/1606.06356 [cs.SI].
31. Human Rights Committee, General comment No. 34 on Article 19 (Freedoms of opinion and expression) of the International Covenant on Civil and Political Rights, CCPR/C/GC/34 (12 September 2011).
32. E. Hunt, 'Tay, Microsoft's AI chatbot, gets a crash course in racism from Twitter' [24 March 2016] The Guardian, https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter?CMP=twt_a-technology_b-gdntech.
33. M. Kaminski, 'From Google to Tolstoy Bot: Should the first Amendment Protect Speech Generated by Algorithms?' [2 September 2014] 128 J.
34. C. D. Manning, 'Computational Linguistics and Deep Learning' [2015] 41 Computational Linguistics.
35. N. Maréchal, 'When bots Tweet: Toward a Normative Framework for Bots on Social Networking Sites' [2016] 10 International Journal of Communication.
36. R. Menn, 'Die Macht der Social Bots' [22 October 2016] Deutschlandfunk, http://www.deutschlandfunk.de/wahlkampf-die-macht-der-socialbots.1818.de.html?dram:article_id=369303.
37. J. Milkner, 'Social Bots im Meinungskampf, Wie Maschinen die öffentliche Meinung beeinflussen und was wir dagegen unternehmen können' [2017] Zeitschrift für Urheber- und Medienrecht.
38. E. Neoelle-Neumann, 'Die Schweigespirale: Öffentliche Meinung – unsere soziale Haut' (Munich: Langen Müller 6. ed., 2001).
39. M. Nowak, 'U.N. Covenant on Civil and Political Rights, CCPR Commentary' (Kehl: N. P. Engel 2nd revised ed.2005), Art. 19 para. 16; Human Rights Committee, General comment No. 34 on Article 19 (Freedoms of opinion and expression) of the International Covenant on Civil and Political Rights, CCPR/C/GC/34 (12 September 2011).
40. D. C. Nunziato, 'The Death of the Public Forum in Cyberspace' [2005] 20 BTLJ.
41. I. Pernice, 'Global Constitutionalism and the Internet: Taking People Seriously', in: R. Hofmann, J Kadelbach (ed.), 'Law Beyond the State' (Frankfurt: Campus 2016)
42. A. Peters, 'Towards Transparency as a Global Norm' in A. Bianchi, A. Peters (ed.), 'Transparency in International Law' (Cambridge: Cambridge University Press 2013).
43. J. Reichwald and D. Pfisterer, 'Autonomie und Intelligenz im Internet der Dinge, Möglichkeiten und Grenzen autonomer Handlungen', [2016] Computer und Recht.
44. 'Social Bots, TA-Vorstudie' [April 2017] Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB), p. 11; see Y. Boshmaf, I. Muslukhov, K. Beznosov et al., 'The Socialbot Network. When bots socialize for fame and money' [2011] Proceedings of the 27th Annual Computer Security Applications Conference.
45. 'Social Bots, Thesenpapier zum öffentlichen Fachgespräch Social Bots – Diskussion und Validierung von Zwischenergebnissen am 26. Januar 2017 beim Deutschen Bundestag' [January 2017] Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB).
46. L. B. Solum, 'Legal Personhood for Artificial Intelligences' [1992] 70 North Carolina Law Review.
47. F. M. Sparr, 'Expanding the Public Forum Doctrine in Cyberspace: Some Lessons from Jersey' [2006] 6 Communication Law Review.
48. A. Steinbach, 'Social Bots im Wahlkampf' [2017] Zeitschrift für Rechtspolitik.
49. The consequences of artificial intelligence on the digital single market, production, consumption, employment and society (own-initiative opinion) [2017] on 526th EESC Plenary Session of May

and 1 June 2017, OJ 2017/C 288/1, para. 1.6, 1.12, 3.33; N. Nevejans, 'European Civil Law Rules in Robotics' [2016], study requested by the European Parliaments Committee on Legal Affairs and published by the Policy Department C: for Citizens' Rights and Legal Affairs.

50. J. A. Tucker, Y. Theocharis and M. E. Roberts, 'From Liberation to Turmoil: Social Media and Democracy' [2017] 28 Journal of Democracy.
51. E. Velázquez, M. Yazdani and P. Suárez-Serrato, 'Socialbots supporting human rights' [31 October 2017], https://arxiv.org/abs/1710.11346 [cs.CY].
52. J. Villasendor, 'Technology and the Role of the Internet in Constitutionally Protected Expression' [2016] 39 Harvard JLPP.
53. V. Volkmann, 'Hate Speech durch Social Bots, Strafrechtliche Zurechnung von Volksverhetzungen gem. § 130 Abs. 1 StGB' [2018] Multi Media und Recht.
54. N. Wenzel, 'Opinion and Expression, Freedom of, International Protection' [2014] Max Planck Encyclopedia of Public International Law (MPEPIL Online).
55. L. Witt, 'Preventing the Rogue Bot Journalist: Protection from Non-Human Defamation' [2017] 15 Colorado Tech. L. J.
56. S. C. Woolley, 'Automating power: Social bot interference in global politics' [4 April 2016] 4 First Monday, http://firstmonday.org/article/view/6161/5300.
57. T. Wu, 'Machine Speech' [2013] 161 U. Pa. L. Rev. 1495.

SELLING AUTHORS' RIGHTS FOR A FRAUD: IS THAT POSSIBLE?

Defossez Delphine Aurélie Laurence[1]

Abstract

While most people are hunting for jobs, some people are hunted by jobs; young academics or professors are asked to become ghostwriters. The cyberspace facilitates this phenomenon; indeed, all over the Internet websites proposing to "help" students are proliferating. Notwithstanding the moral aspect of such practice, this practice raises some legal issues such as: Can someone sell his/ her authorship rights to achieve an illegal purpose?

The concept of "ghostwriting" shares some similarities with the concept of plagiarism, however, the reactions differ remarkably. While plagiarism is condemned as a capital offence for law students, ghostwriting has not really been tackled. Indeed, a student caught using the ideas or words without proper referencing may be suspended, see his degree withhold or even expelled.[2] Whereas rarely does a student loss his degree because of using a ghostwriting service. However, such offence is much more dangerous as students without much knowledge obtain diplomas and enter the job market to the detriment of other 'traditional' students. Money is a big factor, but the Internet is the biggest factor as it allowed such type of company to proliferate, attracting more and more clients.

The purpose of this article is not a judgmental one, instead, this article highlights a practical complication that arises from ghostwriting: with whom resides the authors' rights? The author believes that although the author's rights were sold, due to the fraudulent component of the situation, the rights are reverted to the original author.

Keywords: Ghostwriting- IP rights- fraudulent contracts- digital world.

Introduction

In these difficult times where people are hunting for jobs, some people are hunted by jobs; young academics or professors are asked to become ghostwriters. The cyberspace facilitates this phenomenon through readily accessible information concerning a certain person. This facility of information allows companies providing ghostwriting services to try hiring the person they believe best fit the job. All over the Internet websites proposing to "help" students with their coursework, essays, presentations, dissertations, and so on, are proliferating. Notwithstanding the moral aspect of such practice, this practice poses some legal issues, especially when service is for law school students, such as can someone sell his/ her authorship rights to achieve an illegal purpose?

The concept of "ghostwriting" shares some similarities with the concept of plagiarism, however, the reactions differ remarkably. The concept of "ghostwriting" was defined by Webster as "writ[ing] books, articles, etc. for another who professes to be the author"[3] while he defined plagiarism as "to take ideas, writings, etc. from another and pass them off as one's own."[4] Although the similarities in both definitions are notable, the reactions with regard to the two terms differ remarkably. While plagiarism is condemned and regarded as a capital offence for law students, ghostwriting has not really been tackled. Well-accepted examples of ghostwriting are found in politics where presidential speeches are generally not writing by the President himself. On the other side of the spectrum, supporters of plagiarism are hard to find. Indeed, a student caught using the ideas or words of someone else without proper reference to that person may be suspended, see his degree withhold or even expelled from law school.[5]

---

[1] *PhD in Law, University of Brasilia (UnB), Faculty of Law, with a dissertation on "The Liberalisation of the Aviation Market in Brasil". LL.B (Maastricht University), LL.M. (European University Institute); LL.M. (Swansea University)*

[2] Easley v. Univ. of Mich. Bd. of Regents, 906 F. 2d 1143, 1143-46 (6th Cir. 1990); In re Lamberis, 443 N.E.2d 549, pp. 552-53 (I11. 1982).

[3] 'New World College Dictionary' (Webster's New World 2002) Webster's 4th ed., p. 597.

[4] *Ibid*., p. 1100

[5] Easley v. Univ. of Mich. Bd. of Regents, 906 F. 2d 1143, 1143-46 (6th Cir. 1990); In re Lamberis, 443 N.E.2d 549, p. 552-53 (I11. 1982).

Plagiarism is such a capital offence that a student can be caught even for unintentional plagiarism, which can occur through paraphrasing moving away from the initial source but using similar wording as another source or for only a small portion of the work.[6] Some regards ghostwriting as pure and simple plagiarism because "it is a form of dishonesty, it is a form of cheating, and where students are found guilty of it, there will be serious academic repercussions."[7] However, the chances of being caught are much lower for unpublished works, even if the offence is the same. Indeed, ghostwriting works are often original works that pass any plagiarism detectors.

The line between plagiarism and ghostwriting is extremely thin. As Alexander Lindey defined plagiarism as "literary-or artistic or musical-theft. It is the false assumption of authorship-the wrongful act of taking the product of another's mind, and presenting it as one's own. Copying someone else's story or play or song intact or with inconsequential changes, and adding one's name to the result constitute a simple illustration of plagiarism."[8] The greatest difference between plagiarism and ghostwriting is that the ghostwriter is voluntarily writing for the other, while in plagiarism situation his work is taken by another.

Plagiarism is regarded as one of "the most egregious variety of dishonesty."[9] At the same time, the legal culture is paved with ghostwriting. Many junior lawyers allow their work to pass as the work of the senior lawyers and when the junior lawyer gains enough status, they will start publishing work written by others under his name. Moreover, it is not rare for judicial clerk ghostwriting for a judge. As an American judge once said: "there are a great many judges who would like nothing better than to do their own research and writing[…] The problem is that […] the caseload per federal judge has risen to the point where very few judges, however able and dedicated, can keep up with the flow without heavy reliance on law clerks, staff attorneys, and sometimes externs too."[10] Although these situations might be regarded as unethical, they are nothing compared to students who pay their degrees by hiring ghostwriters.

The blame is not as much on the ghostwriter than on the students demanding such services. As Josie Gurney-Read quoted "I don't have any qualms about my work. Some people sell state of the art vacuum cleaners and I sell excellent academic papers. If I do not offer it, someone else will."[11] Money is a big factor, but the Internet is the biggest factor as it allowed such type of company to proliferate and attract more and more clients.

This article analyses the legal practice of ghostwriting to determine whether someone can sell his authorship rights to commit fraud. The purpose of this article is not a judgmental one, instead, this article highlights a practical complication that arises from ghostwriting: with whom resides the authors' rights? First, the phenomenon of ghostwriting will be discussed with regard to the various forms it can take within the legal culture. Since the focus of this article is on ghostwriting for students, the role of the internet will be discussed. Indeed, the internet has undeniably helped this business to expand. Then the question of whether the original author can sell his or her authorship rights to commit fraud will be discussed; Can the original author reuse the work in one of his publication or are his rights transferred to the person who paid for the work? The author believes that although the author's rights were sold, due to the fraudulent component of the situation, the rights are reverted to the original author. Finally, the effect of such practice will be discussed wherein the moral question will be tackled.

1. Ghostwriting the phenomenon

Ghostwriting has existed for probably as long as authorial attribution and paves the legal culture. Many senior lawyers publish the work of junior lawyers under their names, and after several years, when the junior lawyers have acquired enough status to stop writing for others, they will start using the work of others. Articles in law review could be published under the name of one of the partners even if he was not

[6] J. S. Dursht, 'Judicial Plagiarism: It May Be Fair Use but Is It Ethical?', [1996] 18 CARDOZO L. REV. 1253, p.1253.

[7] J. Gurney-Read, '£1,700 for a dissertation, but what's the real cost of plagiarism?', http://www.telegraph.co.uk/education/educationnews/11532848/1700-for-a-dissertation-but-whats-the-real-cost-of-plagiarism.html, accessed 09 April 2018

[8] A. Lindey, 'Plagiarism and Originality' (New York: Harper. & Brothers 1952), p. 2.

[9] L. G. Lerman, 'Misattribution in Legal Scholarship: Plagiarism, Ghostwriting and Authorship' [2001] 42 S. Tex, Law Review pp. 467-468.

[10] R. A. Posner, 'The Federal Courts: Crisis and Reform' (Harvard University Press, 1985) p. 103.

[11] J. Gurney-Read, *Ibid*.

alone to write it with the other authors sometimes thanked for their assistance in a footnote.[12] The partner could argue that the writer just put down on paper his ideas and that therefore the name of the author is not relevant. Another argument could be that the writer got paid for his work and therefore whatever he produces is the property of the firm.

Looking at the judicial system and the problem of the rising caseload level, it is not rare for judges to delegate the drafting work to the judicial clerks.[13] Some judges edit their clerks' work while others not. Regardless of whether the judge edits or not the work, in all cases the opinion will be published under the judge's name with almost never an acknowledgement.[14]

In academia, it is not uncommon for supervisors to publish articles with their supervisees or to include such work in their own work.[15] The recourse to the use of supervisees' work by supervisors might be due to the time and economic pressure that professors are facing. Indeed, some universities pressure their professors, who want to keep their positions, to publish a specific amount of articles a year. Research assistants are rarely named as co-author, and various justifications can be found; the work of the research assistant is a work for hire as the assistant is getting paid or the ideas are from the professor, the research assistant just did the background researches and so on. However, such situation, although unethical, is accepted.

The phenomenon starts to have serious repercussions when the ghostwriting work is used by students in view of obtaining a degree. The proliferation of ghostwriters can be explained by economic circumstances; Indeed, today's students often work (part or full time) and are therefore time-poor. Some other lack time and ability to do it themselves. Especially in the UK where the level is rising while the English's level of some students is dropping.[16] Stratos Malamatinas, the founder of Oxbridge essays, stated "75 per cent of our customers are foreign students who, although talented, can't express themselves as well in English as in their own language. British universities are happy to take their money, without checking their English."[17] Such statement demonstrates that the disclaimer used by some companies, namely that students are supposed not to pass the work as their own but to rework on the essay they ordered, is just absurd. The companies try just to pass the responsibility to the students. For instance, Thomas Nemet explained that "customers cannot order dissertations from us per se, because that would be illegal. However, it is possible to place an order for a 200-page paper on a particular topic, with the proviso that the client signs an agreement to the effect that this paper will not be handed in the client's own name. Should a client ignore this prohibition, then we cannot be held responsible."[18] This argumentation is very weak because if the person was to write his essay himself, then such services will have no interest. Facing the reality, no one will be willing to pay £300 or 660 to then paraphrase everything, especially since the work is normally an original one and therefore will pass the Turnitin test without problems. Indeed, most "essay-writers are graduates themselves, with postgraduates and PhD holders in great demand. And yes, some are undoubtedly University lecturers looking to make a few quid on the side."[19] This is another argument that attracts students; that their works will supposedly be of higher quality than any work they could produce.

The problem is expanding as exemplified by ACAD WRITE which started in 2005 with 500 euro and which counted a pool of over 300 ghostwriters in various countries in 2015. The number of requests for such services continuously increases. For instance, ACAD WRITE had a turnover of around £200k in 2005, turnover which increased exponentially hitting over £1 million in 2013 and £1.8 million in 2014.[20]

---

[12] L. G. Lerman, 'Misattribution in Legal Scholarship: Plagiarism, Ghostwriting and Authorship' [2001] 42 S. Tex, Law Review p. 467.

[13] J. S. Dursht, 'Judicial Plagiarism: It May Be Fair Use but Is It Ethical?' [1996] 18 CARDOZO L. REV. 1253, p.1253.

[14] L. G. Lerman, *Ibid*.

[15] See for instance: 'Student Wins Plagiarism Suit Against Professor and University', http://www.nytimes.com/1997/09/24/us/student-wins-suit-accusing-a-professor-of-plagiarism.html, accessed 09 April 2018.

[16] J. Gurney-Read, *Ibid*.

[17] Quote taken from C. Middleton, 'Dissertation: A first-class essay? Yours for just £660', http://www.telegraph.co.uk/education/universityeducation/8938495/Dissertation-A-first-class-essay-Yours-for-just-660.html, accessed 09 April 2018.

[18] Quote taken from J. Gurney-Read, *Ibid*.

[19] S. Mann, 'How Ghost-Writers Are Killing University Degrees', http://www.huffingtonpost.co.uk/sandi-mann/ghost-writing-universities_b_5019870.html, accessed 09 April 2018.

[20] J. Gurney-Read, *Ibid*.

The price tag can be hefty with "clients looking for an empirical study can expect to pay in the region of £17,000."[21] Despite the prices, the number of companies on the market has only been increasing.

This increase of offers is facilitated by the Internet. Indeed, these companies can hire anyone who fit their profile, and the person can work from anywhere he wants, as long as the deadline is respected. The Internet also allows companies to be competitive by proposing essays for as little as £300 for a 2:1 and £660 for a first-class essay.[22] Such competitiveness renders the service more and more available to any type of students and not only the wealthiest.

Moreover, Internet has facilitated this method of cheating by allowing the fast exchange of information. As Sandi Mann noted, "coursework was supposed to allow a broader depth of skill and knowledge to be assessed, but when we no longer know who we are assessing, this could turn out to be worthless."[23] The same could hold true for take-home exams.

The phenomenon is starting to unravel with scandals in various universities. For instance, in Australia, 70 students were facing suspension, and two were expelled for having used an online essay writing company: MyMaster. The investigation of Fairfax Media identified up to 1000 students from 16 universities had hired MyMaster to ghostwrite their essays and online tests.[24] The website was targeting a specific type of students as the site was only written in Chinese.[25] In Switzerland, the University of St Gallen has filed criminal charges against 200 students alleged of having submitted ghostwritten works as their own in 2015.[26]

2. Can one sell authors' rights for an illegal purpose?

Starting from the premise that the ghostwriter is so proud of his work that he wants to publish it under his name. Can he still do it or are his rights transferred to the person who paid for the work? Typically, in the relationship between the ghostwriter and the person hiring him, the intention of the parties is that the person hiring the ghostwriter will own the copyrights. However, without any written agreement the copyrights cannot be transferred.

2.1. What is author's right?

Black's Law Dictionary defines author as "one who produces, by his own intellectual labour applied to the materials of his composition, an arrangement or compilation new in itself. A beginner or mover of anything; hence efficient cause of a thing; creator; originator; a composer, as distinguished from an editor, translator or compiler."[27] Interestingly, with regard to scholarly writing, authorship has not been clearly defined in comparison to other fields. For instance, the International Committee of Medical Journal Editors noted that "each author should have participated sufficiently in the work to take public responsibility for the content."[28] This definition of an author is somewhat very different from the approach taken by legal scholars because it requires that any person with significant involvement in the production of the article is cited as one of the authors. Another useful standard was adopted by the American Association of University Professors ("AAUP") in 1990 and states that: "1. In his or her own work, the professor must scrupulously acknowledge every intellectual debt-for ideas, methods, and expressions-by means appropriate to the form of communication. 4. Scholars must make clear the respective contributions of colleagues on a collaborative project, and professors who have the guidance of students as their responsibility must exercise the greatest care not to appropriate a student's ideas, research, or

[21] J. Gurney-Read, *Ibid*.
[22] C. Middleton, *Ibid*.
[23] S. Mann, *Ibid*.
[24] L. Visentin, 'MyMaster essay cheating scandal: More than 70 university students face suspension', http://www.smh.com.au/nsw/mymaster-essay-cheating-scandal-more-than-70-university-students-face-suspension-20150312-1425oe, accessed 09 April 2018.
[25] L. Visentin, *Ibid*.
26 J. Wurz and J. Hunt, 'Swiss universities take action against ghostwriting, 'http://www.swissinfo.ch/eng/in-other-words_swiss-university-takes-action-against-ghostwriting/41879840, accessed 09 April 2018.
[27] H. C. Black, 'Black's Law Dictionary' (5th ed. West Pub. Co, 1981), p.121.
[28] J. P. Kassirer & M.Angell, 'On Authorship and Acknowledgments', [1991] 335 NEW ENG. J. MED. 1460, p.1511.

presentation to the professor's benefit; to do so is to abuse power and trust. 5. In dealing with graduate students, professors must demonstrate by precept and example the necessity of rigorous honesty in the use of sources and of utter respect for the work of others ...."[29]

Authors' rights have emerged in the eighteenth century as a solution to address the inequality in relations between authors and publishers. Contrary to copyrights which were linked to the material think, author's right referred to the content of the book. Through the passing of time, copyrights have englobed author's rights. For instance, both French and German copyright laws protect the work of the mind, respectively *oeuvres de l'esprit* and *persönliche geistige Schöpfungen*.[30] An essential feature of author's rights is that it protects the creativity of the author and that simple effort or investment is not enough, as held in the US case *Feist v. Rural*.[31]

In the beginning, a strong link between the rights and the author existed. For instance, in Germany, ownership rights by corporations was severely restricted or even impossible.[32] Common law being more flexible and business oriented. Therefore, Common law jurisdictions were more willing to accept corporate ownership through the concept of work for hire. This principle means that at Common law, employers own the copyright over the work created by their employees. Consequently, although morally questionable, the fact that a senior partner uses the work of an associate as his own is totally acceptable under Common law rules. Generally, under Civil law, employers only enjoy an exclusive licence to the economic rights on work created by their employees. This difference might explain the wide range of ghostwriting sites operating in the UK while finding a ghostwriter in France is much more difficult. Indeed, while the protection of moral rights has been forcefully defended in Civil law countries, in Common law countries, the protection of personality has been separate from the law of copyrights. However, neither the tort of passing off[33] nor the tort of falsehood can be applied to using a work paid for in order to obtain a university degree.

Authors' rights have two distinct components: the economic rights in the work and the moral rights of the author. The economic rights of the author are a property right limited in time and which may be transferred by the author to other people. Such right allows the author to profit financially from his creation, and include the right to authorise the reproduction of the work in any form, according to Article 9 of the Berne Convention. On the other hand, the protection of the moral rights is based on the view that a creative work reflects part of the author's personality. This idea of the work being an integral part of the author's personality has been forcefully defended in Civil law countries. Consequently, the moral rights are to the author, and cannot be transferred. Unfortunately, the moral rights' regimes differ greatly between countries. For instance, the infringement of the moral rights of an author is actionable as a breach of statutory duty in the United Kingdom and Ireland.[34] Although the regimes differ, typically the right of the author to be identified is granted by all regimes. Such moral rights are protected under Article 6bis of the Berne Convention. The Directive 2006/116 refers to author's rights without many guidelines.

However, none of these laws has ever envisaged the existence of ghostwriter and the legal consequences for authorship rights.

2.2. Selling author's right for fraudulent reasons

"Although explicit consent to the appropriation of one's work is less ethically troubling than nonconsensual use, several problems still remain."[35] For instance, in case of dispute, if the client tries to sue the ghostwriter, can he really rely on the contract terms? Under most laws, especially English law, a

[29] B. L. Williamson, '(Ab) Using Students: [T]he Ethics of Faculty Use of a Student's Work Product', [1994] 26 ARIZ. ST. L.J.1029, pp. 1043-44.
[30] § 2 Abs. 2 UrhG.
[31] Feist Publications, Inc., v. Rural Telephone Service *Co*., 499 U.S. 340 (1991).
[32] §§ 7, 8, 9 UrhG.
[33] The tort of passing off prevents traders from misrepresenting goods or services as being the goods or services of another or related to the goods and services of another. For the requirements see: Lord Diplock in Erven Warnink v. Townend & Sons Ltd. (1979 AC 731, 742 (HL)) (the "Advocaat Case") and Lord Oliver in Reckitt & Colman Products Ltd v Borden Inc [1990] 1 All E.R. 873. The tort of malicious falsehood refers to false statement made maliciously in the view of causing damage to the claimant. Section 3(1) of the Defamation Act 1952
[34] s. 103, Copyright, Designs and Patents Act 1988 c. 48; s. 137, Copyright and Related Rights Act 2000 (No. 28 of 2000)
[35] L. G. Lerman, *Ibid*.

contract with a fraudulent content is invalid or can be voided on the ground that it is contrary to public policy or public interest.[36] An agreement to pay for a work that will then be passed as one's own is contrary to good morals which render the contract void.

Similarly, contracts to commit a civil wrong, such as fraud, are illegal and cannot be enforced by courts. The starting point is the dicta of Mansfield in *Holman v Johnson*[37], where Lord Mansfield explained that the illegality is not ruled for the sake of the defendant but rather that the Court will not lend their aid to a plaintiff which found his cause of action upon an immoral or illegal act or in transgression of a positive law of the UK. If one of the parties to the contract knows that the contract is illegal, then only the innocent party is entitled to rely on the contract.[38] A court will never enforce an illegal contract ordering a party actually to do something that is unlawful or contrary to public policy. As Lord Sumption JSC held in *Les Laboratoires Servier v Apotex*, "although described as a defence, it is, in reality, a rule of judicial abstention. It means that rather than regulating the consequences of an illegal act (for example by restoring the parties to the status quo ante, in the same way as on the rescission of a contract) the courts withhold judicial remedies, leaving the loss to lie where it falls."[39] However, in certain circumstances, a party may be able to claim damages on the contract.

This means that since the contract is illegal, due to the illegality of the object of the contract, the author's rights either do not pass to the client or revolve to the original author. Indeed, an illegal contract cannot be enforced by a guilty party, *Cowan v Milburn*.[40] A student that order an essay to be written with a specific grade for a specific date knows or should know that what he is ordering is illegal. Therefore the student does not have any defence. The severity of the rule is mitigated in two ways; first, the rule only prevents the party from enforcing the contract, it does not prevent him from recovering damages in tort when the other party's conduct constitutes an independent tort.[41] Second, the definition of 'guilty' is rather vague when the illegality lies in the method of performance. A party is not guilty only because he performs a contract unlawfully.[42] The second manner does not apply as it is not only the performance that is unlawful, the object of the contract is to commit fraud.

The original author will thus keep his author's rights, the client, however, might claim restitution in respect to the money paid. The general rule is that money paid under an illegal contract cannot be recovered, *Parkinson v College of Ambulance*.[43] In practice, however, many exceptions exist. One of them is fraudulent misrepresentation if the student can prove that the other party misrepresent the validity of the contract.[44] By doing so, the client will acknowledge his fraud and will probably be expelled from the university in which he studies, therefore, it seems unlikely that the client will ever complain that the original author published the work due to the far-reaching consequences for his future.

3. Effect of Ghostwriter

Ghostwriting is killing university degrees, especially when the demand comes from students at well-known universities. Although these universities try to safeguard the standards of their academic programme and their reputation through the integrity of their students, as Sandi Mann noted: "today's student need not complete a single piece of coursework themselves across their entire degree."[45] Moreover, students, when buying their essays, can require the essay to be of a specific degree class, paying a premium for higher standards of work. Such choice begs the question; is it really possible to achieve such grade when the person writing never assisted to any of the lectures? At the end of the day, students only spend a relatively small sum to enjoy free time while someone else is writing their essays.

[36] Les Laboratoires Servier v Apotex [2014] UKSC 55.
[37] (1775) 1 Cowp 341, at 343.
[38] Clay v Yates [1856] 1 and N 73.
[39] [2014] 3 WLR 1257, at 23.
[40] (1867) L. R. 2 Exch. 230; Alexander v Rayson (1936) 1 KB 169; *Pearce v Brooks* (1866) LR 1 Ex 213.
[41] Saunders v Edwards [1987] 1 WLR 1116.
[42] St John Shipping Corp v. Rank Ltd [1957] 1 QB 267.
[43] [1925] 2 KB 1.
[44] Hughes v Liverpool Victoria Legal Friendly Society [1925] 2 KB 482.
[45] S. Mann, *Ibid*.

Although universities use expensive software designed to detect cheating, all these software are limited to detection of plagiarised works. For instance, Turnitin cannot detect original works that have not been written by the student himself. Additionally, ghostwriters are often students graduated from English universities who have been accustomed to avoid falling into the trap of plagiarism, rendering the work virtually undetectable. Moreover, various companies advertised plagiarism proof scripts, such as academic ghostwriting bragging that "we know if you are caught you lose your degree. In fifteen years our work has never been detected."[46] If the work was written by another student with an average grade, then "it is highly likely that a large percentage of our University graduates will be clutching ghost-written degrees at their graduation ceremonies this summer."[47] This, in turn, devaluates University degrees. At the same time, the fact that law professors use the works of research assistants without truly acknowledging their work, raise a similar problem: the professor is not being truthful in representing that he is the author of the work. The problem thickens as many excused law professors from this practice. How can one condemn a student from using ghostwriting services while that person might use the work of his research assistants as his own?

One of the most harmful results is the delegation of thinking. The student is delegating research and writing to another person. The student is then evaluated based on the thoughts of that other person. Researching is one of the most important steps in writing as it obliges the writer to carefully think about the problem and what kind of information he needs to collect.[48] Law school is normally about preparing critical thinkers, but if the students hire a ghostwriter, first their critical thinking will not evolve, and second, they will have to endorse a certain way of thinking as their own. This delegation of thinking is especially problematic with regard to LL.M or PhD thesis. Indeed, the PhD researcher will have to defend the ideas and a way of thinking of someone else which might not reflect their own. Another aspect is that such services incentivise great thinkers to write essays rather than articles, as articles are not remunerated while essay-writing is.

The delegation of thinking by law professors to research assistants, on top of creating a similar problem as enounced above, can create deception for the reader. Indeed, readers might accord greater authority to the work than it actually merits only because of the respect for the author while the real author is a research assistant.[49] If the professor publishes the article without doing more research, it can be that the mistakes made by the research assistant, due to his lack of experience, will be further disseminated by readers relying on the work.[50] Professor Monroe Freedman explained a story of a senior professor at a prestigious law school who published a book under his own name. He had by the time an impressive CV. After the publication of the book, a complaint from an author of a previously published article arose. The author of the article alleged that extensive portions of the book were taken without any attribution to his article. The professor argued that he did not commit plagiarism, but instead it was his research assistant that was too inexperienced. That explanation was accepted, and the professor has by now access to the status of emeritus at the same law school.[51]

Three situations must be distinguished: the client that leaves *carte blanche* to the writer without giving a title but just a brought topic such as contract law. The second situation is when the client gives the title but leaves the writer to analyse the problem from the point of view that he wants. Finally, the client sends the title and the arguments that he wants to find in his work. While the two first situations are clearly frauds, the latest starts to create problems since it is similar to the situations of senior lawyers or law professors.

Worryingly, these companies try to hook their customers as soon as possible to have a regular workflow. This means that some students are using their services during the whole course of their

[46] 'Academic Ghostwriting', http://www.academicghostwriting.com/, accessed 09 April 2018.
[47] S. Mann, *Ibid*.
[48] E. Fajans & M. R. Falk, 'Against the Tyranny of Paraphrase: Talking Back to Texts', [1993] 78 CORNELL L. REV. 163, p. 166.
[49] D. W. Cooper, 'Unethical Scholarship Today: A Preliminary Typology' [11-12 March 1988] Address Before the Humanities Science and Technology Conference.
[50] L. G. Lerman, *Ibid*., p. 467.
[51] M. H. Freedman, 'The Professional Responsibility of the Law Professor: Three Neglected Questions' [1986] 39 VAND. L. REV. 275, p. 281.

studies.[52] It is particularly concerning as it means that some law students will end up with a LL.B degree while they never wrote any of their assignments during their three years of studies. That the student has a degree without working is a big problem, but the greatest problem is when the student is hired, and the employer soon realises that the student has little to no knowledge, then the specific degree from that university will be meaningless after a while, even the degree held by a student who has average grade but did all his essays on his own. Linked to this problem is the fact that some professors might give lower grades to the essays written by the students themselves if confronted with a large sample of ghostwritten works. As Michelle Bergadaà, a European expert in plagiarism and ghostwriting explained that is highly unfair to the students who do their own work that people paying for their work to be done will obtain the same degree as them.[53]

Conclusion

Ghostwriter companies are undermining the whole system. However, all the blame is not to be put on the companies. These companies are responding to a booming demand. Law schools are also responsible for part of the problem. Indeed, the English system based on short and long-term coursework or take-home exams, allows this kind of practice to proliferate. Some universities do not even require LLM students to sit any exams but only rely on coursework, which facilitates the use of ghostwriting services. Although prestigious universities are claiming that with their type of teaching system, passing off the work of others as his own is difficult.[54] Surely, if a throughout investigation is conducted, ghostwrite works will be found. Close supervision through intensive teaching is not a real barrier for whom wants to cheat the system.

The digitalisation of the law and the teaching of law has enabled new forms of cheating. Indeed, students are prohibited from dishonesty and misrepresentation, but there is no specific requirement of accuracy in the attribution of the work. Through their deceptive behaviour, the students help to corrupt the integrity of the system. Some students might think that it is ok to achieve professional advancement through dishonest and opportunistic behaviour. When the opportunistic behaviour is uncovered, through employers realising that their new employees have little to no knowledge, then the value of specific degrees of that university will decrease even for students who spent their time working on their essays but obtained lesser grades.

Ghostwriting services are not *per se* illegal as author's rights can be sold by the original author. In some countries, the original author remains with moral rights over the essay, in other such as the Common law countries, the ghostwriter can be said as doing work for hire. In Switzerland for instance, the passing off work as one's own is regarded as a forgery for other it is a simple case of fraud. Others such as Michelle Bergadaà call it theft. Whatever is the name given all agree to say that it is highly unfair to the students who do their own work.

The service is not illegal *per se* as it is not advertised as a plagiarism system but as a system providing guidance. So companies get around the law by insisting that their aim is to provide model answers for learning purposes only. Like escorting, where the girl is supposedly only spending time with the client without sexual intercourses, ghostwriting is providing model answers. As Sandi Mann said: "they [the companies] usually insist, quite sternly, that no student should ever submit a piece of coursework that they have not themselves written. Yeah, right." Indeed, everyone knows that after spending 300£ on an essay, the student is willing to re-write that essay that he knows is an original work and therefore 'plagiarism-free.'

When accepting the job, the ghostwriter also accepts to give away his author's right. However, because the work is used to commit a fraud, the rights reverted to the original author as the contract between the ghostwriter and the student is void and unactionable in front of a court. The client can then

[52] J. Gurney-Read, *Ibid*.
[53] J. Wurz and J. Hunt, *Ibid*.
[54] Quoting the spokesman from the University of Oxford, J. Gurney-Read, *Ibid*.

claim damages in tort, but by doing so, he will be caught for plagiarism and probably expelled from the university.

Bibliography

Case-Law

1. Alexander v Rayson (1936) 1 KB 169
2. Clay v Yates [1856] 1 H&N 73
3. Cowan v Milbourn (1867) LR 2 Exch 230
4. Easley v. Univ. of Mich. Bd. of Regents, 906 F. 2d 1143, 1143-46 (6th Cir. 1990)
5. Erven Warnink v. Townend & Sons Ltd. (1979 AC 731, 742 (HL))
6. Feist Publications, Inc., v. Rural Telephone Service Co., 499 U.S. 340 (1991)
7. Holman v Johnson (1775) 1 Cowp 341
8. Hughes v Liverpool Victoria Legal Friendly Society [1925] 2 KB 482
9. In re Lamberis, 443 N.E.2d 549, 552-53 (I11. 1982)
10. Les Laboratoires Servier v Apotex [2014] UKSC 55 ; [2014] 3 WLR 1257
11. Parkinson v College of Ambulance Ltd & Harrison [1925] 2 KB 1
12. Pearce v Brooks (1866) LR 1 Ex 213
13. Reckitt & Colman Products Ltd v Borden Inc [1990] 1 All E.R. 873
14. Saunders v Edwards [1987] 1 WLR 1116
15. St John Shipping Corp v. Rank Ltd [1957] 1 QB 267

Secondary sources

1. 'Academic Ghostwriting', http://www.academicghostwriting.com/, accessed 9 April 2018.
2. Arthur D. Austin, 'Footnotes as Product Differentiation', [1987] 40 VAND. L. REV.1131.
3. Henry Campbell Black, 'Black's Law Dictionary' (5th ed. West Pub. Co, 1981)
4. D. W. Cooper, 'Unethical Scholarship Today: A Preliminary Typology' [11-12 March 1988] Address Before the Humanities Science and Technology Conference
5. J. S. Dursht, 'Judicial Plagiarism: It May Be Fair Use but Is It Ethical?' [1996] 18 CARDOZO L. REV. 1253.
6. E. Fajans and M. R. Falk, 'Against the Tyranny of Paraphrase: Talking Back to Texts' [1993] 78 CORNELL L. REV. 163.
7. M. H. Freedman, 'The Professional Responsibility of the Law Professor: Three Neglected Questions' [1986] 39 VAND. L. REV. 275.
8. J. Gurney-Read, '£1,700 for a dissertation, but what's the real cost of plagiarism?', http://www.telegraph.co.uk/education/educationnews/11532848/1700-for-a-dissertation-but-whats-the-real-cost-of-plagiarism.html, accessed 9 April 2018.
9. J. P. Kassirer & M. Angell, 'On Authorship and Acknowledgments' [1991] 335 NEW ENG. J. MED. 1460.
10. L. G. Lerman, 'Misattribution in Legal Scholarship: Plagiarism, Ghostwriting and Authorship' [2001] 42 S. Tex. Law Review 467.
11. Alexander Lindey, 'Plagiarism and Originality' (New York: Harper. & Brothers, 1952).
12. S. Mann, 'How Ghost-Writers Are Killing University Degrees', http://www.huffingtonpost.co.uk/sandi-mann/ghost-writing-universities_b_5019870.html, accessed 9 April 2018.
13. C. Middleton, 'Dissertation: A first-class essay? Yours for just £660', http://www.telegraph.co.uk/education/universityeducation/8938495/Dissertation-A-first-class-essay-Yours-for-just-660.html, accessed 9 April 2018.
14. 'New World College Dictionary' (Webster's New World 2002) Webster's 4th ed.
15. R. A. Posner, 'The Federal Courts: Crisis and Reform' (Harvard University Press 1985).
16. 'Student Wins Plagiarism Suit Against Professor and University', http://www.nytimes.com/1997/09/24/us/student-wins-suit-accusing-a-professor-of-plagiarism.html, accessed 9 April 2018.

17. L. Visentin, ‘MyMaster essay cheating scandal: More than 70 university students face suspension’, http://www.smh.com.au/nsw/mymaster-essay-cheating-scandal-more-than-70-university-students-face-suspension-20150312-1425oe, accessed 9 April 2018.
18. B. L. Williamson, ‘(Ab) Using Students: [T]he Ethics of Faculty Use of a Student's Work Product’, [1994] 26 ARIZ. ST. L.J.1029.
19. J. Wurz and J. Hunt, ‘Swiss universities take action against ghostwriting, ’http://www.swissinfo.ch/eng/in-other-words_swiss-university-takes-action-against-ghostwriting/41879840, accessed 9 April 2018.

DIGITALIZATION VS. ASSUMPTIONS OF THE THEORY OF INCENTIVES. TOWARDS A CHANGE OF THE PARADIGM FROM EXCLUSIVE RIGHTS TO NON-EXCLUSIVE RIGHTS AS PART OF THE REGULATION OF INTANGIBLE GOODS.

Gliściński Konrad[1]

Abstract

The shaping of the content of rights on intangible goods depends, inter alia, on the assumptions made about the models of organization of production processes and distribution of such goods as works or inventions. The currently adopted method of regulating such goods is based on exclusive rights. The aim of the article is to indicate what assumptions justify the adoption of such a model and their critical analysis. The starting point will be the neoclassical theory of public goods and the theory of incentives based on it, which justifies the creation of exclusive rights for the regulation of intangible goods. The indication will include that the conclusions derived from the theory of incentives do not take into account all the recommendations flowing from the theory of public goods. The theory of public goods does not justify, contrary to the claims made within the theory of incentives, that the creation of exclusive rights is a cost-free action, and desirable in every respect. The main point of the analysis is devoted to the assumption of the theory of incentives, which concerns the dominant model of creation and distribution of works and inventions. Contrary to the tacit assumption of this theory, people undertake creative and inventive activities within various models, guided by different motives. This state of affairs undermines the need to base the system of regulation of intangible goods, such as works or inventions, on the model of exclusive rights. What is more, taking into account other interests of entities creating under various models indicates that exclusive rights are not only not necessary, but can be harmful.

Keywords: theory of incentives, new creative paradigm, non-exclusive rights paradigm, models for the protection of copyright and patent law Introduction, non-market models of human behavior.

Introduction

The process of digitization of intangible goods translated into the growing need to create new regulations related to this area of human activity. In particular, it is visible in connection with the so-called the digital agenda and the project to create a digital single market within the EU. Dominant theoretical basis for constructing the content of rights on intangible goods is the so-called theory of incentives. It is the basis for creating new regulations and interpreting current ones. It assumes that without such rights - due to the non-rival nature of intangible goods - the market will not be able to deliver such goods at socially optimal levels (qualitative and quantitative). As a consequence, on the basis of the theory of interests, it is stated that rights in intangible goods have justification. This theory, however, indicates not only that these rights are justified, but also determines their content and normative character, i.e. that they are private intellectual property rights that grant exclusivity. It is understood that these rights, in certain precisely defined situations, may be subject to limitations. Such restrictions arise only in the context of the conflict of these rights with other rights (the concept of external limitation of rights). The theory of incentives is undoubtedly based on the market model of delivering creativity. Digitization, and the associated reduction in communication costs, however, allowed researchers to see that apart from the market model, there are also other non-market transactions in which creativity arises. Sometimes this

[1] *PhD candidate, Faculty of Law, Department of Civil Law, at Jagiellonian University in Kraków; lecturer at the Intellectual Property Rights Center of H. Grocjusz in Warsaw, and an analyst at the Klecki Foundation. Author of the book entitled "Wszystkie prawa zastrzeżone Historia sporów o autorskie prawa majątkowe, 1469–1928. [All rights reserved. The history of disputes over copyright. 1469 – 1928]. Currently finishing doctoral dissertation on models for the protection of intangible goods.*

phenomenon is referred to as a new paradigm (Ricolfi, Frosio). The aim of the paper will be to present the assumptions of the theory of incentives and its impact on the shape of the current system of rights on intangible goods, based on exclusive rights. Against this background, considerations will be presented that undermine the assumptions behind the theory of incentives and the resulting need to create exclusive rights.

1. Exclusive rights - a short economic perspective

We must start discussion about desired content of the right of intangible goods with the obvious statement that these rights, like all others, are positive. Their existence and content depend on the adopted goals and assumptions as to the relationship between these rights and the desired states of affairs. In other words, these rights are juridical measures aimed at achieving specific goals. The creation of rights involves the imposition of duties on other persons, which can limit the various freedoms of these persons. The constitutional principle of proportionality requires that such a limitation is made only when it is necessary to achieve a socially desirable goal and only to the extent necessary to achieve it.

In addition, it should be indicated that from a regulatory point of view, there is a basic difference on the property rights of material things and rights on intangible goods (e.g. patents, copyrights). For the purpose of further analysis, it is, therefore, appropriate to agree with the following statement:

> property rights in relation to things arise from possession. I have a better right to my wedding ring than you do because in a world of limited physical things I possessed it before you did. At base, this is true of all rights to things, even where my right is acquired from another in some way other than possession (eg, gift, sale, inheritance, specification). Intellectual property rights *must* arise for different, generally probably instrumental, reasons because one cannot possess something with no physical existence. A right to a trademark is not, therefore, a right of the same kind as my right to the clothes on my back. Copying a DVD is not, therefore, the same sort of wrong as stealing a car[2].

The theory of incentives seeks to indicate such instrumental reasons for the creation of copyright and patent law. This theory is the application of the neoclassical theory of public goods for the purpose of justifying the creation of exclusive rights to intangible goods. From this perspective, two model types of goods are distinguished: public goods (non-excludable and non-rivalrous) and private goods (excludable and rivalrous)[3]. In general, it is pointed out that - due to the assumptions adopted on the basis of neoclassical economics - private markets are not able to ensure the production of public goods at a socially optimal level. This situation justifies state intervention. Generally, the literature indicates two basic types of actions that can be taken by the state to reduce market failure caused by the occurrence of public goods: 1) public financing or 2) privatization of public goods[4]. Further considerations will be devoted to the privatization of public goods. At this point, it should only be emphasized that in practice the role of public finances and, more broadly, state activity in the area of production of intangible goods (in particular inventions) is significant. As indicated by **M. Mazzucato** - the role of the state is not limited only to the financing entity.

> In seeking to promote innovation-led growth, it is fundamental to understand the important roles that both the public and private sector can play. This requires not only understanding the importance of the innovation 'ecosystem' but especially what it is that each actor brings to that system. The assumption that the public sector can at best incentivize private sector-led innovation (through subsidies, tax reductions, carbon pricing, technical standards and so

[2] P. Cane, 'Rights in Private Law' in D. Nolan and A. Robertson (red.), 'Rights and Private Law', Oxford 2012, p. 137.

[3] Apart from these model types of goods, the following are also distinguished in economic literature: club goods (excludable and non-rivalrous) and common-pool resources (non-excludable and rivalrous).

[4] see further: K. Gliściński, Rola modelu ochrony dóbr niematerialnych w ramach Społecznego Systemu Wspierania Innowacji – zarys analizy, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego", Prace z Prawa Własności Intelektualnej, nr 3(121)/2013, Kraków 2013, R. Cooter and T. Ulen, 'Ekonomiczna analiza prawa' (Warszawa 2009); J.E. Stiglitz, 'Economic foundations of intellectual property law', Duke Law Journal 57:1693.

on), especially but not only in the face of the recent crisis, fails to account for the many examples in which the leading entrepreneurial force came from the State rather than from the private sector[5].

2. In search of a balance between two recommendations

From the point of view of private law, it is privatization that plays a major role in solving the problem of public goods. From this perspective, it is indicated that the privatization of public goods (by creating legal exclusivity) is a proper way to reduce market failure (recommendation no. 1). It seems reasonable to claim that the purpose of the Directive 2001/29/EC of 22.05.2001 on the harmonisation of certain aspects of copyright and related rights in the information society is to implement this recommendation. According to recital no. 4 harmonization of copyright law is to ensure *high level of protection of intellectual property*. It is assumed that such a high level of protection *will foster substantial investment in creativity and innovation*, and *lead in turn to growth and increased competitiveness of European industry.* Furthermore this *will safeguard employment and encourage new job creation*. As a consequence, the role of the directive is to create a series of mandatory exclusive rights and only optional limitations on these rights[6].

Such a regulatory approach results from taking into account, in the law-making process, only the first recommendation resulting from the public good theory. According to **M. Perelman**, the privatization of public goods - through IPRs - focuses on one aspect of the logic of public goods, while ignoring the second part of this theory. Let us remind you that the theory of public goods is an element of the standard neoclassical economy - operating with the concept of ideal competition. According to it, efficiency is maximized if products are sold at marginal prices. "[A] competitive firm always equates price and marginal cost, since its price is also its marginal revenue"[7]. At the same time, however, a fundamental problem arises here - whether the market can function, with the structure of high fixed costs and low zero marginal costs? As, for example, **D. Begg**, **G. Vernasca**, S**. Fischer** and **R. Dornbusch**, indicate:

> Producing information products such as films, music, and news programmes has a high fixed cost, but distributing these products digitally has almost a zero marginal cost and no capacity constraint. Scale economies are vast. Moreover, if marginal cost is close to zero, smart suppliers will price their products so that marginal revenue is also tiny[8].

This is because, among other things, the theory of supply indicates the existence of the principle of making a decision according to which "sunk costs are sunk. Costs already incurred should not affect new decisions"[9]. However, as part of the IPR discussion, this approach is forgotten. As a consequence, it is indicated that in such conditions the market does not work, so exclusive rights are necessary. As Perelman points out - despite the fact that an important element of neoclassical economics is that efficiency is maximized when goods are sold at prices equal to marginal costs, IPR advocates skip it[10].

In other words, they sweep considerations of efficiency under the carpet, focusing their attention on the profitability of the supplier, satisfied that if the business can make enough profit, nobody need worry about economic efficiency. This approach suggests a position that is inconsistent with the basic economic justification of the market, suggesting a desire to support the interests of business regardless of the consequences for the economy as a whole[11].

As a consequence - as **C. Greenhalgh** and **M. Rogers** indicate: "Economists and others have long argued that strong property rights applied to rival goods result in efficient outcomes. In contrast, strong property rights for nonrival goods involve a trade-off"[12]. Within the very logic of creating exclusive rights – according to the neoclassical theory of incentives - with respect to intangible goods, their inherent

[5] M. Mazzucato, 'The Entrepreneurial State: debunking public vs. private sector myths' (Anthem 2013) p. 167.
[6] Only a restriction which is mandatory is indicated in Article 5 (1).
[7] D. Begg, G. Vernasca, S. Fischer and R. Dornbusch, 'Economics' (London 2011) 10th Edition, p. 183.
[8] D. Begg, G. Vernasca, S. Fischer and R. Dornbusch, 'Economics' (London 2011) 10th Edition, p. 161.
[9] D. Begg, G. Vernasca, S. Fischer and R. Dornbusch, 'Economics' (London 2011) 10th Edition, p. 155.
[10] M. Perelman, 'Steal this idea. Intellectual property rights and the corporate confiscation of creativity' (New York 2002) pp. 180-188.
[11] M. Perelman, *Ibid*., p. 186.
[12] C. Greenhalgh and M. Rogers, 'Innovation, intellectual property and economic growth' (Princeton 2010) p. 27.

ineffectiveness is assumed. This is why the final shape of IPR is determined by conflicting recommendations resulting from the economic nature of intangible goods. That is why, the theory of public goods does not justify the unilateral strengthening (broadening) of exclusive rights. Consequently, it means that you need to look a balance between the state of complete exclusion and the state of free use of such goods. Each regulation must, therefore, take into account both opposing values. On the one hand, there is a threat that the public good will be produced below the socially desirable level. This state of affairs justifies the creation of exclusive rights, in accordance with recommendation no. 1. On the other hand, the introduction of restrictions on the use of goods will lead to its underutilization at a socially desirable level. It means that the privatization of public goods (e.g. by creating exclusive rights) is ineffective (creates a deadweight loss). This results in the recommendation No. 2, according to which the sphere of freedom (i.e. restrictions on exclusive rights) should be increased.

3. The tacit assumption of the incentives theory

As **N. Elkin-Koren**, **E. M. Salzenberger** pointed out the incentives theory rests upon two main assertions. "The first is that information is a public good and thus without central intervention, the investment in creative expressions and the resulting cultural and technological progress will be insufficient. The second is that property rights are the cheapest and most effective way for society to hold out these incentives"[13]. As it seems, the theory of incentives is based on yet another, tacit assumption, according to which the market model of production and distribution of intangible goods is one (strong version) or basic (weak version) model under which inventions and works are created. This is the assumption on which neoclassical economics is based.

Traditionally, the history of the development of rights on intangible goods is divided into two main periods. The first one in which privileges were created and the second when copyright and patent law were developed. There are many differences between the privilege-based system and the copyright and patent-based system. However, from our perspective, both of these systems are based on the same model for the protection of intangible goods, which is exclusive rights model. The system of regulation of intangible goods, based on exclusive rights, began to take shape with the emergence of merchant capitalism (XV century). As a consequence, it is possible to distinguish a period in which rights on intangible goods were governed by the principle of freedom of use (which existed since the beginning of civilization) and a period of exclusive rights. The regulatory principle of the first period is reflected in the Latin sentence *Oratio publicata res libera est*[14]. On the other hand, the system based on exclusive rights began to develop as Western Europe began the process called "Great Transformation" by **K. Polanyi.**

> The transformation implies a change in the motive of action on the part of the members of society: for the motive of subsistence, that of gain must be substituted. All transactions are turned into money transactions, and these, in turn, require that a medium of exchange be introduced into every articulation of industrial life. All incomes must derive from the sale of something or other, and whatever the actual source of a person's income, it must be regarded as resulting from sale[15].

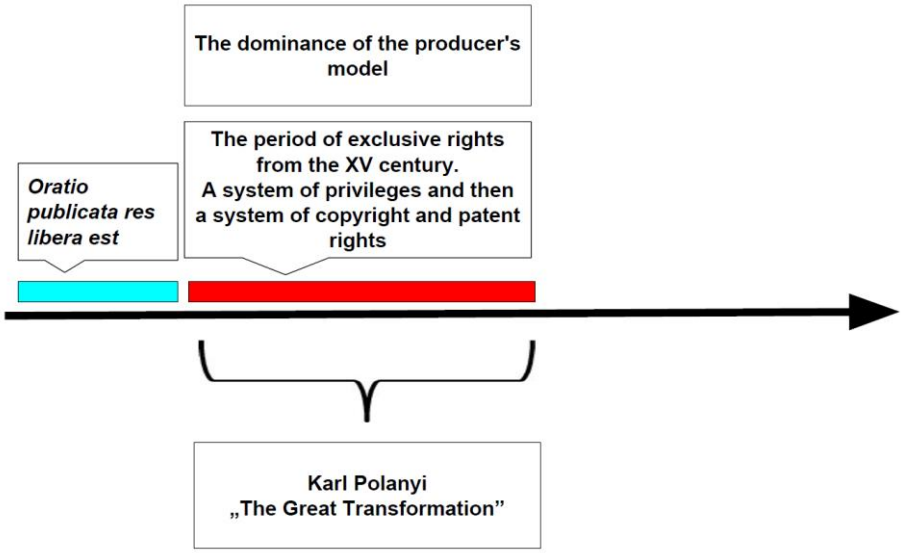
Therefore, the system of exclusive rights was intended to facilitate the organization of production processes and distribution of works and inventions that were created within the market production model. According to it, individual private entities are involved in the production processes of goods not to use them by themselves, or to share them with other people, etc., but to sell them (deliver) to consumers in the form of products or services. Producers supplying goods to many recipients, thanks to exclusive rights, can accumulate capital and allocate it to the production of new inventions and works. Owner of IPR, can decide who and on what basis (including at what price) has access to his inventions and works. This

[13] N. Elkin-Koren and E. M. Salzenberger, 'The law and economics of intellectual property in the digital age. The limits of analysis' (New York 2013) p. 57.
[14] Compare also: S. M. Grzybowski, 'Ochrona osobista stosunku do dzieła po śmierci twórcy – zagadnienia ogólne' (Kraków 1933) p. 21.
[15] K. Polanyi, 'The Great Transformation. The political and economic origins of our time' (Boston 2001) p. 43.

market-based innovation model was defined by **C. Baldwin** and **E. Hippel** as a centralized[16] **producers' model**. In economics, treating the producer model as the primary source of innovation originates from the theory of entrepreneurship (innovation) developed by **J. Schumpeter**. It was he who set up the producer (innovator) at the center of the economic development system. Recognition of this model as dominant (basic) has translated into political and legal actions aimed at building a system of motivating and stimulating theories of incentives.

> Producers, it is argued, are motivated to innovate by the expectation of profits. These profits will disappear if anyone can simply copy producers' innovations, and therefore, producers must be granted subsidies or intellectual property rights that give them exclusive control over their innovations for some period of time[17].

Figure 1: A simplified scheme for the development of regulation of intangible goods



4. Is the market model of production and distribution the only / basic model of generating works and inventions?

The producer's model - the market model of the organization, based on the principle of equivalent exchange - it is not the only model in which works and inventions are created. This does not mean, however, that the only alternative to the market model is the public funding model. **J. Rifkin** points out – "We are so used to thinking of the capitalist market and government as the only two means of organizing economic life that we overlook the other organizing model in our midst that we depend on daily to deliver a range of goods and services that neither market nor government provides"[18]. **Y. Benkler** describing how free software is created spoke about **commons-based peer production**. This new production model - in his opinion - is radically decentralized, collaborative, and non-proprietary. It is based on "sharing resources and outputs among widely distributed, loosely connected individuals who cooperate with each other without relying on either market signals or managerial commands"[19]. **M. Ricolfi**, in turn, indicates the emergence of a **new paradigm of creativity**. In his opinion, this model is characterized by "a non-market transaction which is part and parcel of an economic and social production mode based on

[16] Centralized, i.e. enabling the individual entity to control - via the IPR - the entire production and distribution (commercialization) process of the intangible goods.
[17] C. Y. Baldwin and E. Hippel, 'Modelling a Paradigm Shift: From Producer Innovation to User and Open Collaborative Innovation' [2011] Organization Science 22.6, p. 2.
[18] J. Rifkin, 'The zero marginal cost society. The internet of things, the collaborative commons, and the eclipse of capitalism', (New York 2014).
[19] Y. Benkler, 'The wealth of networks. How social production transforms markets and freedom' (London 2006) p. 60.

cooperation and sharin"[20]. As for the organization models of the creation of inventions, **C. Baldwin** and **E. Hippel** distinguish two models: **single user innovators** and **open collaborative innovation**. In the case of the user's model, inventors engage in an innovative activity, not to sell their inventions, but therefore to use them directly for their needs. Open collaborative projects, "attract participants who do not plan to use the design created by the project, but are instead motivated by incentives such as by incentives such as learning, reputation, and the fun of participation"[21]. Next to this, in his last book, Hippel distinguished the model of **free innovation,** which he defined as "a functionally novel product, service, or process that (1) was developed by consumers at private cost during their unpaid discretionary time (that is, no one paid them to do it) and (2) is not protected by its developers, and so is potentially acquirable by anyone without payment—for free. No compensated transactions take place in the development or in the diffusion of free innovations"[22]. All these examples indicate that the profit motive from the sale of products (works, inventions) is not the only motive for people to undertake creative and inventive activities.

5. The incentives theory and non-market transactions

From the point of view of the incentives theory, the above-indicated non-market models, should either not arise or should be completely marginal. Creators and inventors should not engage in creative and inventive activities, without legally guaranteed the possibility of appropriating the benefits of the effects of such activities. According to the theory of incentives, this is the relationship that justifies the creation of exclusive rights. The evidence collected by the above-mentioned authors, however, supports the thesis that people engage in such activity, without making access to such goods dependent on the fact of getting something in return.

At the same time, it should be emphasized that, these other models have not been created suddenly due to the emergence of the Internet (and resulting in a reduction in communication costs). Other than proprietary (i.e. based on exclusive rights) models of societal organizations have existed for a long time. The analysis of such other models based on commons was conducted, among others, by **E. Ostrom**[23].There is no doubt that the development of the Internet (and the associated reduction in communication costs) caused that human activity under non-market organizational structures has begun to be more perceptible. What is equally important, it turned out that such activity may not only produce complementary goods. It seems that – to certain extent – these alternatives models can compete with market models of production of intangible goods. At this point, however, it is important to point out that people undertake creative and inventive activities, apart from the market model and it is not a new phenomenon. On the contrary, history provides convincing arguments that people have made and continue to take such actions for various reasons. In other words, the monetary motif has never been the sole or basic motive for creative and inventive activities. Works and inventions were created in times and places where exclusive rights did not exist. This obvious observation - which is contrary to the basic assumption of the theory of incentives - is also confirmed by contemporary research. As **S. Bowels** and **H. Gintis** point out, in the light of the available research, assumption that „collective action is a motor of human history is considerably less puzzling"[24]. In their opinion, in fact

> The experiments confirmed that self-interest is indeed a powerful motive, but also that other motives are no less important. Even when substantial sums of money are at stake, many, perhaps most, experimental subjects were found to be fair-minded, generous toward those similarly inclined, and nasty toward those who violate these prosocial precepts[25].

[20] M. Ricolfi, 'The new paradigm of creativity and innovation and its corollaries for the law of obligations' in P. Drahos, G. Ghidini, H. Ullrich and L. Moraia, Kritika: Essays on Intellectual Property [2015] Volume 1, Cheltenham, p. 187.
[21] C. Y. Baldwin and E. Hippel, 'Modelling a Paradigm Shift: From Producer Innovation to User and Open Collaborative Innovation' [2011} Organization Science 22.6, p. 18.
[22] E. Hippel, 'Free Innovation' (Cambridge 2016) p. 1.
[23] E. Ostrom, 'Governing the Commons: The Evolution of Institutions for Collective Action' (Cambridge 1990).
[24] S. Bowles and H. Gintis, 'A cooperative species: human reciprocity and its evolution' (Princeton 2011) p. 6.
[25] S. Bowles and H. Gintis, *Ibid*.

The theory of incentives fits into the broader phenomenon of understanding the whole economy as a science of incentives[26]. "It is easy to miss the novelty of this definition. The language of incentives is a recent development in economic thought. The word <<incentive>> does not appear in the writings of Adam Smith or other classical economists. In fact, it didn't enter economic discourse until the twentieth century and didn't become prominent until the 1980s and 1990s. As **M. J. Sandel** points out incentives "are interventions that the economist (or policymaker) designs, engineers, and imposes on the world"[27]. In the case of rights on intangible goods, the argument that the limitation of exclusive rights will translate into a decrease in the willingness to invest (time or money) in creative and inventive activities, is repeated in all possible ways. The climax of this approach was the period of the market triumphalism of the 1980s. The consequence of tat way of thinking was the establishment of the TRIPS agreement[28]. The market approach is based primarily on emphasizing the freedom of individuals; their natural need to enter into voluntary exchange transactions, which in turn lead to the maximization of social well-being and the belief that the market is the best aggregator of information and a mechanism for forecasting the future. At the same time, it is indicated that all spheres of human life are in fact subject to (and should be subject to) market logic. This approach was fully expressed by **G. Becker** in his book The Economic Approach to Human Behavior (1976). However, as pointed out by **F. Block** and **M. R. Somers** - such an economic approach is wrong and is based on:

> unfounded assumption that human nature is that of a *homo economicus,* motivated above all by material self-interest or utility maximization. Moreover, it holds that our collective existence is that of homo economicus *writ large*; instead of simply having a market economy as *part* of collective life, we live in an entire market *society* shaped exclusively by the laws of the market. Finally, these market principles are, in effect perceived as part of the *natural* order of things; they are as immutable as the laws of nature and equally resistant to human intervention[29].

6. What does it mean, or more questions than answers...

Such evidence weakens the basic assumption underlying the theory of incentives, and hence the justification for creating exclusive rights in relation to intangible goods. Non-market models for the creation and distribution of works and inventions described above are not dependent on the existence of exclusive rights. On the contrary, the existence of such rights can generate difficulties for development of that alternatives models. The current shape of the system of rights on intangible goods is adapted to the needs (assumptions) of one of the models of the creation of works and inventions, i.e. the producer's model. It seems, however, that an adequate regulation system should take into account various models, their assumptions and contradictory recommendations resulting from them. Such a theoretical assumption, if it is to serve as a basis for shaping regulatory policy, of course requires answering a number of questions, both empirical and analytical.

First of all, it should be determined what is the real significance of alternative ways of generating inventions and works in relation to the producer's model? Making this determination, however, it should be borne in mind that the producer's model, for 500 years, in contrast to non-market models, obtained regulatory support. However, this state of affairs did not result from the recognition that the model has an advantage over other forms of organization. The history of development of rights on intangible goods justifies the claim that entities interested in creating in this model - as entities oriented on profit - had an interest in lobbying for it. At the same time, in practice, works and inventions created and distributed in other models did not compete with those of the producer's model. This state of affairs resulted from

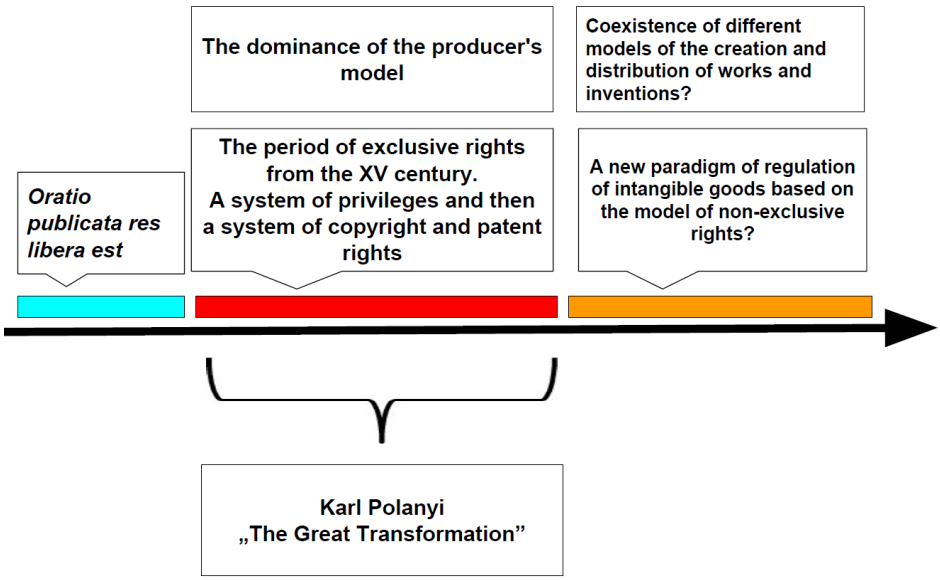
[26] J. Wilkin, 'Instytucjonalne i kulturowe podstawy gospodarowania. Humanistyczna perspektywa ekonomii' (Warszawa 2016) p. 32; M. J. Sandel, 'What Money Can't Buy. The Moral Limits of Markets' (London 2012) p. 85.
[27] M. J. Sandel, *Ibid*., p. 86.
[28] See more: C. May and S. K. Sell, 'Intellectual property rights. A critical history' (London 2006); P. Drahos and J. Braithwaite, 'Information Feudalism: Who Owns the Knowledge Economy?' (London 2002); J. Boyle, 'The Second Enclosure Movement and the Construction of the Public Domain' [Winter 2003] 66 Law and Contemporary Problems, pp. 33-74 https://scholarship.law.duke.edu/lcp/vol66/iss1/2, accessed 01 February 2018.
[29] F. Block and M. R. Somers, 'The Power of Market Fundamentalism. Karl Polanyi's Critique' (Cambridge 2014) p. 225.

technological limitations. When, along with the development of digital technologies, communication costs were significantly reduced, it turned out that the producer's model has a growing competition.

At this point, one should ask another question, i.e. how exclusive rights, protecting the producer's model, affect the possibilities of creating and distributing intangible goods within other models? Exclusive rights, which are also extended to the rights to dependent works / inventions, significantly limit the possibilities of using goods created in the producer's model by persons creating in other models. If these other models are considered equal, then such a limitation can not be justified. Once again, it should be emphasized that exclusive rights were not created as an end in itself. These rights were created because they were recognized as necessary for the creation and distribution of works and inventions. The theory of incentives justifies this, indicating that in the producer's model, producers act for profit, and thus the possibility of achieving them should be legally secured. If, however, works and inventions can arise without these rights (as is the case with non-market models), the justification for their creation is weakened. Exclusive rights serve the interests of entities operating under the producer's model. Creators and inventors working within other models have different interests and needs that justify a different type of legal protection. There is no theoretical reason why entities operating in other models should adapt to the rules created for one model.

The third issue is therefore the answer to the question how to reconcile the interests of entities operating in different models. The previous dominance of the system adapted to the needs of the producer's model - in connection with the recognition of the existence of other models - requires changes. It seems that further analyzes should aim to take into account the interests of other entities than those operating under the producer's model. One of the possible directions of the proposed reforms is in this context to increase the significance of non-exclusive rights[30]. This may lead to the transition to the next paradigm of regulation of intangible goods.

Figure 2: Possible development of regulation of intangible goods



[30] M. Ricolfi, 'The new paradigm of creativity and innovation and its corollaries for the law of obligations' in P. Drahos, G. Ghidini, H. Ullrich and L. Moraia, 'Kritika: Essays on Intellectual Property' (Cheltenham 2015) Volume 1; G. Frosio, 'A History of Aesthetics from Homer to Digital Mash-ups: Cumulative Creativity and the Demise of Copyright Exclusivity' [2015] Law and Humanities, Volume 9; D. Krauspenhaar, 'Liability Rules in Patent Law. A Legal and Economic Analysis' (Heidelberg 2015); R. Castro Bernieri, 'Ex-post liability rules in modern patent law' (Antwerpen 2010); A. Kur and J. Schovsbo, 'Expropriation or Fair Game for All? The Gradual Dismantling of the IP Exclusivity Paradigm Max Planck Institute for Intellectual Property' [2009] Competition & Tax Law Research Paper No. 09-14; K. Gliściński, 'Wszystkie prawa zastrzeżone. Historia sporów o autorskie prawa majątkowe' (Warszawa 2016) pp. 1469-1928.

Conclusions

The system of regulation of intangible goods, such as inventions and works, was shaped by the assumption that one or the basic model thanks to which the society can gain access to such goods is a model based on market transactions (producer's model). With the creation of the Internet it became clear that such an assumption is not true. It turned out that people engage their time and abilities in creating inventions and works not only because they want to make a profit from selling them. In other words, there are alternative to the producer's model models of the organization of production and distribution processes of intangible goods. It should be emphasized that such alternative human activity is nothing new and has always been an element of the creative landscape. The creation of the Internet and the associated reduction in communication and collaboration costs only made it possible to visualize this fact. The full development of other models of the organization of human creative activity, however, is limited by the rules created for the needs of one model – i.e. the producer's model. As it seems, a properly designed system of regulation of intangible goods should take into account the various models of organization of production processes and the distribution of such goods. Consequently, it should also take into account the different interests of the entities creating in such alternative models. In my opinion, there is no theoretically relevant argument justifying the existence of the preference of the producer's model. This preference consists in the fact that the interests of the entities creating in this model have been recognized as universal and secured by the system of rights. It should be emphasized that for entities creating in alternative models, exclusive rights are not important, and even hinder creation in these alternative models. Exclusive rights are needed only for entities that are interested in the sale of works or inventions. For entities which create under the alternative models it is more important to obtain legal freedom to use the already existing goods for the needs of creating their own works and inventions, as well as the possibility of freely sharing new goods created by them. Entities that create for other reasons than the desire to directly sell the intangible goods created by them, should not be burdened with obligations resulting from the existence of exclusive rights. The fact that these alternative models may compete with the producer's model does not mean that their existence and development should be limited. Entities interested in creating under the producer's model should adapt to the changed social and economic environment. The models analysed above can cooperate with each other, providing the society with various goods of different quality. However, for such cooperation to occur, the rules created for the protection of one model must undergo a significant reform. The first step in this respect should be to increase the role of non-exclusive rights in the system regulating intangible goods.

Bibliography

1. K. J. Arrow, ‘Economic Welfare and the Allocation of Resources for Invention’ in National Bureau of Economic Research (ed.), The Rate and Direction of Inventive Activity, Princeton: Princeton University Press 1962.
2. C. Y. Baldwin and E. Hippel, ‘Modelling a Paradigm Shift: From Producer Innovation to User and Open Collaborative Innovation’ [2011] Organization Science 22.6.
3. D. Begg, G. Vernasca, S. Fischer and R. Dornbusch, ‘Economics’ (London 2011) 10th Edition.
4. Y. Benkler, The Penguin and the Leviathan: How Cooperation Triumphs Over Self-Interest, New York 2011.
5. Y. Benkler, ‘The wealth of networks. How social production transforms markets and freedom’ (London 2006).
6. F. Block and M. R. Somers, ‘The Power of Market Fundamentalism. Karl Polanyi's Critique’ (Cambridge 2014).
7. S. Bowles and H. Gintis, ‘A cooperative species: human reciprocity and its evolution’ (Princeton 2011).
8. J. Boyle, ‘The Second Enclosure Movement and the Construction of the Public Domain’ [Winter 2003] 66 Law and Contemporary Problems, https://scholarship.law.duke.edu/lcp/vol66/iss1/2, accessed 01 February 2018.

9. P. Drahos, J. Braithwaite, Information Feudalism: Who Owns the Knowledge Economy?, London 2002.
10. G. Calabresi, A. Douglas Melamed, Property Rules, Liability Rules, and Inalienability: One View of the Cathedral, Harvard Law Review, Volume 85, April 1972, Number 6.
11. P. Cane, 'Rights in Private Law' in D. Nolan and A. Robertson (red.), 'Rights and Private Law', Oxford 2012.
12. R. Castro Bernieri, 'Ex-post liability rules in modern patent law' (Antwerpen 2010).
13. W. M. Cohen, R. R. Nelson, J. P. Walsh, Protecting Their Intellectual Assets: Appropriability Conditions and Why U.S. Manufacturing Firms Patent (or Not), NBER Working Paper No. 7552 (2000).
14. R. Cooter and T. Ulen, 'Ekonomiczna analiza prawa' (Warszawa 2009).
15. P. Drahos and J. Braithwaite, 'Information Feudalism: Who Owns the Knowledge Economy?' (London 2002).
16. N. Elkin-Koren and E. M. Salzenberger, 'The law and economics of intellectual property in the digital age. The limits of analysis' (New York 2013).
17. G. Frosio, 'A History of Aesthetics from Homer to Digital Mash-ups: Cumulative Creativity and the Demise of Copyright Exclusivity' [2015] Law and Humanities, Volume 9.
18. K. Gliściński, Rola modelu ochrony dóbr niematerialnych w ramach Społecznego Systemu Wspierania Innowacji – zarys analizy, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego", Prace z Prawa Własności Intelektualnej, nr 3(121)/2013, Kraków 2013.
19. K. Gliściński, 'Wszystkie prawa zastrzeżone. Historia sporów o autorskie prawa majątkowe' (Warszawa 2016).
20. C. Greenhalgh and M. Rogers, 'Innovation, intellectual property and economic growth' (Princeton 2010).
21. S. M. Grzybowski, 'Ochrona osobista stosunku do dzieła po śmierci twórcy – zagadnienia ogólne' (Kraków 1933).
22. E. Hippel, 'Free Innovation' (Cambridge 2016).
23. W. N. Hohfeld, Some fundamental legal conceptions as applied in judicial reasoning, The Yale Law Journal Vol. 23, No. 1 (Nov., 1913, http://www.jstor.org/stable/785533 (22.05.2017).
24. D. Krauspenhaar, 'Liability Rules in Patent Law. A Legal and Economic Analysis' (Heidelberg 2015).
25. A. Kur and J. Schovsbo, 'Expropriation or Fair Game for All? The Gradual Dismantling of the IP Exclusivity Paradigm Max Planck Institute for Intellectual Property' [2009] Competition & Tax Law Research Paper No. 09-14.
26. M. Lemley, P. Weiser, Should property or liability rules govern information?, Texas Law Review, Vol. 85, numer 4, 2007.
27. R. C. Levin, A. K. Klevorick, R. R. Nelson, S. G. Winter, Appropriating the Returns from Industrial Research and Development, Brookings Paper-s on Economic Activity, 3:1987.
28. C. May and S. K. Sell, 'Intellectual property rights. A critical history' (London 2006).
29. A. Marmor, Law in the age of pluralism, Oxford 2007.
30. M. Mazzucato, 'The Entrepreneurial State: debunking public vs. private sector myths' (Anthem 2013).
31. E. Ostrom, 'Governing the Commons: The Evolution of Institutions for Collective Action' (Cambridge 1990).
32. M. Perelman, 'Steal this idea. Intellectual property rights and the corporate confiscation of creativity' (New York 2002).
33. K. Polanyi, 'The Great Transformation. The political and economic origins of our time' (Boston 2001).
34. M. Ricolfi, 'The new paradigm of creativity and innovation and its corollaries for the law of obligations' in P. Drahos, G. Ghidini, H. Ullrich and L. Moraia, 'Kritika: Essays on Intellectual Property' (Cheltenham 2015) Volume 1.
35. J. Rifkin, 'The zero marginal cost society. The internet of things, the collaborative commons, and the eclipse of capitalism', (New York 2014).
36. M. J. Sandel, 'What Money Can't Buy. The Moral Limits of Markets' (London 2012).
37. J.E. Stiglitz, 'Economic foundations of intellectual property law', Duke Law Journal 57:1693.

38. J. E. Stiglitz, B. Greenwald, Creating a Learning Society: A New Approach to Growth, Development, and Social Progress, New York 2014.
39. J. Wilkin, ‘Instytucjonalne i kulturowe podstawy gospodarowania. Humanistyczna perspektywa ekonomii’ (Warszawa 2016).
40. S. Wronkowska, ‘Problemy racjonalnego tworzenia prawa’ (Poznań 1982).

THE INFLUENCE OF DIGITALIZATION TO THE LEGAL PROTECTION OF TRADE SECRETS

Kontrimas Vaidas[1]

Abstract

The economy is increasingly based on knowledge and valuable proprietary information, which is used as a business competitive tool. Most of knowledge or information from which business derive competitive advantages nowadays is considered to be and protected as trade secrets. We should admit that fast paced development and use of information technologies, as a part of digitalization process, increasingly influences not only the business competition, but also the protection and use of business knowledge and valuable proprietary information. Especially given the fact that most of the information is stored and accessible as electronic data.

This paper will explore what is the influence of development and use of information technologies to legal protection of trade secrets and to prohibition of unfair competition actions upon unlawful disclosure and (or) use of trade secrets. Subsequently, this paper will deal with analysis of new European Union regulation on protection of trade secrets, (i. e. directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure) and will highlight whether new European Union regulation covers main challenges of digitalization to the protection of trade secrets.

Keywords: Digitalization, trade secrets, protection, unfair competition.

Introduction

Nowadays the economy is increasingly based on knowledge and valuable proprietary information. Such information and (or) knowledge is certainly considered to be business intangible asset. Of course, such information and (or) knowledge is used as a business competitive tool. However, not every innovation or knowledge can be legally protected as a patent. Moreover, in certain cases a patent could not be treated as an efficient form of protection. Especially due to legal regulation, which provides patent protection for a certain limited period of time. For these reasons, most of knowledge or information from which business derive competitive advantages nowadays is considered to be and protected as trade secrets.

We should admit that fast paced development and use of information technologies, as a part of digitalization process, increasingly influences not only the business competition, but also the protection and use of business knowledge and valuable proprietary information. Especially given the fact that most of the information is stored and accessible as electronic data.

In the light of the above, this paper will explore what is the influence of development and use of information technologies to legal protection of trade secrets and to prohibition of unfair competition actions upon unlawful disclosure and (or) use of trade secrets. Subsequently, this paper will deal with analysis of new European Union regulation on protection of trade secrets, i. e. directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure[2], which has to be implemented by Member States by 9 June 2018. This analysis will highlight whether new European Union regulation covers the main challenges of digitalization to the protection of trade secrets.

---

[1] *PhD student at the Vilnius University, Faculty of Law. The field of research is concerned with unfair competition actions, the prohibition of unfair competition, determination of damages caused by unfair competition actions and protection of trade secrets, etc.*

[2] European Parliament and of Council Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L 157.

These aspects are important, as the protection of trade secrets is becoming more complex due to the fact that knowledge and information are significant not only to business and its competition, but also to the spread of development and innovation in information technologies.

1. Definition of trade secrets

Before analysing the protection of trade secrets and the influence of development and use of information technologies to legal protection of trade secrets, it shall be clarified and defined what knowledge and valuable proprietary information shall be considered as trade secrets. Moreover, it is worth to analyse what protection is granted to trade secrets in accordance to legislation.

First of all, it should be noted that information having commercial (industrial) value can be protected as commercial (trade) secret, provided that the information meets the criteria indicated in the Art. 1.116(1) of the Civil Code of the Republic of Lithuania (hereinafter referred to as – the Civil Code)[3] and developed in the practice of the Supreme Court of Lithuania[4]:

I. the information should be secret. This means that information which could be treated as trade secrets should not be new, unique (unlike other industrial property objects, such as patents, designs and other), but trade secrets must not be disclosed publicly;
II. the information should have commercial value. The information should create commercial value, financial benefit for the entity against other participants of the market (given the fact that other participants of the market do not know such information);
III. the owner of the information protects the secrecy of the information. This means that the holder of trade secrets should make reasonable efforts to protect trade secrets. These reasonable efforts could be of a legal nature (recognition of information as a secret, making confidentiality obligations in various settlement agreements and others) and of a factual nature (limiting access to information in company and taking other actions to secure information).

Secondly, the Art 1.116 of the Civil Code not only provides the criteria of trade secret, but also grants a certain protection related to disclosure and use of trade secrets. Art. 1.116(4) of the Civil Code establishes that persons who unlawfully disclosed, acquired and (or) used trade secrets shall be bound to compensate for the damages caused to the holder of trade secrets. Though, legal protection of trade secrets and civil liability for unlawful actions related to trade secrets are granted not only by the Art 1.116(4) of the Civil Code, but also by prohibition of unfair competition provided in international and national legal regulation.

The provisions related to prohibition of unfair competition on the international level are provided in the Art. 10bis of the Paris Convention for the Protection of Industrial Property[5], adopted in 1883, as well as the Model provisions on protection against unfair competition[6] developed and published by the World Intellectual Property Organization in 1996.

Prohibition of unfair competition is also included in the Art. 15(1) of the Law on Competition of the Republic of Lithuania[7] (hereinafter referred to as - the Law on Competition) where 7 groups of prohibited actions are listed out. One of the group of prohibited actions are focused on the protection of trade secrets. In the Art 15(1) of the Law on Competition it is prohibited to use, transfer, disclose of information representing a trade secret of another undertaking without its consent as well as obtaining of such information from persons having no right to transfer such information, in order to compete, seeking self-benefit or inflicting damage on that undertaking. Moreover, the Law on Competition provides remedies if the aforementioned prohibition was violated. In accordance with the Art 16 (1) of the Law on Competition,

[3] Civil code of the Republic of Lithuania (Valstybės žinios 2000, No. 74-2262).
[4] Decision of the Supreme court of Lithuania, Case No. 3K-3-676/2013 [2013]; Decision of the Supreme court of Lithuania, Case No. 3K-3-447/2014 [2014]; Decision of the Supreme court of Lithuania, Case No. 3K-3-524/2014 [2014]; Decision of the Supreme court of Lithuania, Case No. 3K-3-421-695/2015 [2015]; Decision of the Supreme court of Lithuania, Case No. 3K-7-6-706/2016 [2016].
[5] Paris Convention for the Protection of Industrial Property (Valstybės žinios, 1996, No. 75-1796).
[6] World Intellectual Property Organization. 'Model provisions on protection against unfair competition' (Publication of the World Intellectual Property Organization, 1996, No. 832).
[7] Law on Competition of the Republic of Lithuania (Valstybės žinios, 1999, No. 30-856).

the undertaking whose legitimate interests were violated by actions of unfair competition is entitled to bring a claim before the court seeking included, but not limited (i) to terminate the illegal actions; (ii) to compensate damages caused by illegal actions.

2. The influence of digitalization to legal protection of trade secrets and to prohibition of unfair competition actions

Fast paced development and use of information technologies, as a part of cross-cutting digitalization process, increasingly influences not only our daily life, business, but also all fields of law (civil law, intellectual property law, criminal law, procedural law and etc.). We should admit that protection of trade secrets is being influenced by digitalization as well.

It could be distinguished the following aspects regarding the influence of development and use of information technologies to legal protection of trade secrets and to prohibition of unfair competition actions upon unlawful disclosure and (or) use of trade secrets.

First of all, business is increasingly more orientated in e-commerce. Sale of goods and (or) provision of services is now heavily dependent on information and communication technology. In the digital economy, access to data has become increasingly important for the companies in order to compete[8]. The increased use of information technologies in business determines that nowadays most of the information (including knowledge and valuable proprietary information) is stored and accessible as electronic data. Especially in these cases when business models are internet-based. Even documents could be signed using e-signatures, most of communication is made via e-mails or using other digital communication channels. This means that today even physical copies of documents may be non-existing.

The fact that information is stored and accessible as electronic data, means that trade secrets are exposed to misappropriation to a larger extent. Large quantities of documents or data (that could be treated as trade secrets) can be easily copied, downloaded and (or) transferred without making much effort and very fast. This means that trade secrets are increasingly more open to hacking attacks from the outside. Moreover, trade secrets could be easier misappropriated by employees and (or) business partners.

Thus, digitalization process results in an increased risk for the protection of trade secrets because it becomes easier to disclose trade secrets and (or) to commit unfair competition actions.

Secondly, an increased use of information technologies determines that business is becoming more global and trade secrets could be used not only in the state where the holder of trade secrets has it's domicile, but in other state(s). Respectively, unlawful disclosure of trade secrets and (or) unfair competition actions could cross the borders of one state. In the light of possible global nature of such violations, there could be faced these legal difficulties related to protection of trade secrets:

I. due to digitalization and globalization it may be difficult to establish an infringement and (or) to identify persons who committed a violation;
II. legal protection of trade secrets may differ in particular countries. For example, in one state information could be considered as trade secrets, however in another state the same information may be not protected as trade secrets. Such a weak cross-border protection of trade secrets may restrict innovation and unreasonably increase business' costs in order to secure certain information. This is duly evidenced by the Internal Market Survey[9] that was commissioned by European Union. A large share of the survey respondents reported that, when trading in more than one European Union country, they apply different trade secrets protection measures depending on the country in question. According to the survey, 40% of EU companies would refrain from sharing trade secrets with other parties

[8] G. Surblytė. 'Data Mobility at the Intersection of Data, Trade Secret Protection and the Mobility of Employees in the Digital Economy' [2016] Max Planck Institute for Innovation and Competition Research Paper No. 16-03.

[9] 'Study on Trade Secrets and Confidential Business Information in the Internal Market' http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf.

because of fear of losing the confidentiality of the information through misuse or release without their authorisation[10];

III. forms of misappropriation of trade secrets may differ in particular countries, i. e. in one state actions performed with trade secrets could be recognized as violation, however in another state the same actions could be considered as legal.

Thirdly, today more and more information is stored using cloud-based services, that offer business the ability to store and access information remotely via the Internet. This gives the ability to quickly and easily access stored information and to make available or "share" that information with multiple individuals both inside and outside a business. However, this means placing actual or potential trade secrets in the hands of a third-party: the cloud computing service.[11]

On the one hand, using cloud-based services for storage of trade secrets increases the threat to the secrecy of trade secrets. It is easier for third persons to access to trade secrets. On the other hand, using cloud-based services rises certain legal issues. For example, where the server is located in one or more off-shore jurisdictions, what law will govern access to the data stored on the server (and how do you know where your data is really located)?[12] Moreover, does the cloud-based services provider assumes the obligation to protect stored information or data as trade secrets? These questions are extremely important not only for protection of information itself, but also due to the reason that one of the criteria for information or data to be considered as trade secrets is reasonable efforts of the holder of trade secrets to protect such information.

Finally, development and use of information technologies makes it easier to collect and process information from the publicly available sources, which then could be used for business development. Such collected and processed information (despite the fact that certain parts of this information could be found in publicly available digital sources) could be treated as trade secrets. For example, collected and processed statistical information about past prices in certain public procurements. In this regard, two or more independent entities may collect and process information in the same way, i. e. two or more independent entities may create same trade secrets. In such cases it might be unclear, which entity should be entitled the protection of trade secrets.

3. Does new European Union regulation on the protection of trade secrets cover main challenges of digitalization

On 8 June 2016 it was adopted new European Union regulation on protection of trade secrets, i. e. directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (hereinafter referred to as – the Directive). Member States has to implement the Directive by 9 June 2018. Taking this into account, particular legal regulation should be changed. It is intended to change certain articles of the Civil Code of the Republic of Lithuania and of the Civil Procedure Code of the Republic of Lithuania[13]. Moreover, it is proposed to adopt new legislation – the Law on legal protection of trade secrets of the Republic of Lithuania[14].

The preamble of the Directive confirms that new European Union regulation was adopted *inter alia* taking into account that (i) recent developments, such as globalisation, increased outsourcing and the increased use of information and communication technology contribute to increasing the risk of dishonest practices aimed at misappropriating trade secrets; (ii) there are important differences in the Member States' legislation as regards the protection of trade secrets against their unlawful acquisition, use or disclosure by other persons; (iii) it is appropriate to provide for rules at Union level to approximate the

[10] 'Study on Trade Secrets and Confidential Business Information in the Internal Market' http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf.

[11] S. K. Sandeen. 'Lost in the Cloud: Information Flows and the Implications of Cloud Computing for Trade' [2014] Virginia Journal of Law and Technology, Vol. 19.

[12] H. K. Lidstone. 'Using the Cloud: Trade Secrets and Confidential Information Aren't So Secret' [2013], https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2358472.

[13] Civil Procedure Code of the Republic of Lithuania (Valstybės žinios 2002, No. 36-1340).

[14] Government of the Republic of Lithuania. 11 October 2017 Resolution No. 823 (TAR, No. 16270).

laws of the Member States so as to ensure that there is a sufficient and consistent level of civil redress in the internal market in the event of unlawful acquisition, use or disclosure of a trade secret.

Aforementioned provisions of the preamble and regulation of the Directive confirms that the main aim of European Union regulation is to define a standardised level of trade secrets protection for European Union internal market by setting minimum standard for protection to trade secrets. For example, Art. 2 of the Directive establishes four elements of a trade secret; a trade secret should meet the following criteria: (i) it should be information; (ii) the information should be secret; (iii) the information should have commercial value due to secrecy; (iv) the holder of the information should take measures to keep it secret. The aforementioned trade secret definition is derived from the Agreement on Trade-Related Aspects of Intellectual Property Rights[15].

Moreover, regulation of the Directive defines (i) harmonised remedies to the holder of trade secrets after unauthorised use of trade secrets, (ii) harmonised measures in litigation to prevent the leak of trade secrets during civil proceedings.

Given the aforementioned, new European Union regulation covers the second challenge (indicated in the 2nd part of this paper) which is related to the influence of digitalization and globalization to the protection of trade secrets. I. e. the Directive eliminates the differences in Member States' legislation as regards the protection of trade secrets against their unlawful acquisition, use or disclosure.

It should be noted that in accordance with the Art 3 (a) of the Directive the acquisition of a trade secret shall be considered lawful when the trade secret is obtained by independent discovery or creation. This means that provisions of the Directive should not create any exclusive rights to trade secrets if the independent discovery of the same information was made. This regulation of the Directive covers the fourth challenge related to the cases when two or more independent entities create same trade secrets.

While in terms of the first and the third challenges (indicated in the 2nd part of this paper), we should admit that the holder of trade secrets himself has to take factual and legal measures to cover these challenges related to secrecy of trade secrets. For example, the holder of trade secrets could make technical restrictions to information and enter into confidentiality agreements with cloud-based services provider.

Conclusions

Development and use of information technologies makes negative influence to the legal protection of trade secrets. It could be distinguished the following aspects related to digitalization's influence to the protection of trade secrets: (i) digitalization process results in an increased risk for the protection of trade secrets because it becomes easier to disclose trade secrets and (or) to commit unfair competition actions; (ii) different trade secrets protection measures, depending on the country in question, lead to refrainment from sharing trade secrets with business partners or from expanding business in other countries; (iii) using cloud-based services for storage of trade secrets rises important legal issues related to protection of trade secrets; (iv) development and use of information technologies makes it easier to independently discover, create the information considered as trade secrets.

New European Union regulation on the protection of trade secrets provides guidelines for Member States' legal regulation, which should cover reasonable part of the aforementioned challenges of digitalization's influence to the protection of trade secrets. However, provisions of the Directive do not provide solutions to all problems in relation to the protection of trade secrets. Therefore, the holder of trade secrets must make efforts by applying technical and legal measures for proper protection of trade secrets.

Bibliography

Books, articles

[15] World Trade Organisation, 'The Agreement on Trade-Related Aspects of Intellectual Property Rights'.

1. H. K. Lidstone, 'Using the Cloud: Trade Secrets and Confidential Information Aren't So Secret' [2013], https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2358472.
2. S. K. Sandeen. 'Lost in the Cloud: Information Flows and the Implications of Cloud Computing for Trade' [2014] Virginia Journal of Law and Technology, Vol. 19.
3. G. Surblytė. 'Data Mobility at the Intersection of Data, Trade Secret Protection and the Mobility of Employees in the Digital Economy' [2016] Max Planck Institute for Innovation and Competition Research Paper No. 16-03.

Legislation

1. Civil code of the Republic of Lithuania (Valstybės žinios 2000, No. 74-2262).
2. Civil Procedure Code of the Republic of Lithuania (Valstybės žinios 2002, No. 36-1340).
3. European Parliament and of Council Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L 157.
4. Government of the Republic of Lithuania. 11 October 2017 Resolution No. 823 (TAR, No. 16270).
5. Law on Competition of the Republic of Lithuania (Valstybės žinios, 1999, No. 30-856).
6. Paris Convention for the Protection of Industrial Property (Valstybės žinios, 1996, No. 75-1796).
7. World Intellectual Property Organization. 'Model provisions on protection against unfair competition' (Publication of the World Intellectual Property Organization, 1996, No. 832).
8. World Trade Organisation. 'The Agreement on Trade-Related Aspects of Intellectual Property Rights'.

Cases

1. Decision of the Supreme court of Lithuania, Case No. 3K-3-421-695/2015 [2015];
2. Decision of the Supreme court of Lithuania, Case No. 3K-3-447/2014 [2014];
3. Decision of the Supreme court of Lithuania, Case No. 3K-3-524/2014 [2014];
4. Decision of the Supreme court of Lithuania, Case No. 3K-3-676/2013 [2013];
5. Decision of the Supreme court of Lithuania, Case No. 3K-7-6-706/2016 [2016];

Other sources:

1. 'Study on Trade Secrets and Confidential Business Information in the Internal Market' http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf.

A "EUROPEAN" APPROACH TOWARDS DIGITAL ECONOMY: SOME RECENT TAX LAW DEVELOPMENTS

Liotta Alessandro[1]

Abstract

The aim of this paper is to identify the solutions proposed by the EU Commission to tackle the hideous problems deriving from the (mis)use of digital technologies in the MNEs structures. First, the proposed paper will attempt to give a quick overview of OECD BEPS Action Plan, focusing on Action 1 and, consequently, on the position adopted by the EU Commission on the digital economy. Secondly, the paper will give a glimpse at the short-term solutions initially proposed by the Commission, and then it will focus on the interim solution that has eventually been elaborated by the Commission. In addition, it will give a critical point of view regarding the questionable approach of the EU Commission towards these direct tax issues emerging from the digital economy and the use of legislative power in a context where it is debated whether the EU has competence. This is also a good occasion to evaluate the relationship between competition law issues and the power of the Commission to protect and enforce the internal market on the one hand, and the tax sovereignty of the Member States on the other hand. The interim solution will also be evaluated in respect to its compliance with the fundamental freedoms and the EU State aid legislation as set forth by Article 107 TFEU. Finally, the paper will briefly point out the main aspects of the long-term measure, which sets forth provisions regarding the virtual permanent establishment.

Keywords: Tax Digital Economy EU competition

Introduction

The publication of the Final Reports of the 2015 BEPS (Base Erosion and Profit Shifting) Action Plan allowed the OECD to identify the most serious and urgent tax issues its Member States were required to tackle, given the technological development the world has faced in the last years. More specifically, Action 1 of the above-mentioned project, entitled "Addressing the Tax Challenges of the Digital Economy" dealt with the various shapes aggressive tax planning could take thanks to digital platforms[1].

The European Institutions, inspired by the work carried out by the OECD, have felt the urge to stop phenomena of tax avoidance that often characterizes the business models of the MNEs that make use of intangibles. If, on the one hand, the EU has recognised the necessity to intervene rapidly as a community, rather than waiting for the governments of the Member States to adopt the needed measures, on the other hand it has realized that it is impossible to deal with the problem at issue in short term.

Or, better yet, to give an effective response to the problem in short terms.

[1] *Master of Laws at Università degli Studi di Palermo, LL.M. in International Tax Law at King's College London, PhD candidate in "Law and Business", LUISS Guido Carli (Rome), Faculty of Law, with a dissertation in Tax Law on the application of CFC legislation to IP Holding Companies. Visiting Researcher at UNIL (Université de Lausanne), from October 2017 to December 2017 and currently Visiting Scholar at UC Berkeley, Boalt Hall Law School. Main interests: Tax Law, both from a domestic and an international perspective, and EU Law issues, especially those related to Tax Law. Email address: aliotta@luiss.it*

[1] As it was underlined by the Final Report of the BEPS Action Plan 1, p. 82, for what concerns VAT, […] "under certain conditions opportunities for tax planning by businesses and corresponding BEPS concerns for governments in relation to VAT may arise with respect to (i) remote digital supplies to exempt businesses and (ii) remote digital supplies acquired by enterprises that have establishments (branches) in more than one jurisdiction (MLE) that are engaged in exempt activities". Conversely, with reference to direct taxes, the BEPS Action Plan 1, p. 78 highlighted profit splitting could occur in four different ways: "1. Minimisation of taxation in the market country by avoiding a taxable presence, or in the case of a taxable presence, either by shifting gross profits via trading structures or by reducing net profit by maximising deductions at the level of the payer; 2. Low or no withholding tax at source; 3. Low or no taxation at the level of the recipient (which can be achieved via low-tax jurisdictions, preferential regimes, or hybrid mismatch arrangements) with entitlement to substantial non-routine profits often built-up via intra-group arrangements; 4. No current taxation of the low-tax profits at the level of the ultimate parent".

In this respect, the European Commission has identified some short-term measures, which should give a first, albeit not definitive answer to the tax issues, and which are going to be followed by other long-term measures.

1. BEPS Action Plan 1 and the objectives of the EU initiatives

The OECD BEPS Action Plan Final Reports, issued in late 2015, describe and deepen the hideous phenomenon known as profit splitting, which represents a priority concern for the Tax Administrations of the OECD Member States, as it allows MNEs to divert their profits to low tax jurisdictions, to lower their tax base in the high tax jurisdictions where they have subsidies or P.E., this resulting in a consistent loss of revenue for the OECD Member States. Most of these Actions somehow deal with the challenges arising from the use (or the misuse) of intangibles and digital economy[2] and struggle to find solutions that can reconcile the necessity to tax certain types of revenue[3] with the needs of those enterprises that are involved in the production or distribution of digital goods and/or services.

Given the importance of the problem, the EU Commission invited the other European Institutions to introduce a legislative framework known as "Fair and Efficient Tax System in the European Union for the Digital Single Market".

On September 21st, 2017, the Commission sent a Communication to the Parliament and the Council[4], claiming the necessity to understand and provide solutions for the distortive effect that aggressive tax planning of certain MNEs in the context of digital economy might have in the common market. According to the Commission, "the Digital Single Market (DSM) is one of the 10 political priorities of the European Commission. The DSM strategy aims to open up digital opportunities for people and businesses in a market of over 500 million EU consumers. Completing the Digital Single Market could contribute to EUR 415 billion per year to Europe's economy, create jobs and transform our public services". This was followed by the conclusions adopted on October 19th, 2017[5].

On December 5th, 2017, the ECOFIN Council[6] looked forward to appropriate Commission proposals by early 2018, taking into account relevant developments in the ongoing discussions at the OECD. Eventually, on March 21st, 2018, the Commission published two proposals, which are supposed to introduce an interim solution[7] and a long-term solution[8], and two respective Communications, as well as an Impact Assessment Report.

Even though the EU Institutions push hard and encourage the adoption of the required measures, they are aware of the difficulties and that it is not possible to introduce effective fast and long-lasting tax tools in a short period of time. Consequently, the strategy the EU has decided to carry on implies the introduction of an interim-solution[9] (the digital services tax Directive Proposal), as part of a huge and far more complex plan.

---

[2] The Action Plans at issue are designed to counter tax avoidance and tax evasion at an international level and should be read as part of a general and more complex plan. They are meant to introduce different suggestions and solutions to certain tax problems, which might also be overlapping. This might be the case of Action 3 (Designing Controlled Foreign Company Rules), or Action 6 (Prevent Treaty Abuse), or even Action 7 (Prevent the Artificial Avoidance of PE Status). Whereas others were tailored around the concept of intangible, and might address more specific issues, such as Action 5 (Counter Harmful Tax Practices More Effectively) and Action 8-10 (Aligning Transfer Pricing Outcomes with Value Creation). It is indeed interesting that Action 1, despite its very specific target, attracts and sums up some aspects of each of the above-mentioned Actions. In this respect, see P. Saint-Amans and R. Russo, 'The BEPS Package: Promise Kept, in Bulletin for International Taxation' [2016] IBFD, p. 236.

[3] As frequently underlined by the EU Commission, there are weaknesses in the international tax rules as they were originally designed in the 1920s for "brick and mortar" businesses and have now become outdated. In particular, this has led to a misalignment of the place where value is created, notably in the case of user contributions, and the allocation of the taxing rights and ability to enforce taxation.

[4] Proposal for a Council Directive COM (2017) 547.

[5] European Council meeting – Conclusions EUCO 14/27.

[6] ECOFIN Council conclusion, "A" Item note 15175/17.

[7] Proposal for a Council Directive COM (2018) 148: Proposal for a Council Directive on the common system of a digital services tax on revenues resulting from the provision of certain digital services.

[8] Proposal for a Council Directive COM (2018) 147: Proposal for a Council Directive laying down rules relating to the corporate taxation of a significant digital presence.

[9] Conversely, Action Plan 1 of the BEPS Project criticizes the adoption of interim-solutions. The Final Report of Action Plan 1 states that "[…] none of the other three options analysed by the TFDE [(Tax Force on the Digital Economy)] were recommended at this stage. This is because, among other reasons, it is expected that the measures developed in the BEPS Project will have a substantial impact on BEPS issues

In fact, alongside with these proposals, the Commission has already launched the CCCTB (Common Consolidated Corporate Tax Base)[10] and a new VAT Directive on e-commerce[11] has been recently approved by the Council[12]. These pieces of legislation are meant to be the pillars of a new tax system that, as far as the Commission is concerned, should prevent, or contribute to considerably reduce, the level of tax avoidance within the internal market and, thus, could create a level playing field.

2. The short-term solution

The above-mentioned Directive Proposal on the digital service tax (DST) is not the first solution elaborated by Commission to tackle the tax issues arising from digital economy, as on September 21st, 2017, it proposed three alternative measures, such as an equalisation levy on the turnover of digital companies, a withholding tax on digital transactions and a levy on revenues generated from the provision of digital services or advertising activities.

Even though the Commission has not reproduced these solutions, it might be interesting to summarize the main aspects of such measures.

While the equalisation levy was meant to tax the turnover of digital companies, that is to say the gross revenue of those entrepreneurial (either B2B or B2C) activities carried out on the internet[13], the withholding tax on digital transactions was supposed to be applied as a global withholding tax on all the payments made to non-resident subjects[14], and the levy on revenues generated from the provision of digital services was conceived to take into consideration, for tax purposes, all the transactions carried out remotely in case the providing company were to have a significant economic presence in the country where the service is provided.

What the Commission ended up with is a Directive proposal, the scope of which is "to put forward a measure that targets the revenues stemming from the supply of certain digital services and that is easy to implement and helps to level the playing field in the interim period until a comprehensive solution is in place"[15]. The Commission points out that the introduction of the Digital Services Tax (DST) is in line with the general objectives of the proposal, whose aim is: to protect the integrity of the Single Market and to ensure its proper functioning; to make sure that the public finances within the Union are sustainable and that the national tax bases are not eroded; to ensure that social fairness is preserved and that there is a level playing field for all businesses operating in the Union and; to fight against aggressive tax planning

previously identified in the digital economy, that certain BEPS measures will mitigate some aspects of the broader tax challenges, and that consumption taxes will be levied effectively in the market country".

[10] Proposal for a Council Directive COM (2016) 683.

[11] Proposal for a Council Directive COM (2016) 757.

[12] Some commentators have underlined that, despite the action of the whole EU and of its Institutions could improve the cohesion and the harmonization of the internal market, this would essentially keep the international scenario unchanged. Consequently, a global approach would be recommended. According to M. F. De Wilde, 'Taxation of Multinational Enterprises in a Global Market: Moving to Corporate Tax 2.0?', in Bulletin for International Taxation [2016] IBFD, p. 182, "the OECD/G20's package addresses the various issues through a series of specific action points; however, it leaves the existing international corporate taxation framework essentially intact. The same is basically true for the approaches currently being taken within an EU context (at least at present), given that the Commission has recognized the need for a long-term solution for the European Union in its proposals for the Common Consolidated Corporate Tax Base (CCCTB). Although the long-term EU solutions envisaged take matters a step further than the OECD (G20 has done, at least analytically , any EU-wide solution, regardless of its merits, will be subject to geographical limitations that would allow base erosion and profit shifting issues to continue to arise beyond the water's edge, i.e. in respect of economic activities beyond the European Union's outer geographical borders".

[13] The equalisation levy has already been adopted in India, where it is applied at a 6% tax rate on the commissions paid by resident enterprises to non-resident subjects for online advertising services worth more than 1'500 US Dollars (100'000 Indian Rupees) during the tax year. To deepen the Indian equalisation levy, see, *ex multis*, S. Basak, 'Equalisation Levy: A New Perspective of E-commerce Taxation' in Intertax, Volume 44, p. 845; S. Varansi and M. Nagappan, 'Financial Budget for 2016-2017: Has India put Its BEPS Foot Forward?' in Intertax, Volume 44, p. 550; M. K. Singh, 'Taxation of Digital Economy: And Indian Perspective' in Intertax, Volume 45, p. 467.

[14] This type of tax was encouraged by part of the commentators. More in details, Y. Brauner and P. Pistone, 'Adapting Current International Taxation to New Business Models: Two Proposals for the European Union, in Bulletin for International Taxation' [2017] IBFD, claimed that "the withholding tax solution would be a flexible, immediate solution to the most acute challenges of the digital economy. It is a solution that would avoid critical technical problems and would work in the direction of better cooperation between states to arrive at collaborative solutions, even if, at present, such a solution has not yet presented itself. It could also become an implementation mechanism for a virtual PE solution, of one were to be agreed on by a sufficient number of the Member States".

[15] Proposal for a Council Directive COM (2018) 148, p. 3.

and to close the gaps that currently exist in the international rules which makes it possible for some digital companies to escape taxation in countries where they operate and create value.

Preliminarily, it is worth noticing that the Commission puts the stress on the competition issues deriving from nowadays digitalized economy and considers tax measures as tools to create a homogeneous and – as far as possible – harmonized market.

If, on the one hand, this competition-oriented approach can be appreciated, since it represents the essence of the activity of the Commission and, more broadly, of the EU in general, it might be claimed that the introduction of pieces of legislation that limit the legislative power of the Member States in tax matters could be beyond the competence of the EU, even though according to the Commission, the Directive proposal is based on Article 113 of the TFEU[16]. This provision enables the EU Institutions, with a special legislative procedure, to adopt provisions for the harmonisation of Member States' legislation concerning other forms of indirect taxation to the extent that such harmonisation is necessary to ensure the establishment and the functioning of the internal market and to avoid distortion of competition. The Commission states that an action at EU level is needed in order to mitigate the fragmentation of the internal market and the creation of distortions of competition within the Union due to the adoption of divergent unilateral actions at national level.

After this brief introduction regarding the legislative technique and procedure chosen by the EU to adopt this piece of legislation, it is necessary now to summarize the key elements of the Directive proposal that should introduce an interim solution to the problems at issue.

In a nutshell, the Digital Service Tax is going to levy on revenues from the supply of certain digital services, as defined and qualified by Article 3 of the proposed Directive[17]. Taxable revenues should be those resulting from the provision of the following services: (i) the placing on a digital interface of advertising targeted at users of that interface; (ii) the making of multi-sided digital interfaces which allow users to find other users and to interact with them, and which may also facilitate the provision of underlying supplies of goods or services directly between users (sometimes referred to as "intermediation" services); and (iii) the transmission of data collected about users and generated from such users' activities on digital interfaces. Consequently, if no revenues are obtained from the supply of such services, there should be no DST liability. Article 3, paragraph 3, specifies that point (i) shall apply whether or not the digital interface is owned by the entity responsible for placing the advertising on it and that where the entity placing the advertising does not own the digital interface, that entity, and not the owner of the interface, shall be considered to be providing a service falling within point (i), whereas paragraph 4 underlines that point (ii) shall not include: a) the making available of a digital interface where the sole or main purpose of making the interface available is for the entity making it available to supply digital content to users or to supply communication services to users or to supply payment services to users; b) the supply by a trading venue or a systematic internaliser of some services referred to in Annex I to Directive 2014/65/EU; (c) the supply

[16] Even if the Commission promotes a supranational strategy to rule and regulate the phenomenon of digital economy, especially given its concerns related to the protection of competition within the internal market, commentators have stated that the EU should not have a "full legislative power", at least in the direct taxes field. In this respect, see H. Panayi, 'The Compatibility of the OECD/G20 Base Erosion and Profit Shifting Proposals with EU Law' in Bulletin for International Taxation [2016] IBFD, p. 95, who claims that "[…] the European Union cannot interfere with how a Member State exercises its taxing rights with regard to other countries". The legal basis of the Directive proposal COM(2018)147 (which will be analysed in the following paragraph) is Article 115 TFEU, which j provides for the Council, acting unanimously in accordance with a special legislative procedure and after consulting the European Parliament and the Economic and Social Committee, to issue directives for the approximation of such laws, regulations or administrative provisions of the Member States as directly affect the establishment or functioning of the internal market. This provision is commonly used by the EU where taxes other than indirect taxes are involved. Furthermore, the EU may introduce tax law provisions according to Article 352 TFEU, which requires the Council, acting unanimously on a proposal from the Commission and after obtaining the consent of the European Parliament, to take appropriate measures to attain one of the objectives set out in the Treaties if those Treaties have not provided the necessary powers.

[17] According to Article 3, "the services falling within the scope of DST are those where the participation of a user in a digital activity constitutes an essential input for the business carrying out that activity and which enable that business to obtain revenues therefrom. […] These services can be provided remotely, without the provider of the services necessarily being physically established in the jurisdiction where the users are and value is created. Therefore, such businesses models are responsible for the greatest difference between where profits are taxed and where value is created. However, what is subject to taxation are the revenues obtained from the monetisation of the user input, not the user participation in itself". User participation can contribute to the value of a business in various ways. For example, digital businesses can derive data about users' activities on digital interfaces, which is typically used to target advertising at such users, or which can be transmitted to third parties for consideration. Another way is through the active and sustained engagement of users in multi-sided digital interfaces, which build on network effects where, broadly speaking, the value of the service increases with the number of users using the interface.

by regulated crowdfunding service provider of any of the services referred to in Annex I to Directive 2014/65/EU, or a service consisting in the facilitation of the granting of loans. Point (iii) shall not include the transmission of data by a trading venue, systematic internaliser or regulated crowdfunding service provider.

Article 4 establishes when a subject might be deemed a taxable person in the context of the DST and it sets forth the following conditions: (i) the total amount of worldwide revenues reported by the entity for the relevant financial year exceeds EUR 750.000.000; (ii) the total amount of taxable revenues obtained by the entity within the Union during the relevant financial year exceeds EUR 50.000.000.

Article 5 identifies the place of taxation by determining which proportion of the taxable revenues obtained by an entity has to be treated as obtained in a Member State for the purposes of this tax. In other words, it establishes that DST is due in the Member State or Member States where the users are located[18]. Paragraph 2 provides that "with respect to a taxable service: a user shall be deemed to be located in a Member State in a tax period if: (a) in the case of a service falling within Article 3(1)(a), the advertising in question appears on the user's device at a time when the device is being used in that Member State in that tax period to access a digital interface; (b) in the case of a service falling within Article 3(1)(b): (i) if the service involves a multi-sided digital interface that facilitates the provision of underlying supplies of goods or services directly between users, the user uses a device in that Member State in that tax period to access the digital interface and concludes an underlying transaction on that interface in that tax period; (ii) if the service involves a multi-sided digital interface of a kind not covered by point (i), the user has an account for all or part of that tax period allowing the user to access the digital interface and that account was opened using a device in that Member State; (c) in the case of a service falling within Article 3(1)(c), data generated from the user having used a device in that Member State to access a digital interface, whether during that tax period or any previous one, is transmitted in that tax period. Paragraph 3, then describes the ways the proportion of an entity's total taxable revenues that is treated under paragraph 1 as obtained in a Member State shall be determined. The DST tax rate shall be 3% (Article 8).

After having mentioned the key points of the Digital Services Tax, it is possible to address some of the most interesting and controversial aspects of the EU action in the area of tax law.

As it appears from the current situation, the EU Institutions seem to have realized that the internal market issues and the problems deriving from the coexistence of 28 law systems often involve tax law, and they have started to introduce pieces of legislation that certainly limit the power of the Member States to shape their tax systems the way they prefer.

What the EU is undoubtedly doing is using tax law as a tool to protect the internal market and to prevent the companies from distorting the market by exploiting the different legislations of the Member States. While the solutions initially proposed by the Commission could be claimed to be incompatible with certain fundamental principles of EU Law like, for example, the freedom of establishment, as set forth by Article 49 of the TFEU[19], the interim-solution eventually chosen seems to be compliant with this fundamental freedom, as it is supposed to be applied in the whole territory of the EU. In fact, the EU Institutions believe the introduction of a sole tax, adopted by all the Member States would not lead to any

[18] According to the Directive Proposal, "The taxable revenues resulting from the provision of a taxable service have to be treated for the purposes of this Directive as obtained in a Member State in a tax period if a user with respect to such services is deemed to be located in that Member State in that tax period according to the rules in Article 5(2), which have to be applied for each type of taxable service. In the case of users involved in a taxable service which are located in different Member States or non-Union jurisdictions, the taxable revenues obtained by an entity from the provision of that service would have to be distributed to each Member State proportionally and according to the several allocation keys laid down in Article 5(3) for each type of taxable service. Such allocation keys have been set out taking into account the nature of each of the taxable services and, in particular, what triggers the receipt of revenues for the provider of the service. In the case of a taxable service consisting in the placing of advertising on a digital interface, the number of times an advertisement tax has appeared on users' devices in a tax period in a Member State is taken into account for the purposes of determining the proportion of revenues to be allocated in that tax period to that Member State".

[19] The compatibility of the tax tools used by the Member States with the freedom of establishment has been subject to the attention of the ECJ in various judgment. See, *ex multis*, Case C-446/04 FII GLO; Case C-35/11 Test Claimants FII; Case C-492/04 Lasertec; Case C-251/98 Baars; Case C-436/00 X e Y; Case C-264/96 ICI; Case C-446/03 Marks & Spencer; Case C-337/08 X Holding; Case C-18/11 Philips Electronics; Case C-231/05 OY AA; Caso-250/95 Futura Participations Singer; Case C-293/06 Deutsche Shell; Case C-414/06 Lidl Belgium.

violation of the EU principles, whereas if the Member States were allowed to design their own tax, this could interfere with the aforementioned principles[20].

It might be argued that the DST is not compatible with Article 107 TFEU and the EU State aid principles. One of the conditions that needs to be fulfilled according to Article 107 TFEU is selectivity[21]. It could be said that the adoption of the proposed Directive could lead to a distortion of competition under the paradigm of EU State aid law where the transactions taxed according to the proposed Directive were deemed to be comparable with those operations that have the same content (e.g. advertising) but are not carried out digitally. It is extremely hard to establish whether the DST, as applied and implemented by the Member States, could be considered a State aid.

However, also in the context of competition law, it is possible to point out the relation between the policy of the EU and the tax policies of the Member States[22].

Finally, the purpose of the DST is not only to prevent any distortion in the internal market, but also to tackle those episodes of tax avoidance that may take place in the context of digital economy. Article 6 of the Anti-Tax Avoidance Directive (ATAD)[23] allows a Member State to ignore an arrangement or a series of arrangements which, having been put into place for the main purpose or one of the main purposes of obtaining a tax advantage that defeats the object or purpose of the applicable tax law, are not genuine having regard to all relevant facts and circumstances. An arrangement may comprise more than one step or part. Since Article 6 is a general provision that establishes an important principle in the context of EU law, the DST Directive proposal must be read and applied accordingly, considering its anti-avoidance purpose.

3. The long-term solution: the key points

The second Directive proposal issued by the Commission regards the concept of permanent establishment and, more in details, the definition of significant digital presence, as suggested by the OECD. Although Action 7 of the BEPS Action Plan provides some solutions to the avoidance of the status

[20] Even if this type of approach is understandable in principle, it might be claimed that in many past cases, the ECJ did not recognize the taxing rights of the Member States as relevant reasons to restrict the application of the fundamental freedoms, even though the taxpayers had transferred their legal seats in low tax jurisdictions. In other words, the application of low tax rates was not conceived as a problem for the integrity of the internal market, whereas the ECJ tended to preserve the freedom of establishment. What seems to be happening nowadays is that the EU wants to preserve that freedom by introducing a tax, that is the same for all the Member States, and, simultaneously, wants to preserve the taxing rights of the Member States, not because they are considered a value themselves, but because they appear useful in the context of the internal market and in the perspective of a digitalized economy.

[21] About the concept of selectivity see, *ex multis*, A. Jones and B. Sufrin, 'EU Competition Law, Cases & Materials' (Oxford 2010), Fourth Edition, p. 1279. N. Phedon and I. E. Rusu, 'The Concept of Selectivity: an Ever Wider Scope' in European State Aid Law Quarterly [2012] p. 791; C. Quigley, 'General Taxation and State aid' in A. Biondi, P. Eeckhout and J. Flynn, 'The Law of State aid in the European Union' (Oxford) p. 207; G. M. Barbara, 'Advocate General Opinions on Tax Autonomy of European Region: from the Basque Country Case (1999) to the Gibraltar Case (2011)' in European Taxation [2012] p. 164; R. Schütze, 'European Law' (Cambridge 2015) p. 770; J. Temple Lang, 'The Gibraltar State Aid and Taxation Judgment – a "Methodological Revolution?"' in European State Aid Law Quarterly [2012] p. 805. The concept of geographical and material selectivity has been variously interpreted by the ECJ. See, *ex multis*, Case C – 256/97 DMTransport; Case T – 127/99, T – 129/99 e T – 148/99 Territorio Històrico de Alava – Diputaciòn Foral de Alava and others v Commission; Case C – 75/97 Belgium v Commission; Case C – 143/99 Adria-Wien Pipeline; Case T- 445/05 Associazione Italiana del Risparmio Gestito e Fineco Asset Management v Commission.

[22] See T. Lyons, 'The modernisation of EU state aid law and taxation' [2014] British Tax Review, p. 113. The Author states that "so far as EU law is concerned, it has for many years been clear that tax falls within the ambit of state-aid law". The problem of the role of States in the internal market (both players and regulators) has been highlighted by A. Kardachaki and M. Van Hulten, 'Report on the EUCOTAX Conference "State Aid, Intangibles and Rulings"' [2017] EC Tax Review p. 284. The Authors point out that "[…] the current debate illustrates that the EU fiscal State aid may have limits to its reach. States act both as regulator and as a market operator in tax matters, and those roles cannot be reconciled if we want to tackle competition between States. The current criteria to assess fiscal State aid are focused on competition between undertakings and the intervention of States in the internal market. But what if we try to define the actions of the State as an operator in the tax law market? Could we for instance interpret the advantage test better by thinking about the objectives of States? Given these complexities, political rather than legal solutions seem better suited to solve this problem".

[23] Council Directive 2016/1164/EU.

of permanent establishment[24], Action 1 deals with the digital permanent establishment more specifically[25]. In this respect, the Commission adopted the suggestion of the OECD and issued a Directive which is going to redefine the concept of permanent establishment.

Essentially, the proposal, after having identified its scope (Article 2) and having defined the various concepts for applying the provisions in the Directive (e.g. digital services, digital interface, revenues, entity, user and tax period) in Article 3, describes what significant digital presence in Article 4 and warns that it should be regarded as an addition to the existing permanent establishment concept, and enlists the profits attributable to the significant digital presence in Article 5.

According to Article 4, a permanent establishment shall be deemed to exist if a significant digital presence through which a business is wholly or partially carried on exists. Paragraph 3 provides that a SDP shall be considered to exist in a Member State in a tax period if the business carried on through it consists of digital services through a digital interface and one or more of the following conditions is met with respect to the supply of those services by the entity carrying on that business, taken together with the supply of any such services through a digital interface by each of that entity's associated enterprises in aggregate: (a) the proportion of total revenues obtained in that tax period and resulting from the supply of those digital services to users located in that Member State in that tax period exceeds EUR 7.000.000; (b) the number of users of one or more of those digital services who are located in that Member State in that tax period exceeds 100.000; (c) the number of business contracts for the supply of any such digital service that are concluded in that tax period by users located in that Member State exceeds 3.000. The provision establishes, thus, three different thresholds which allow to identify when a significant digital presence occurs and, consequently, if there is a (virtual) permanent establishment. Paragraph 4 underlines that a user shall be deemed to be located in a Member State in a tax period if the user uses a device in that Member State in that tax period to access the digital interface through which the digital services are supplied, while paragraph 7 establishes that the proportion of total revenues referred to in paragraph 3 (a) shall be determined in proportion to the number of times that devices are used in that tax period by users located anywhere in the world to access the digital interface through which the digital services are supplied.

Briefly, Article 5 states that the profits that are attributable to or in respect of a significant digital presence in a Member State shall be taxable within the corporate tax framework of that Member State only. While paragraph 2 identifies the type of profits attributable as those that the digital presence would have earned if it had been a separate and independent enterprise performing the same or similar activities under the same or similar conditions, taking into account the functions performed, assets used and risks

[24] Action 7 of the BEPS Action Plan addresses several issues, such as: the artificial avoidance of PE status by the use of commissionaire arrangements; the abuse of the "independent agent" exception in Article 5(6) of the OECD Model and instances in which such an agent could be closes related to the principal; the artificial avoidance of PE status by way of the specific activity exception in Article 5(4); the related concern with regard to enterprises misusing the exceptions in Article 5(4) by fragmenting activities; and the abuse of the exception in Article 5(3) by splitting of contracts.

[25] Action 1 basically identifies the importance of the digital economy and sets out its features and typical business models. It also raises the question of redefining the nexus for taxation in the source state and suggests, as a solution, the introduction of the significant economic presence (SEP) nexus. See B. Larking, 'A Review of Comments on the Tax Challenges of the Digital Economy, in Bulletin for International Taxation' [2018]: "Allocation of profits to a SEP is the next tricky issue and the OECD considers both the possibility of adapting traditional profit allocation principles […] as well as alternative methods such as formulary (fractional) apportionment or deemed profit-based methods". The Author believes the SEP would not work, as problems would arise regarding both threshold and profit allocation. Other commentators put the stress on the threshold. See Y. Brauner and P. Pistone, 'Adapting Current International Taxation to New Business Models: Two Proposals for the European Union': "[…] in order to avoid an excessive fragmentation of the taxable base, we envisage that the application of the virtual PE should take place along the lines of a *de minimis* threshold. This could operate with a similar function to that which a construction PE has in Article 5(3) of the OECD Model. With reference to an intervention on this topic at EU level, the Authors believe that "the introduction of a virtual PE concept into EU law would be a constructive step forward and an effective global action to bring international tax categories and concept back into line with the business models. It would also represent a friendly development in cooperation with the OECD, as it would essentially preserve the OECD PE standard and facilitate OECD action to realize a possible expansion of this solution at a later time. Finally, it would not prevent the European Union from applying this solution in a context of formulary apportionment, provided, of course, that the factors along which the formula applies were amended in a way that would take into account the different features of the new business models connected with the digital economy".

assumed, through a digital interface, paragraph 3 describes the way such profits are determined[26], and paragraph 5 enlists the economically significant activities.

Conclusions

The initiative of the EU is surely in line with the most recent international developments in the area of digital economy and is aimed at tackling the above-mentioned issues. The effort of the Commission is to be appreciated, because its purpose is to redefine corporate taxes under a European paradigm, in a homogeneous and complete framework (especially if we think about how these new proposals will interact with the CCCTB Directive proposal), in order to prevent distortive and abusive phenomena. It is still too early to evaluate if and how these proposals will manage to reach their objective in an effective and satisfactory way, but it is true that the aggressive action of the EU limits (maybe too much) the ability of the Member States to rule their own tax systems and it could represent a political issue with reference to the relationship between the EU and its Member States.

Bibliography

1. G. M. Barbara, 'Advocate General Opinions on Tax Autonomy of European Region: from the Basque Country Case (1999) to the Gibraltar Case (2011)' in European Taxation [2012].
2. S. Basak, 'Equalisation Levy: A New Perspective of E-commerce Taxation' in Intertax, Volume 44.
3. Y. Brauner and P. Pistone, 'Adapting Current International Taxation to New Business Models: Two Proposals for the European Union, in Bulletin for International Taxation' [2017] IBFD.
4. Case C – 143/99 Adria-Wien Pipeline.
5. Case C-18/11 Philips Electronics.
6. Case C-251/98 Baars.
7. Case C – 256/97 DMTransport.
8. Case C-264/96 IC.
9. Case C-293/06 Deutsche Shell.
10. Case C-337/08 X Holding.
11. Case C-35/11 Test Claimants FII.
12. Case C-414/06 Lidl Belgium.
13. Case C-436/00 X e Y.
14. Case C-446/03 Marks & Spencer.
15. Case C-446/04 FII GLO.
16. Case C-492/04 Lasertec.
17. Case C – 75/97 Belgium v Commission.
18. Case C-231/05 OY AA.
19. Case T – 127/99, T – 129/99 e T – 148/99 Territorio Històrico de Alava – Diputaciòn Foral de Alava and others v Commission.
20. Case T- 445/05 Associazione Italiana del Risparmio Gestito e Fineco Asset Management v Commission.
21. Caso-250/95 Futura Participations Singer.
22. Council Directive 2016/1164/EU.
23. ECOFIN Council conclusion, "A" Item note 15175/17.
24. European Council meeting – Conclusions EUCO 14/27.
25. A. Jones and B. Sufrin, 'EU Competition Law, Cases & Materials' (Oxford 2010), Fourth Edition.
26. A. Kardachaki and M. Van Hulten, 'Report on the EUCOTAX Conference "State Aid, Intangibles and Rulings"' [2017] EC Tax Review.
27. B. Larking, 'A Review of Comments on the Tax Challenges of the Digital Economy, in Bulletin for International Taxation' [2018].

[26] For the purposes of paragraph 2 the determination of profits attributable to or in respect of the significant digital presence shall be based on a functional analysis. In order to determine the functions of and attribute the economic ownership of assets and risks to, the significant digital presence, the economically significant activities performed by such presence through a digital interface shall be taken into account. For this purpose, activities undertaken by the enterprise through a digital interface related to data or users shall be considered economically significant activities of the significant digital presence which attribute risks and the economic ownership of assets to such presence.

28. T. Lyons, 'The modernisation of EU state aid law and taxation' [2014] British Tax Review.
29. OECD BEPS Action Plan 1 "Addressing the Tax Challenges of the Digital Economy" Final Report.
30. H. Panayi, 'The Compatibility of the OECD/G20 Base Erosion and Profit Shifting Proposals with EU Law' in Bulletin for International Taxation [2016] IBFD.
31. N. Phedon and I. E. Rusu, 'The Concept of Selectivity: an Ever Wider Scope' in European State Aid Law Quarterly [2012].
32. Proposal for a Council Directive COM (2016) 683.
33. Proposal for a Council Directive COM (2016) 757.
34. Proposal for a Council Directive COM (2017) 547.
35. Proposal for a Council Directive COM (2018) 148.
36. Proposal for a Council Directive COM (2018) 147.
37. C. Quigley, 'General Taxation and State aid' in A. Biondi, P. Eeckhout and J. Flynn, 'The Law of State aid in the European Union' (Oxford).
38. P. Saint-Amans and R. Russo, 'The BEPS Package: Promise Kept, in Bulletin for International Taxation' [2016] IBFD.
39. R. Schütze, 'European Law' (Cambridge 2015).
40. M. K. Singh, 'Taxation of Digital Economy: And Indian Perspective' in Intertax, Volume 45.
41. J. Temple Lang, 'The Gibraltar State Aid and Taxation Judgment – a "Methodological Revolution?"' in European State Aid Law Quarterly [2012].
42. S. Varansi and M. Nagappan, 'Financial Budget for 2016-2017: Has India put Its BEPS Foot Forward?' in Intertax, Volume 44.
43. M. F. De Wilde, 'Taxation of Multinational Enterprises in a Global Market: Moving to Corporate Tax 2.0?', in Bulletin for International Taxation [2016] IBFD.

DATA PROTECTION AS A COMPETITION CONCERN: CAN DATA PROTECTION VIOLATION AMOUNT TO ABUSE OF A DOMINANT POSITION?

Małobęcka Iga[1]

Abstract

The ongoing investigation against Facebook initiated by the Bundeskartellamt (German Federal Cartel Authority) shows that data protection infringements may also constitute a matter of concern for the competition authorities, particularly when committed by companies that exercise a dominant role on the markets.

The Bundeskartellamt is examining whether Facebook has abused its allegedly dominant position in the market for social networks by imposing unfair (exploitative) terms on its users. According to Bundeskartellamt's preliminary assessment dated December 2017, Facebook's policies, which presumably violate data protection provisions, could amount to exploitative abuse, i.e. a form of abuse of a dominant position prohibited by EU and national competition laws.

The Bundeskartellamt's investigation, raises important questions concerning the boundaries between the competition and data protection laws, as well as whether competition authorities are competent to tackle data protection violations.

On the one hand, even if Facebook's terms infringe data protection law, it can be questioned whether competition law is an adequate tool to remedy such violation. Critics argue that competition authorities lack appropriate expertise to assess such violations and that blurring the boundaries between the two separate fields of law that have different focus and serve different goals is unfounded.

On the other hand, if data are a fundamental factor in determining the dominance of a company, and serve as an essential input to its products or services, data protection and competition laws seem to intersect. In such cases, a dominant entity may find it profitable to infringe privacy laws to gain an advantage over its competitors.

Against this background, this paper analyses whether data protection violation should be considered as a concern for competition law, in particular whether it could amount to abuse of dominant position, and, if so, under which circumstances.

Keywords: Personal data, data protection, competition law, abuse of dominant position, online platforms.

Introduction

In recent years a lot of attention has been given to data protection concerns arising from the extensive collection, processing and commercial use of personal data in digital markets, especially by such data-driven companies[2] as Google or Facebook[3].

Processing of personal data by such companies has been under the spotlight of European data protection authorities in the European Union already for a while and resulted in a few high profile cases before the CJUE[4] and national data protection authorities[5].

---

[1] *PhD candidate at the Chair of European Law, Faculty of Law and Administration, University of Warsaw, graduated from Law at University of Warsaw and Law and Economics (LL.M.) at University of Utrecht. Author's research interests focus on the interplay between competition, data protection and IP law, as well as regulation of new technologies and innovation. Email: iga.malobecka@gmail.com.*

[2] By data-driven companies I understand companies that are in possession of large volume of data (so called big data), especially personal data and their business model relies in processing of that data and extracting value from it.

[3] These companies form part of so called GAFA – Google, Amazon, Facebook, Apple.

[4] See for example: Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, ECLI:EU:C:2014:317 (so called "right to be forgotten" case) or Case C-362/14 Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650, in which the CJEU invalidated Safe harbour decision.

[5] A total of six European data protection authorities have investigated Facebook policies (see: Common Statement by the Contact Group of the Data Protection Authorities of The Netherlands, France, Spain, Hamburg and Belgium,: https://www.privacycommission.be/sites/privacycommission/files/documents/Common%20Statement%20Facebook%20-%20final%20-

These cases have highlighted limitations of national and the EU data protection law[6] and made policymakers aware that privacy violations may have consequences that go beyond data protection law. Since then it has been argued that privacy violations by data-driven companies may not be effectively and sufficiently solved solely by data protection law. In its opinion of 2014 the European Data Protection Supervisor (EPDS) explicitly encouraged national data protection, competition and consumer protection authorities to cooperate in order to effectively counteract data protection infringements in online environment[7].

In particular, as shows the ongoing investigation against Facebook initiated by the Bundeskartellamt (German Federal Cartel Authority) in March 2016, data protection infringements may constitute a matter of concern for the competition authorities, particularly when committed by dominant undertakings.

The Bundeskartellamt's investigation, which have both advocates and critics, raises important questions concerning i.a. the boundaries between the competition and data protection laws, as well as whether competition authorities are competent to tackle data protection violations.

Against the main findings of the Bundeskartellamt's preliminary assessment, this paper analyses the question of whether data protection violation should be considered a concern for competition law, in particular whether it could amount to abuse of dominant position, and, if so, under which circumstances.

It is organized as follows. First, I explain what is the reasoning behind incorporating data protection considerations into competition law analysis. Secondly, I present and analyse main assumptions of Bundeskartellamt's preliminary assessment. Thirdly, I consider whether competition law could be an adequate and effective remedy for data protection infringements. Fourth part provides concluding remarks.

1. Setting the scene – reasons for incorporating data protection considerations into competition law analysis

A question of whether data protection considerations should be incorporated into competition law analysis is not straightforward. On the one hand, it can be argued that competition law and data protection law are different fields of law, with their own goals, concepts and remedies. They had evolved as separate law regimes and are enforced by different public authorities. Guided by such assumption, one could think that there is no need to blur the boundaries between them and consider data protection issues in competition analysis.

However, this assumption should be confronted with the ongoing debate on how competition, data protection and consumer protection laws[8] intersect and interact in the digital economy[9].

1.1. Interaction of data protection, competition and consumer protection laws in the digital economy

In order to comprehend the reasons for such interaction between different fields of law in the digital economy, it is essential to shortly explain what are its key features and how it differs from the "old economy".

withOUT%20signatures.pdf), some of which has ended with imposing a fine on Facebook (see e.g.: https://www.privacycommission.be/en/news/judgment-facebook-case). These include: France, Belgium, Germany, the Netherlands, Spain and Italy.

[6] B. J. Koops, 'The Trouble with European Data Protection Law' [2014] Tilburg Law School Research Paper No. 04/2015.

[7] Preliminary Opinion of the EDPS, 'Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy' [2014]. Also: EDPS, 'Report of workshop on Privacy, Consumers, Competition and Big Data' [2014].

[8] However, consumer protection issues are not a subject of this paper and will not be further elaborated on.

[9] See e.g.: Preliminary Opinion of the EDPS, 'Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy' [2014]. Also: F. Costa-Cabral and O. Lynskey, 'Family ties: the intersection between data protection and competition in EU Law' [2017] Common Market Law Review, 54 (1), p. 11-50; M. K. Ohlhausen and A. Okuliar, 'Competition, Consumer Protection, and the Right (Approach) to Privacy' [2015] Antitrust Law Journal pp. 37-38.

The development of digital economy has been accompanied by the rise of new businesses models that are mostly built upon personal data – its collection, processing, extracting knowledge from it and applying conclusions from this process to products or services they offer[10]. Personal data propel functioning of the online industry, and are increasingly becoming an essential input to online businesses (search engines or social networking being one of the most prominent examples thereof).

Without having access to personal data such companies are not able to design and offer products or services, which would be competitive in comparison with products developed by a firm that has a superior access to users' data and feedback[11]. Hence, without having this essential input a firm may find it difficult, if not impossible, to enter and to stay on the market. It should then not come as a surprise that data, especially personal data, have been already acclaimed a new oil of the digital economy[12].

Moreover, contrary to the "old economy", most of services provided by data-driven companies, such as search engines, social networks or e-commerce platforms, are offered free of charge, providing individuals with a possibility to use their functionalities without having to pay for them[13]. However, in practice it is only partially true, as the companies collect in return vast amount of personal data of users (e.g. about their profile, preferences or behaviour) and monetise it by offering advertisers possibility to target particular group of users, which have been identified on the basis of collected data[14]. At the same time, users rarely are aware that when they use such services, they actually agree on giving away their personal data and part of their privacy[15].

Against this background, it may seem that the initial assumption about the separation of competition and data protection law, which may be true for traditional markets, may no longer be appropriate in digital economy and online markets.

Already in 2012, the former Commissioner for Competition J. Almunia pointed out the possibility that "*a single dominant company could of course think to infringe privacy laws to gain an advantage over its competitors*"[16]. This idea has been elaborated on by the European Data Protection Supervisor (EDPS) G. Buttarelli, who in his speech from 2015 stated that „*we should be prepared for potential abuse of dominance cases which also may involve a breach of data protection rules*"[17].

The reasoning behind this argument is that a dominant undertaking in the digital market, whose business model relies on processing personal data, may find it profitable to infringe data protection law in order to collect more personal data. It is because data, especially personal data, is one of the most valuable asset they have that enables them to develop better products and services, and offer more effective targeted advertising services, which are, in turn, their main source of revenue[18].

This argument, although praised by some EU officials, has not been followed by the European Commission and the Court of Justice of the European Union ("CJEU").

---

[10] OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being' [2015].

[11] Autorité de la concurrence and Bundeskartellamt, 'Competition law and data' [2016] pp. 8-11.

[12] 'The world's most valuable resource is no longer oil, but data',´[6 May 2017] The Economist.

[13] M. S. Gal and D. L. Rubinfeld, 'The Hidden Costs of Free Goods: Implications for Antitrust Enforcement' [2015] UC Berkeley Public Law Research Paper No. 259425. Also: Preliminary Opinion of the EDPS, 'Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy' [2014].

[14] I. Graef, 'Blurring Boundaries of Consumer Welfare: How to Create Synergies between Competition, Consumer and Data Protection Law in Digital Markets' [2016] p. 2. Also: A. J. Burnside, 'No Such Thing as a Free Search: Antitrust and the Pursuit of Privacy Goals' [2015] CPI Antitrust Chronicle 5(2) p. 7. Also: Autorité de la concurrence and Bundeskartellamt, "Competition law and data' [2016] pp. 10-11.

[15] G. Colangelo and M. Maggiolino, 'Data Protection in Attention Markets: Protecting Privacy through Competition?' [2017] Journal of European Competition Law & Practice 8 (6) p. 363.

[16] J. Almunia, 'Speech: Competition and personal data protection, Privacy Platform event: Competition and Privacy in Markets of Data Brussels' [26 November 2012].

[17] G. Buttarelli, 'Keynote speech at Joint ERA-EDPS seminar, workshop Competition Rebooted: Enforcement and personal data in digital markets Brussels' [24 September 2015].

[18] See *e. g.* https://economictimes.indiatimes.com/news/international/business/google-facebook-dominated-online-advertising-revenue-in-q3/articleshow/62033838.cms and https://www.cnbc.com/2017/12/20/google-facebook-digital-ad-marketshare-growth-pivotal.html.

1.2. Data protection and competition law in the EU case law – inclusion, exclusion or complementarity?

Up until now there has been no abuse of dominance case before the European Commission and the CJEU that would incorporate data protection considerations in the competition law analysis[19].

Actually, on the contrary, the European Commission and the CJEU have so far been rather reluctant to admit data protection concerns in the EU competition law enforcement, be it a merger control, abuse of dominance or cartel case[20].

In 2006 the CJEU in its judgment in Asnef-Equifax concerning agreements between financial institutions on the exchange of customer solvency information (personal data) indicated that "*any possible issues relating to the sensitivity of personal data are not, as such, a matter for competition law, they may be resolved on the basis of the relevant provisions governing data protection*"[21].

The European Commission rejected data protection interests when assessing the *Google/DoubleClick, Facebook/WhatsApp* and *Microsoft/LinkedIn* mergers, and took the view that "*any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules*"[22]. In Microsoft/LinkedIn merger, however, the Commission modified its stance and added that "*privacy-related concerns (...) can be taken into account in the competition assessment to the extent that consumers see it as a significant factor of quality, and the merging parties compete with each other on this factor*".

Thus, both the CJEU and the European Commission seem to share the same view that that data protection concerns should, in principle, be addressed by data protection laws rather than competition rules[23]. Nonetheless, it should be emphasized that stance of the CJEU and the Commission does not imply that privacy is irrelevant to competition enforcement at all[24]. It rather seems to indicate that competition law should be applied in pursuit of its own objectives[25] and data protection and competition law complement each other.

Regardless of the European Commission's and the CJEU's stance, in 2016 the French and German competition authorities published a joint study "Competition Law and Data", in which they recognized that "*decisions taken by an undertaking regarding the collection and use of personal data can have, in parallel, implications on economic and competition dimensions. Therefore, privacy policies should be considered from a competition standpoint whenever these policies are liable to affect competition, notably when they are implemented by a dominant undertaking for which data serves as a main input of its products or services*"[26]. In their view, although data protection and competition laws serve different goals, privacy concerns cannot be excluded from consideration under competition law simply by virtue of their nature[27].

Against this background, the ongoing investigation against Facebook initiated by the Bundeskartellamt on suspicion that the social network provider had abused its dominant position by infringing data protection rules may become a breakthrough and lead the way for other competition authorities[28]. It is the first time a European competition authority has examined whether a company has violated competition law by infringing data protection rules.

Thus, in the next section I will analyse main findings of the Bundeskartellamt's preliminary assessment released on 19th December 2017. Although the case is still pending and a final decision is

---

[19] G. Colangelo and M. Maggiolino, 'Data Protection in Attention Markets: Protecting Privacy through Competition?' [2017] Journal of European Competition Law & Practice 8 (6) p. 366.

[20] I. Graef, 'Blurring Boundaries of Consumer Welfare: How to Create Synergies between Competition, Consumer and Data Protection Law in Digital Markets' [2016] p. 18.

[21] Asnef-Equifax v Asociación de Usuarios de Servicios Bancarios, Case C-238/05, ECLI:EU:C:2006:734, para. 63.

[22] Facebook/WhatsApp, Case No COMP/M.7217, Commission Decision [2014], OJ C417/4, para. 164.

[23] Autorité de la concurrence and Bundeskartellamt, 'Competition law and data' [2016].

[24] I. Graef, 'Blurring Boundaries of Consumer Welfare: How to Create Synergies between Competition, Consumer and Data Protection Law in Digital Markets', [2016] p. 19.

[25] A.J. Burnside, 'No Such Thing as a Free Search: Antitrust and the Pursuit of Privacy Goals' [2015] CPI Antitrust Chronicle 5 (2) p. 4.

[26] Autorité de la concurrence and Bundeskartellamt, 'Competition law and data' [2016] p. 23.

[27] *Ibid*.

[28] http://blogs.lse.ac.uk/mediapolicyproject/2016/03/23/data-protection-through-the-lens-of-competition-law-will-germany-lead-the-way/.

not expected before early summer 2018[29], the preliminary assessment allows to understand Bundeskartellamt's approach and assess its assumptions.

2. Bundeskartellamt vs. Facebook – outline of the Bundeskartellamt's preliminary assessment

On March 2, 2016 the Bundeskartellamt announced it had initiated proceedings against Facebook[30] on suspicion that it had abused its dominant position by infringing data protection rules[31].

Since then the Bundeskartellamt has been examining whether Facebook, by adopting its terms of service that presumably violate data protection laws and imposing it on users, has abused its allegedly dominant position in the market for social networks.

On December 19, 2017, the Bundeskartellamt published a press release on its preliminary assessment and a background paper, which made clear what would be the focus of the abuse of dominance proceedings. Main findings thereof will be discussed below.

2.1. Why are data protection issues relevant for the Bundeskartellamt?

The Bundeskartellamt takes the view that where access to the personal data of users is essential for the market position of a company, as it is in case of Facebook, the question of how that company handles the personal data of its users is no longer relevant only for data protection authorities, but it becomes an equally relevant question for the competition authorities, as well[32].

The authority considers that in the digital economy, the collection and processing of personal data has become an entrepreneurial activity that is of great relevance for the competitive performance of an undertaking. While examining whether Facebook's terms of service violate data protection rules, the Bundeskartellamt claims to work closely with data protection agencies. However, it should be noted that so far there has been no decision of German data protection authority, which would consider that Facebook's terms and conditions breach data protection law.

It is also worth noting that under the German competition law, access to personal data constitutes a criterion for assessing market power, in particular in the case of online platforms and networks (§ 18(3a) GWB)[33].

In the preliminary assessment, the Bundeskartellamt alleges that Facebook has a superior access to the personal data of its users and other competition-relevant data. In case of social networks, which are data-driven products, access to such data is indispensable to viably compete in the market, i.e. both offer users a competitive product and monetise it by means of advertising.

2.2. Separate market for social networks and Facebook's dominant position

Basically, in order to determine that an undertaking has abused its dominant position under Art. 102 TFEU[34], or national competition law (in Germany: § 19 GWB[35]), it is essential to establish that an undertaking concerned holds a dominant position on a specific relevant market.

---

[29] Bundeskartellamt, 'Preliminary assessment in Facebook proceeding: Facebook's collection and use of data from third-party sources is abusive' [19 December 2017] Press release, https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/19_12_2017_Facebook.html?nn=3591568.

[30] To be precise: Facebook Inc., the Irish subsidiary of the company and Facebook Germany GmbH.

[31] Bundeskartellamt, 'Bundeskartellamt initiates proceeding against Facebook on suspicion of having abused its market power by infringing data protection rules' [2 March 2016] Press release, https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html.

[32] Background information on the Facebook proceeding [19 December 2017] pp. 1-2.

[33] This criterion was introduced in the last amendment of the German Act against Restraints of Competition (GWB – Gesetz gegen Wettbewerbsbeschränkungen) – so called Ninth Amendment of the GWB, which entered into force on 9 June 9 2017.

[34] Treaty on the Functioning of the European Union (Consolidated version) [2012] OJ C 326/47.

[35] Gesetz gegen Wettbewerbsbeschränkungen (Act against Restraints of Competition).

Thus, a first step in any abuse of dominance case is to define the relevant (product, geographical and temporal) market and then to establish that a particular undertaking holds a dominant position on that market[36].

Under EU competition law, dominance is defined as "*a position of economic strength enjoyed by an undertaking, which enables it to prevent effective competition being maintained on a relevant market, by affording it the power to behave to an appreciable extent independently of its competitors, its customers and ultimately of consumers*"[37]. This independence means that dominant undertaking's decisions are largely insensitive to the actions and reactions of competitors, customers and, ultimately, consumers[38]. Actually, referring this definition to the case at issue, it can be argued that the ability to retain users despite continual disregard of their privacy might be seen as a confirmation of dominance, i.e. the ability to act without the need to be concerned about the reaction of customers[39].

This was also the path followed by the Bundeskartelamt[40]. In the current proceedings, the Bundeskartellamt has defined a separate relevant market for social networks in Germany and holds the view that Facebook, with around 30 million users per month in Germany of which 23 million use Facebook on a daily basis, has a dominant position on that market[41].

Although the Bundeskartellamt acknowledges that several smaller German operators of social networks such as Google+ are active in the same market, it considers that due to existence of direct network effects they can provide only limited substitutability[42]. Moreover, professional networks (LinkedIn and Xing), messaging services (WhatsApp and Snapchat) or other social media (YouTube or Twitter) are not considered part of the same relevant product market, because from the users' perspective they satisfy complementary needs and do not constitute real substitutes[43]. Interestingly, the Bundeskartellamt found that German users mainly use Facebook to stay in touch with friends within Germany, therefore, the relevant geographical market is limited to Germany[44]. However, in its preliminary assessment the Bundeskartellamt provides little evidence supporting such delineation of the relevant market and it seems that potential line of defence of Facebook may consists in undermining the national dimension of Facebook's market.

Facebook's dominant position has been established basing on its high market shares, identity-based direct network effects[45], as well as high barriers to entry. The Bundeskartellamt argues that due to existence of network effects, users are "locked in" and find it "extremely difficult" to switch to other social network. Moreover, market entry of new competitors is further hindered by indirect network effects. It means that social networks, as a service financed by advertising revenues, has to achieve critical number of users (potential ads-addressees) in order to offer competitive advertising services. Without sufficient number of users, a new entrant will not be able to survive on the market. Furthermore, the Bundeskartellamt has not found "multi-homing" (i.e. parallel use of different social networks by the same users) in the social networks market, which could potentially have a deconcentration effect and could be used as an argument in favour of Facebook[46].

These findings have led the Bundeskartellamt to conclude that Facebook is not only dominant on the market for social networks, but should be seen as a quasi-monopolist. As such, it is subject to "special

[36] R. Whish and D. Bailey, 'Competition Law' (London: Oxford University Press 2012) pp. 180-181.

[37] See: Case 27/76 United Brands Company and United Brands Continentaal v Commission, ECLI:EU:C:1978:22, para 65. However, economists would not consider whether an undertaking has a dominant position but whether it has substantial market power. See: R. Whish and D. Bailey, 'Competition Law' (London: Oxford University Press 2012) p. 180.

[38] Communication from the Commission — Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, C 45/7, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009XC0224(01)&from=EN.

[39] A. J. Burnside, 'No Such Thing as a Free Search: Antitrust and the Pursuit of Privacy Goals' [2015] CPI Antitrust Chronicle 5 (2) p. 6.

[40] Bundeskartellamt, 'Big Data und Wettbewerb', Schriftenreihe „Wettbewerb und Verbraucherschutz in der digitalen Wirtschaft", pp. 12-13.

[41] Background information on the Facebook proceeding [19 December 2017] p. 3.

[42] *Ibid*.

[43] *Ibid*.

[44] *Ibid*.

[45] Identity-based direct network effects reflect the fact that when users have to choose a social network, their choice will be driven by its size and the possibility to find the persons they want to be in contact with on it.

[46] Background information on the Facebook proceeding [19 December 2017] p. 3.

obligations"[47] and bears a "special responsibility" not to allow its conduct to impair undistorted competition on the internal market[48].

Nonetheless, it seems that this part of the Bundeskartellamt's background information on the Facebook proceeding has raised rather more questions than it has answered, mainly due to several legal ambiguities concerning, inter alia, establishing market definition, market shares and Facebook's "quasi-monopolist" position.

2.3. Abuse of dominant position – violation of data protection rules?

In general, abuse of dominant position can take different forms and the list included in Art. 102 TFEU is not exhaustive[49]. Typically, they are divided into exclusionary and exploitative abuses[50]. Whereas exclusionary abuse covers different types of practices that aim at excluding competitors from the relevant market and restrict competition, exploitative abuse, in turn, consists of directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions, thereby exploiting customers or suppliers. In other words, prohibition of exploitative abuses expressed both in EU and national competition law aims to protect the opposite market side (customers, suppliers, consumers) from being exploited by a dominant undertaking.

It is worth noting that in the "old economy" one would consider exploitation in terms of charging an excessive price. However, since in the digital economy the payment for the services is not in cash but in personal data, the exploitation might well consists in other types conduct, e.g. excessive harvesting of such data[51].

In the case at issue, the Bundeskartellamt alleges that Facebook engages in exploitative abuse contrary to § 19 GWB[52]. The Bundesrkatellamt alleges that Facebook imposes unfair (exploitative) business terms on users. Their exploitative character consists in making the use of its social network conditional upon the user granting the company unlimited permission to use his personal data. Bearing in mind that there is no alternative social network available on the market, the user has to choose between agreeing to "the whole Facebook package" (i.e., Facebook's terms and conditions), including an extensive permission to process his or her personal data, or not to use social networks at all.

2.3.1. Data collected "on" and "off" Facebook

When in March 2016 the Bundeskartellamt announced commencement of Facebook investigation, many commentators thought that the authority would pursue potential privacy violations resulting from Facebook's terms of service as a whole.

Nonetheless, the Bundeskartellamt has decided to draw a distinction between user data collected through the use of Facebook ("on Facebook") and user data obtained from other sources ("off Facebook"). The ongoing investigation focuses on the terms and conditions Facebook is applying to data from third party sources, which include services owned by Facebook (e.g. WhatsApp or Instagram), as well as websites and apps of other operators with embedded Facebook APIs[53] (such as the Facebook "Like" button or a "Log-in" option).

According to the Bundeskartellamt, these terms allows Facebook to collect data from users as they call up one of these third party's website, even if they blocked web tracking in their browser or device

[47] Bundeskartellamt, 'Bundeskartellamt initiates proceeding against Facebook on suspicion of having abused its market power by infringing data protection rules' [2 March 2016] Press release.

[48] According to the CJEU case law, holding a dominant position confers a special responsibility on the undertaking concerned, not to allow its conduct to impair undistorted competition on the internal market. See: Case 322/81 Nederlandsche Banden Industrie Michelin (Michelin I) v Commission, para 57.

[49] R. Whish and D. Bailey, 'Competition Law' (London: Oxford University Press 2012) p. 193.

[50] *Ibid*., p. 201.

[51] A.J. Burnside, 'No Such Thing as a Free Search: Antitrust and the Pursuit of Privacy Goals' [2015] CPI Antitrust Chronicle 5 (2) p. 4.

[52] The Bundeskartellamt examines Facebook's practice under national law - § 19 GWB, which contains the general prohibition to abuse a dominant position, and not Art. 102 TFUE. However, § 19 GWB is a provision of national law that corresponds to Art. 102 TFEU.

[53] API stands for application programming interfaces.

settings or do not click on the "Like" or "Log-in" buttons. This data is subsequently merged with data from the user's Facebook account, thereby creating a detailed profile of each user[54].

Use of personal data generated by users on Facebook itself ("on Facebook") is not subject to the current proceedings. Interestingly, in that regard, the Bundeskartellamt explains that as a rule, "*competition concerns do not arise where, as part of a business model which is based on a company offering a product or service for free and monetising this through targeted advertising, data that are generated through the use of the product or service are used for advertising activities*". The Bundeskartellamt understands that this the very nature of social network and when users use such a free service, they must expect that a certain processing of their data will take place. What is more, the authority's argument goes, users themselves can influence the extent of their data being processed by deciding which information and data they want to share on Facebook. However, in my view, such assumption disregards the fact that most people confronted with lengthy and sometimes incomprehensible terms and conditions, and with no alternative option available, agree on everything without reading[55]. Therefore, also with regard to "on Facebook" data it can be doubted whether "*the consumers are sufficiently informed about the type and extent of data collected*"[56].

2.3.2. How does Facebook terms of service violate data protection rules?

The Bundeskartellamt does not explain exactly on which legal basis it finds that a breach of data protection law has taken place and what rules have been infringed. It notes, however, that its assessment involves the principles of the harmonised European data protection rules, especially the EU General Data Protection Regulation (GDPR)[57], which will be applied as of 25th May 2018, as well as the currently applicable Data Protection Directive[58].

Having regard to the findings of the Bundeskartellamt, it is possible to predict what data protection rules may, in the view of the Bundeskartellamt, have been breached by Facebook.

Consent

First of all, the Bundeskartellamt argues that due to Facebook's market power and lack of viable alternatives, users cannot switch to other social networks. Consequently, if they want to use Facebook, they have no other option than to accept its terms of service. According to GDPR, consent, being one of the legal basis of lawful data processing, should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her (recital 32, Art. 4(11), Art. 7 GDPR)[59].

Consent given by Facebook users under above mentioned circumstances could be deemed contrary to data protection rules which seek to ensure that "*users can decide freely and without coercion on how their personal data are used*"[60]. Moreover, as users are mostly unaware what is the exact extent of collected data and purposes of processing, it is also doubtful whether such consent is sufficiently informed. Thus, if consent given by Facebook users did not fulfil above requirements, it could be considered invalid. As a result, Facebook would process personal data of its users without a legal basis.

Purpose limitation and data minimisation

Facebook's terms of service may also be considered contrary to the key principles of personal data processing: principle of purpose limitation referred to in Art. 5(1)(b) GDPR (Art. 6(1)(b) Data Protection

[54] Facebook/Germany – a new frontier for privacy and competition?

[55] B.J. Koops, 'The Trouble with European Data Protection Law' [2014] Tilburg Law School Research Paper No. 04/2015.

[56] Bundeskartellamt, 'Bundeskartellamt initiates proceeding against Facebook on suspicion of having abused its market power by infringing data protection rules' [2 March 2016] Press release.

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

[58] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) [1995] OJ L 281/31.

[59] Art. 2(f) Data Protection Directive.

[60] Background information on the Facebook proceeding [19 December 2017] p. 4.

Directive), as well as principle of data minimisation contained in Art. 5(1)(c) GDPR (Art. 6(1)(c) Data Protection Directive)[61].

According to these principles, personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes (principle of purpose limitation), as well as must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (principle of data minimisation).

In the case at issue, it can be argued that Facebook collects personal data beyond what is necessary to accomplish purposes of processing, and processes it in a way that is incompatible with those purposes.

Transparency requirements

Facebook's terms of service may be in breach of transparency requirements set out in Art. 5(1)(a) and Art. 12 GDPR[62]. Under principle of transparency, it should be transparent to data subjects that their personal data are collected, used or otherwise processed and to what extent their personal data are or will be processed. The controller must ensure that data subject is rightly informed about the existence of the processing operation and its purposes (recital 60 GDPR).

Since, as already noted, Facebook users are oblivious as to which data from which sources are merged to develop a detailed profile of them and their online activities, it can be contended that Facebook does not effectively fulfil transparency requirements.

2.3.3. Searching for a link between alleged data protection breaches and abuse of dominance

Whereas basing on scarce information included in the preliminary assessment, it is possible to predict which data protection rules could have been breached by Facebook in the case at issue, the Bundeskartellamt's preliminary assessment does not convincingly clarify how these alleged data protection breaches lead to an exploitative abuse of dominance.

It does not suffice to state that Facebook's terms of service are in breach of data protection, thus are unfair and since users do not have other option than to accept it in order to use the social network, they are also exploitative and therefore constitute an abuse of dominance.

Apart from the alleged data protection violation there must be some other criteria which allow for establishing that Facebook has abused its dominant position. However, at this stage of proceeding, they cannot be inferred from the materials published by the Bundeskartellamt.

3. Competition law as a remedy for data protection infringements?

Having presented and discussed main assumptions of the Bundeskartellamt preliminary assessment, this section will evaluate whether competition law can be an effective, adequate and permissible remedy of data protection infringements.

First of all, whatever the approach of competition authorities will be, i.e. whether competition authorities decide to pursue data protection violations under Art. 102 TFEU[63] or not, it should be remembered that prohibition of abuse of a dominant position has limited scope of applicability. It would address only such data protection violations which would be committed by dominant undertakings. Thus, violation of data protection by non-dominant undertakings could not be tackled by competition authorities.

Although intuitively one could think that Google, Facebook, or Amazon are dominant in their respective relevant markets, a competition authority must conduct a detailed analysis of each relevant market and undertaking's market power. Defining relevant market and establishing dominance in the

[61] I. Graef, 'Blurring Boundaries of Consumer Welfare: How to Create Synergies between Competition, Consumer and Data Protection Law in Digital Markets' [2016] p. 16.

[62] Art. 29 Working Party, Guidelines on transparency under Regulation 2016/679, adopted on 29 November 2017 as last Revised and Adopted on 11 April 2018 (WP260 rev.01).

[63] Or corresponding national provision containing the prohibition of abuse of a dominant position.

digital markets, which are dynamic, where users typically do not have to pay for services they receive and there are no economic or technical barriers for users to switch, can be, however, quite challenging[64].

Secondly, in my view competition authority is not in position to examine infringements of data protection laws. Policing data protection law falls within the competence of data protection authorities, which is conferred upon them by national law. If competition authority grants itself a right to determine existence of a breach of data protection law, which does not fall within its competence, it could be accused of breaching constitutional principle of legality, which states that authorities can only act on the basis and within the law. Simple "*cooperation with data protection authorities"*[65] does not seem sufficient.

This evaluation would be different, if it had been previously established by competent data protection authority or a court that a dominant firm breached data protection laws. In such situation, however, it could be questioned why competition authorities, which have scarce resources, should pursue a conduct that already has been examined and sanctioned by data protection authorities. Thus, although I recognize that both proceedings have different goals, the potential negative effect of such conduct on competition would be mitigated within data protection proceedings and competition authority's resources could be used to pursue other infringements of competition law. Pursuing data protection violations under competition law could thus be seen as either contrary to principle of legality, or ineffective, especially in terms of distributing public resources.

Thirdly, it should be emphasized that a violation of data protection law by a dominant undertaking can under no circumstances be automatically equated with an abuse of dominant position. Such allegation should be well-grounded and supported by competition law arguments. If the competition authority assumes that such violation constitutes an exploitative abuse of dominance, it must state the reasons why particular conduct is unfair and exploitative, and how it harms consumers and competition. Although the Bundeskartellamt states that there must be "*a connection between such an infringement and market dominance*", it does not explain what is this connection.

Fourthly, it should be observed that Facebook case reflects a tendency of extending "special responsibility" of a dominant firm to comply with all fields of law, not only competition law[66]. This tendency results from the CJEU's judgement in *AstraZeneca*, in which it was made clear breach of one field of law could be relevant for determining an infringement of competition law.[67] To support the inclusion of data protection considerations in competition law some scholars also refer to the CJEU's judgement in *Allianz Hungaria*[68]. In that case the CJEU held that statutory requirements stemming from other fields of domestic law could be taken into account when assessing whether there was a restriction of competition. However, these two judgements should be confronted with the CJEU's judgement in *Asnef – Equifax* and the European Commission's decision-making practice, which explicitly excludes privacy issues from competition law.

To sum up, under certain circumstances violation of data protection laws can give rise to an abuse of dominant position, and in that regard, competition law could be perceived as permissible remedy to data protection infringements. However, there are reasonable doubts whether it would be most adequate and effective way of pursuing privacy infringements.

Conclusion

The digital economy has created new challenges, both for data protection and competition authorities. As shows the ongoing investigation against Facebook by the Bundeskartellamt, data protection infringements may constitute a matter of concern for the competition authorities, when

[64] See: J. M. Newman, 'Antitrust in Zero-Price Markets: Foundations' [2015] 164 U. Pa. L. Rev. 149, https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9504&context=penn_law_review. Also: https://chillingcompetition.com/2016/03/02/facebook-privacy-and-article-102-a-first-comment-on-the-bundeskartellamts-investigation/.

[65] Background information on the Facebook proceeding [19 December 2017] p. 5.

[66] https://chillingcompetition.com/2016/03/02/facebook-privacy-and-article-102-a-first-comment-on-the-bundeskartellamts-investigation/.

[67] AstraZeneca v Commission, Case C-457/10 P, ECLI:EU:C:2012:770

[68] Allianz Hungária Biztosító and Others v Gazdasági Versenyhivata*l*, Case C-32/11, ECLI:EU:C:2013:160. See e.g.: F. Costa-Cabral and O. Lynskey, 'Family ties: the intersection between data protection and competition in EU Law' [2017] Common Market Law Review 54 (1) pp. 11-50.

committed by dominant undertakings. However, violation of data protection laws by dominant firms may give rise to an abuse of dominant position only under certain circumstances. Moreover, although competition law may seem a permissible remedy for breaches of data protection laws, effectiveness and legitimacy of such solution can be questioned. As the EU Commissioner for Competition, Margrethe Vestager, put it "*we can't expect competition enforcement to solve all our privacy problems. Our first line of defence will always be rules that are designed specifically to guarantee our privacy".* Without a doubt, that rules will be strengthened under new general data protection regulation[69].

Bibliography

Books

1. R. Whish and D. Bailey, 'Competition Law' (London: Oxford University Press 2012).

Articles

1. A. J. Burnside, 'No Such Thing as a Free Search: Antitrust and the Pursuit of Privacy Goals' [2015] CPI Antitrust Chronicle 5 (2).
2. F. Costa-Cabral and O. Lynskey, 'Family ties: the intersection between data protection and competition in EU Law' [2017] Common Market Law Review, 54 (1).
3. G. Colangelo and M. Maggiolino, 'Data Protection in Attention Markets: Protecting Privacy through Competition?' [2017] Journal of European Competition Law & Practice 8 (6).
4. M. S. Gal and D. L. Rubinfeld, 'The Hidden Costs of Free Goods: Implications for Antitrust Enforcement' [2015] UC Berkeley Public Law Research Paper No. 259425, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2529425.
5. I. Graef, 'Blurring Boundaries of Consumer Welfare: How to Create Synergies between Competition, Consumer and Data Protection Law in Digital Markets' [2016], https://ssrn.com/abstract=2881969.
6. B. J. Koops, 'The Trouble with European Data Protection Law' [2014] Tilburg Law School Research Paper No. 04/2015, https://ssrn.com/abstract=2505692.
7. M. K. Ohlhausen and A. Okuliar, 'Competition, Consumer Protection, and the Right (Approach) to Privacy' [2015] Antitrust Law Journal.
8. 'The world's most valuable resource is no longer oil, but data' [6 May 2017] The Economist.

Cases

1. Allianz Hungária Biztosító and Others v Gazdasági Versenyhivatal, Case C-32/11, ECLI:EU:C:2013:160
2. Asnef-Equifax v Asociación de Usuarios de Servicios Bancarios, Case C-238/05, ECLI:EU:C:2006:734
3. AstraZeneca v Commission, Case C-457/10 P, ECLI:EU:C:2012:770
4. Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, ECLI:EU:C:2014:317.
5. Case C-362/14 Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650
6. Facebook/WhatsApp, Case No COMP/M.7217, Commission Decision [2014], OJ C417/4
7. Google/DoubleClick, Case COMP/M.4731, Commission Decision [2008], OJ C184/10
8. Microsoft/LinkedIn (Case COMP/M.8124) Commission Decision [2017] OJ C184/10

Legislation

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free

[69] M. Vestager, '"Making data work for us", speech at Data Ethics event on Data as Power' [9 September 2016] The EU Commissioner for Competition Copenhagen, https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/making-data-workus_en.

movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.
2. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) [1995] OJ L 281/31.
3. Treaty on the Functioning of the European Union (Consolidated version) [2012] OJ C 326/47.

Other sources

1. J. Almunia, Speech: Competition and personal data protection, Privacy Platform event: Competition and Privacy in Markets of Data Brussels, 26 November 2012, available at http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm.
2. Art. 29 Working Party, Guidelines on transparency under Regulation 2016/679, adopted on 29 November 2017 as last Revised and Adopted on 11 April 2018 (WP260 rev.01).
3. Autorité de la concurrence and Bundeskartellamt, 'Competition law and data' [10 May 2016], http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf.
4. Background information on the Facebook proceeding, 19 December 2017. https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/19_12_2017_Facebook.html?nn=3591568.
5. Bundeskartellamt, 'Big Data und Wettbewerb', Schriftenreihe „Wettbewerb und Verbraucherschutz in der digitalen Wirtschaft", https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Schriftenreihe_Digitales/Schriftenreihe_Digitales_1.pdf?__blob=publicationFile&v=3.
6. Bundeskartellamt, 'Bundeskartellamt initiates proceeding against Facebook on suspicion of having abused its market power by infringing data protection rules', Press release, 2 March 2016, https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html.
7. Bundeskartellamt, 'Preliminary assessment in Facebook proceeding: Facebook's collection and use of data from third-party sources is abusive', Press release, 19 December 2017, https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/19_12_2017_Facebook.html?nn=3591568.
8. G. Buttarelli, Keynote speech at Joint ERA-EDPS seminar, workshop Competition Rebooted: Enforcement and personal data in digital markets Brussels, 24 September 2015, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2015/15-09-24_ERA_GB_EN.pdfChillin'Competition, 'Facebook, Privacy and Article 102- a first comment on the Bundeskartellamt's investigation', https://chillingcompetition.com/2016/03/02/facebook-privacy-and-article-102-a-first-comment-on-the-bundeskartellamts-investigation/.
9. Data protection through the lens of competition law: will Germany lead the way?, [2016],http://blogs.lse.ac.uk/mediapolicyproject/2016/03/23/data-protection-through-the-lens-of-competition-law-will-germany-lead-the-way/.
10. EDPS, Report of workshop on Privacy, Consumers, Competition and Big Data, 2 June 2014, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Big%20data/14-07-11_EDPS_Report_Workshop_Big_data_EN.pdfOECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being' [2015], http://www.oecd.org/innovation/data-driven-innovation-9789264229358-en.htm.
11. Preliminary Opinion of the EDPS, 'Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy' [2014], https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf.
12. The world's most valuable resource is no longer oil, but data, The Economist, 6.05.2017 https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource.
13. M. Vestager, Speech "Making data work for us", speech at Data Ethics event on Data as Power, Copenhagen, 9 September 2016, https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/making-data-workus_en.

14. G. Buttarelli, Keynote speech at Joint ERA-EDPS seminar, workshop Competition Rebooted: Enforcement and personal data in digital markets Brussels, 24 September 2015.

CRIMINAL LIABILITY OF LAWYERS FOR CORRUPTION OFFENCES

Mickevičiūtė Laura[1]

Abstract

The goal of this research is to analyse the criminal liability of lawyers for corruption offences from theoretical and practical perspectives. This article includes such different topics as legal ethics, corruption offences and lawyers' liability. As a general rule, lawyers must always follow the highest ethical rules. The use of professional status to commit offences, *inter alia*, corruption offences, is incompatible with the legal ethics and it violates ethical principles. Criminal liability as the ultimate measure (*ultima ratio*) could be applicable to lawyers who commit corruption offences such as active and passive bribery, abuse of office, or active and passive trading in influence.

This research consists of three parts. The first part introduces the legal regulation of lawyers' criminal liability for corruption offences. The second analyses the consequences of sentencing. Also, the possibility of application of the right to be forgotten to corrupt lawyers is analysed here. The third part examines the Lithuanian case-law in corruption cases. The purpose of this analysis is to answer the following questions: firstly, what legal professionals frequently commit corruption offences? Secondly, what corruption offences (active and passive bribery, trading in influence, or abuse of office) have mostly been committed by lawyers. Thirdly, what is the policy of legal consequences (penalties, penal effect measures, etc.) for corruption crimes committed by lawyers?

Keywords: legal ethics, lawyers, corruption offences, criminal liability, digital journalism

Introduction

The morality is not the same as ethics, but these two categories define the general boundaries of expecting behaviour of individuals, *inter alia,* lawyers. It should be mentioned that, on the one hand, scholars consider that the rules of legal ethics diverge from morality.[2] On the other hand, others argue that ethics should be understood as a general category. This means that ethical rules of various professions should not be divergent.[3] In my opinion, differences of ethical rules are inventible because these rules depend on the essence of a specific legal profession.[4]

As a general rule, lawyers must always behave according to the highest ethical standards. In Lithuania codes of ethics establish ethical principles describing lawyers' behaviour in both professional and personal life for various categories of lawyers such as judges[5], notaries[6], bailiffs[7], prosecutors[8] and advocates[9].

According to B. A. Green, "criminal law has a role in defining the standards of professional conduct governing lawyers directly and, by influencing the drafters of disciplinary rules, indirectly".[10] Although B. A. Green discusses the situation in the USA, his idea is compatible with the regulation in Lithuania. For instance, some of ethical principles for lawyers' behaviour are related to the prevention of corruption

[1] *PhD student at Vilnius University Faculty of Law, Department of Criminal Justice; title of doctoral thesis in preparation is 'Criminal Liability for Trading in Influence'. Fields of research: criminal law, qualification of crimes, corruption offences, trading in influence.*

[2] S. R. Galoob and S. Li 'Are Legal Ethics Ethical? A Survey Experiment' [2013] the Georgetown Journal of Legal Ethics 26 p. 481-490.

[3] J. Gumbis 'Diskusijos apie etiką nuolatos privalo būti dienotvarkėje' [2009], https://www.infolex.lt/portal/start.asp?act=news&Tema=50&str=32390).

[4] The comparison of the ethical rules of various legal professions shows some differences. For example, only an attorney has the ethical duty of confidentiality which talks about the attorney-client privilege. For example, it means, that attorney should not report about his client's guilty. It could be understood as the exception of a moral rule to report about criminal acts to the police.

[5] Lietuvos Respublikos teisėjų etikos kodeksas (Ethics Code of Judges of the Republic of Lithuania) [2006] 12 P-8.

[6] Lietuvos Respublikos notarų etikos kodeksas (Code of Ethics of Notaries of the Republic of Lithuania) [2015] 6.

[7] Antstolių profesinės etikos kodeksas (Code of Professional Ethics of Bailiffs) [2013] 1R-71.

[8] Lietuvos Respublikos prokurorų etikos kodeksas (Code of Ethics of Prosecutors of the Republic of Lithuania) [2012] I-15.

[9] Lietuvos advokatų etikos kodeksas (Code of Ethics of Lithuanian Advocates) [2016] 1R-133.

[10] B. A. Green 'The Criminal Regulation of Lawyers' [1998] Fordham Law Review 67 (02) p. 331.

crimes. Article 12 paragraph 5 of the Code for Judges in the Republic of Lithuania provides that judges should be fair as well as disinterested and not take a bribe. If a judge takes a bribe, he or she breaches the ethical principle of honesty as well as selflessness and commits bribery. It goes without saying that codes of legal ethics are necessary to draw the boundaries of suitable and required behaviour of lawyers. It is obvious that each criminal activity violates principles of ethics and generally negatively affects professional and institutional reputations.

Despite having a good education, job and social status[11] lawyers are not an exception and from time to time they commit various crimes – mostly of the non-violent variety[12]. This article focus on corruption offences committed by lawyers because these crimes are directly related to the breach of ethical principles established in codes of lawyers' ethics. Also, the purpose of this paper is not only present the analysis of the notion of corruption offences but also to review the consequences of the application of criminal liability to lawyers. Also, the impact of digitization on the application of criminal liability to lawyers is discussed here.

An empirical research is carried out in this paper – qualitative analysis of the decisions of the Supreme Court of the Republic of Lithuania in corruption cases. The purpose of this empirical analysis is to review three aspects. Firstly, what legal professionals frequently commit corruption offences? Secondly, what corruption offences (active and passive bribery, trading in influence, or abuse of office) have mostly been committed by lawyers. Thirdly, what is the policy of legal consequences (penalties, penal effect measures, etc.) for corruption crimes committed by lawyers?

1. The legal regulation of lawyers' criminal liability for corruption offences

International and national institutions pay much attention to the fight against corruption. It is a crucial and global issue which has a negative impact on democracy, the economy, institutions and human rights. Also, this phenomenon has serious consequences for the state, its institutions and every person.[13] Therefore, international legal acts – the Council of Europe Criminal Law Convention on Corruption (hereinafter – the Criminal Law Convention) and the United Nations Convention against Corruption[14] (hereinafter – the UN Convention) – were adopted some years ago. The main aim of these legal acts is to fight against corruption. Lithuania has ratified both conventions.

The Criminal Law Convention on Corruption requires Member States to criminalise such acts as active bribery (Article 2 and 7), passive bribery (Article 3 and 8), active and passive trading in influence[15] (Article 12). All of these criminal acts are mentioned in the UN Convention. Furthermore, the UN Convention establishes that States should consider criminalising abuse of functions (Article 19).

The Criminal Code of the Republic of Lithuania[16] establishes criminal liability for passive bribery (Article 225), active bribery (Article 227), passive and active trading in influence (Article 226) and abuse of office (Article 228). The subject of passive bribery and abuse of office has to comply with not only common but specific features. Therefore, only a civil servant or a person equivalent thereto could be convicted of passive bribery or abuse of office. According to Article 230 of the Criminal Code of the Republic of Lithuania, judges, prosecutors, advocates, bailiffs, notaries and their assistants fall within the scope of the meaning of a civil servant and a person equivalent thereto.

---

[11] According to D. Weisburd, "high occupational status may offer many advantages in this world, but it appears to be neither a guarantee against becoming a criminal nor an assurance that one's crimes will be organizationally complex" in B. A. Green 'The Criminal Regulation of Lawyers' [1998] Fordham Law Review 67 (02) p. 327.

[12] There are some cases when lawyers are convicted of violent crimes. For instance, in Lithuania a prosecutor was convicted of domestic violence. The Court of Appeal of Lithuania's decision was rendered on 3 February 2014 in criminal case No. 1A-139/2014.

[13] The Council of Europe Criminal Law Convention on Corruption [1999] (available at https://rm.coe.int/168007f3f5).

[14] The United Nations Convention against Corruption [2003], https://www.unodc.org/documents/brussels/UN_Convention_Against_Corruption.pdf).

[15] Article 37 paragraph 1 of the Criminal Law Convention provides that States may, at the time of signature, reserve the right not to establish trading in influence as a criminal offence under domestic law. Lithuania did not make this reservation. *See* A chart of signatures and ratifications of Treaty 173, Criminal Law Convention on Corruption, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/173/signatures?p_auth=5u0z8Cen.

[16] Lietuvos Respublikos baudžiamasis kodeksas (the Criminal Code of the Republic of Lithuania) [2000] Žin. 89-2741.

In Lithuania there are no differences between the regulation of lawyers' and other civil servants' criminal liability for corruption offences – the same *corpus delicti* and sanctions. The Germany Criminal Code[17] establishes different penalties for judges (Article 331 paragraph 2 ("passive bribery")). According to this regulation, the criminal liability of judges is heavier than a public official or person entrusted with special public service.

The lawyers' conduct is limited according to ethical rules (principles). As is mentioned earlier, lawyers commit crimes, *inter alia,* corruption offences. There is no doubt that each criminal act is related to the violation of boundaries of lawyers' ethical principles.[18] Scholars present various cases of how lawyers commit corruption offences. They separate the following types of liability, which depend on the level of involvement of the lawyer in any corrupt activity: *principal liability* (lawyers directly carry out a corrupt act), *accessory liability* (indirectly involved in the payment of a bribe such as an accessory or accomplice to a principal offender as well as an intermediary) and *other liability* (related to anti-money laundering legislation).[19] Lawyers commit corruption offences not only for personal financial purposes but also for professional ones. For instance, an attorney could be an illegal intermediary between his or her client and a judge or prosecutor. For example, an attorney takes a bribe from his or her client and brings it to a judge or prosecutor for favourable decisions for his or her client.

2. Consequences

The consequences of the application of lawyers' criminal liability are another aspect that should be discussed. In advance, the three groups of consequences should be mentioned: first of all, legal consequences established in the criminal law; second, the consequences related to professional liability; lastly, the consequences caused by publicity of criminal proceedings.

The Criminal Code of the Republic of Lithuania establishes various penalties (such as fines, restriction of liberty, arrest, fixed-term custodial sentence) for corruption crimes. A particular penalty depends on the type and level of the crime. For example, Article 225 paragraph 3 provides only a fixed-term custodial sentence for high-qualified passive bribery. In comparison with high-qualified passive bribery, the high-qualified active bribery is punishable by alternative penalties – a fine or a fixed-term custodial sentence. According to the Criminal Code of the Republic of Lithuania, the deprivation of the right to be employed in a certain position is not a penalty but the penal effect measure and it could be applied to lawyers together with the penalty imposed for corruption offences. The court can deprive the right to be employed in a certain position for a certain period of time.

The conviction of corruption offences affects lawyers' career. Legal scholars emphasize that lawyers who are found guilty of corruption offences not only face criminal penalties but are also subject to professional discipline.[20] According to Article 52 of the Law on Courts of the Republic of Lithuania[21], the lawyer who was convicted of corruption offences will have never become a judge. The same regulation is for lawyers who want to become a prosecutor[22]. A rather different regulation is applicable to lawyers who want to become attorneys[23]. A lawyer who committed corruption offences cannot be an attorney when the judgment for conviction becomes *res judicata*. However, this restriction is limited by the time-period.

[17] 'The German Criminal Code', https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html.

[18] J. F. McSorley 'Criminal Lawyers or Lawyer Criminals? Ethics of the Criminal Defense Bar Under Attack' [1998], https://www.floridabar.org/news/tfb-journal/?durl=%2FDIVCOM%2FJN%2Fjnjournal01.nsf%2FArticles%2F2B90FFA8FDFA911885256ADB005D619F.

[19] 'The Role of Lawyers in the Fight against Corruption. A Summary Report' [2013], https://www.trust.org/contentAsset/raw-data/af585d7d-6a7f-4c65-9b5c-3b5534118c74/file); D. Middleton and M. Levi 'Let Sleeping Lawyers Lie: Organized Crime, Lawyers and the Regulation of Legal Services' [2015] The British Journal of Criminology 55 (4) p. 647–668.

[20] H. R. Lieberman 'Lawyers Who Commit Crimes: Disciplinary Consequences' [2013], http://nylegalethics.attorney/lawyers-who-commit-crimes-disciplinary-consequences/.

[21] Lietuvos Respublikos teismų įstatymas [1994] Žin. 46-851.

[22] Lietuvos Respublikos prokuratūros įstatymas (the Republic of Lithuania Law on the Prosecution Service) [1994] Žin. 81-1514.

[23] Lietuvos Respublikos advokatūros įstatymas (the Republic of Lithuania Law on the Bar) [2004] Žin. 50-1632.

Scholars consider whether criminals could expect privacy during criminal proceedings at all.[24] The same question is considered in this article – whether convicted lawyers could expect privacy. The High Court of Justice of the United Kingdom found that "the crime and punishment information is not information of a private nature"[25]. The publicity of criminal proceedings is a general rule also established in the Code of Criminal Procedure of the Republic of Lithuania[26]. Journalists can participate in the hearings and/or to ask the institutions of the pre-trial investigation or courts to give certain information about some facts of cases. It ensures both the right to freedom of expressions and the right to be informed. Today digital journalism helps to ensure that information about criminal proceedings would be provided effectively and timely.

Also, the result of the process of digitalization is that the society can easily find information about old criminal cases. According to Y. Haga, this digitalization process helps to forget how to forget. The right to be forgotten must be discussed.[27] Article 17 of the General Data Protection Regulation[28] establishes the right to be forgotten which means that "the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay".

The publicity of criminal proceedings may cause consequences such as public criminal labelling[29] or unjust punishment[30]. There is no one simple answer to the question whether lawyers convicted of corruption offences have the right to be forgotten or not.[31] The main aspect is to strike a balance between the right to be forgotten and the right to freedom of expressions/the right to be informed. According to GDPR, the right to be forgotten is not absolute. This means that some restrictions are possible. Some scholars argue that some information about convictions of corruption offense despite the fact that it was many years ago it is still important for some reasons.[32] The difficult question is what information is irrelevant and outdated. The following aspects should be considered: the status of offender (a public or private person), the nature of crime (the public interest), the length of time after the conviction (according to the Criminal code of the Republic of Lithuania, a convicted person shall be considered as having no criminal record after previous convictions expire).[33]

3. Analysis of the criminal liability of lawyers in the case-law of the Supreme Court of Lithuania

According to the previous research that was conducted by Transparency International Lithuania in 2016,[34] most passive bribery offenses are committed by police officers and most active bribery is committed by private persons.

The Author has made empirical research on the application of criminal liability for corruption offences and analysed the decisions of Supreme Court of Lithuania which were rendered during 2004-2018 years. The legal information system 'infolex' was used to get access to the decisions rendered by the Supreme Court of Lithuania. All of the criminal cases that proceeded in 2004-2018, in which 'Article 225 or Article 226, or Article 227, or Article 228' were mentioned, were reviewed. Decisions addressed to lawyers are included in the analysis.

---

[24] *See* M. Tunick 'Privacy and Punishment' [2013] Social Theory and Practice 39 (4) pp. 643-668; K. Hadjimatheou, 'Criminal Labelling, Publicity, and Punishment' [2016] Law and Philosophy 35 pp. 567–593.

[25] NT1 & NT2 v Google LLC, Case No. Q15X04127,HQ15X04128 [2018].

[26] Lietuvos Respublikos baudžiamojo proceso kodeksas [2002] Žin. 37-1341.

[27] Y. Haga, 'Right to be Forgotten: A New Privacy Right in the Era of Internet' [2017] New Technology, Big Data and the Law p. 98-99.

[28] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119.

[29] K. Hadjimatheou, 'Criminal Labelling, Publicity, and Punishment' [2016] Law and Philosophy 35 pp. 567–593.

[30] M. Tunick, 'Privacy and Punishment' [2013] Social Theory and Practice 39 (4) pp. 643-668.

[31] *See* G. Brock, 'The Right to be Forgotten – Privacy and the Media in the Digital Age' (I. B.Tauris 2016); Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12 [2014].

[32] Y. Haga, 'Right to be Forgotten: A New Privacy Right in the Era of Internet' [2017] New Technology, Big Data and the Law pp. 108-109.

[33] *Ibid*.; NT1 & NT2 v Google LLC, Case No. Q15X04127, HQ15X04128 [2018].

[34] Kyšininkavimas Lietuvoje: bylų analizė ir asmens, teisiamo už kyšininkavimą, prekybą poveikiu ir papirkinėjimą, sociologinis portretas [2016], http://www.transparency.lt/wp-content/uploads/2016/02/Kysininkavimas_Lietuvoje_2006-2013.pdf.

The number of relevant decisions is only 12[35]. The results show that corruption offences that were committed by lawyers represent only the smallest part of corruption crimes. Also, it is important to keep in mind the latency[36]. Criminal cases are analysed in table 1 in detail.

Despite the fact that the small number of cases limits the ability to generalise conclusions, some findings have still been drawn. Firstly, lawyers such as judges, prosecutors, attorneys, notaries and bailiffs were convicted mostly of trading in influence. The tendency is seen that the number of convictions of trading in influence have peaked since 2011.[37] Also, trading in influence was mainly committed by attorneys. Furthermore, attorneys were mainly convicted of various corruption offences such as active and passive bribery and trading in influence. Meanwhile, a judge was only convicted of passive bribery and trading in influence. There were several cases in which bailiffs were convicted of abuse of office because they used their position in order to get undue advantages.

Lastly, the research shows the sentencing policy of lawyers for corruption offences. This research reveals that courts basically fined lawyers for corruption offences. A real imprisonment has been imposed to none of the lawyers. Though some lawyers were sentenced to imprisonment, the enforcement of penalties of imprisonment was suspended. The courts often imposed two penal effect measures – the confiscation of property and the deprivation of the right to be employed in a certain position.

Table 1

Crime (number of cases)	Article (para.)	Year of crime	Lawyer's profession	Penalty and penal effect measures
Active bribery (2)	227 (1)	2014	Attorney	A fine and two penal effect measures – confiscation of property and deprivation of the right to be employed in a certain position.
	227 (2)	2013	Attorney	Release from criminal liability on bail and the penal effect measure – deprivation of the right to be employed in a certain position.
Passive bribery (3)	225 (3) (two crimes)	2009	Bailiff	A fine and suspension of an imprisonment sentence.
	225 (2)	2011	Judge	A fine and a penal effect measure – confiscation of property.
	225 (1)	2010	Prosecutor	Suspension of an imprisonment sentence.
Passive trading in influence (5)	226 (2)	2013	Attorney	A fine and a penal effect measure – confiscation of property.
	226 (2)	2011	Judge	A fine and a penal effect measure – confiscation of property.
	226 (2)	2014	Assistant of an attorney	A fine.
	226 (2)	2014	Attorney	A fine.
	226 (1)	2007-2009	Attorney	Arrest.
Abuse of office (3)	228 (2) (two crimes)	2004-2005	Bailiff	A fine and deprivation of the right to be employed in a certain position.
	228 (2) (four crimes)	2006-2007	Prosecutor	A fine and a penal effect measure – deprivation of the right to be employed in a certain position.
	228 (2)	2003 -2005	Bailiff	Deprivation of the right to be employed in a certain position and a penal effect measure – confiscation of property.

[35] In one criminal case a judge was convicted of both bribery and trading in influence.

[36] G. Sakalauskas, *et. al.* 'Registruotas ir latentinis nusikalstamumas Lietuvoje: tendencijos, lyginamieji aspektai ir aplinkos veiksniai' (Vilnius: Eugrimas 2011) p. 152.

[37] In general, statistics of pre-trial investigations show that since 2011 the number of pre-trial investigations of trading in influence has been changing, available at http://prokuraturos.lt/lt/administracine-informacija/planavimo-dokumentai-ataskaitos/ataskaitos/138. It should be mentioned that on 21 June 2011 fundamental amendments to the regulation of trading in influence were adopted. On the one hand, these amendments could have an impact on the statistics. On the other hand, the statistics has been changing because of the work of pre-trial investigation institutions. Lietuvos Respublikos baudžiamojo kodekso 7, 42, 67, 68, 74, 123[1], 125, 126, 134, 142, 144, 176, 177, 204, 205, 210, 211, 213, 220, 223, 225, 226, 227, 228, 228[1], 229, 230, 253[1], 255, 257, 263, 268, 278, 281, 297, 308[1]straipsnių pakeitimo ir papildymo, Kodekso papildymo 68[1], 68[1]straipsniais ir 44, 45 straipsnių pripažinimo netekusiais galios įstatymas [2011] Žin. 81-3959.

Conclusions

I. The general norms of the Criminal Code of the Republic of Lithuania that establish criminal liability for corruption offences (active and passive bribery, trading in influence, abuse of office) are also applied to lawyers such as judges, prosecutors, attorneys, bailiffs, notaries and their assistants. Legal and unjust punishment could be imposed on lawyers who found guilty of corruption offences. The unjust punishment is imposed by society.

II. The right to be forgotten is not absolute. Thus, for some people, *inter alia*, convicted lawyers, this right might be restricted. Convicted lawyers might invoke this right depending on particular facts of the case and person. However, the court must strike a balance between the right to be forgotten and other relevant rights in this case.

III. In Lithuania the number of criminal cases in which lawyers have been convicted of corruption offences is low. The courts mainly impose a fine or a suspension of imprisonment regardless of the type of a crime or profession.

Bibliography

Legal acts:

1. Antstolių profesinės etikos kodeksas (Code of Professional Ethics of Bailiffs) [2013] 1R-71.
2. Lietuvos advokatų etikos kodeksas (Code of Ethics of Lithuanian Advocates) [2016] 1R-133.
3. Lietuvos Respublikos advokatūros įstatymas (the Republic of Lithuania Law on the Bar) [2004] Žin. 50-1632.
4. Lietuvos Respublikos baudžiamasis kodeksas [2000] Žin. 89-2741.
5. Lietuvos Respublikos baudžiamojo kodekso 7, 42, 67, 68, 74, 123^1, 125, 126, 134, 142, 144, 176, 177, 204, 205, 210, 211, 213, 220, 223, 225, 226, 227, 228, 228^1, 229, 230, 253^1, 255, 257, 263, 268, 278, 281, 297, 308^1 straipsnių pakeitimo ir papildymo, Kodekso papildymo 68^1, 68^1straipsniais ir 44, 45 straipsnių pripažinimo netekusiais galios įstatymas [2011] Žin. 81-3959.
6. Lietuvos Respublikos baudžiamojo proceso kodeksas [2002] Žin. 37-1341.
7. Lietuvos Respublikos notarų etikos kodeksas (Code of Ethics of Notaries of the Republic of Lithuania) [2015] 6.
8. Lietuvos Respublikos prokurorų etikos kodeksas (Code of Ethics of Prosecutors of the Republic of Lithuania) [2012] I-15.
9. Lietuvos Respublikos prokuratūros įstatymas (the Republic of Lithuania Law on the Prosecution Service) [1994] Žin. 81-1514.
10. Lietuvos Respublikos teisėjų etikos kodeksas (Code of Ethics of Judges of the Republic of Lithuania) [2006] 12 P-8.
11. Lietuvos Respublikos teismų įstatymas [1994] Žin. 46-851.
12. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119.
13. The Council of Europe Criminal Law Convention on Corruption [1999], https://rm.coe.int/168007f3f5.
14. 'The German Criminal Code', https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html.
15. The United Nations Convention against Corruption [2003], https://www.unodc.org/documents/brussels/UN_Convention_Against_Corruption.pdf.

Books and articles:

1. G. Brock, 'The Right to be Forgotten – Privacy and the Media in the Digital Age' (I.B.Tauris 2016).
2. S. R. Galoob and S. Li, 'Are Legal Ethics Ethical? A Survey Experiment' [2013] The Georgetown Journal of Legal Ethics 26.
3. B. A. Green, 'The Criminal Regulation of Lawyers' [1998] Fordham Law Review 67(02).

4. K. Hadjimatheou, 'Criminal Labelling, Publicity, and Punishment' [2016] Law and Philosophy 35.
5. Y. Haga, 'Right to be Forgotten: A New Privacy Right in the Era of Internet' [2017] New Technology, Big Data and the Law.
6. H. R. Lieberman, 'Lawyers Who Commit Crimes: Disciplinary Consequences' [2013], http://nylegalethics.attorney/lawyers-who-commit-crimes-disciplinary-consequences/.
7. J. F. McSorley 'Criminal Lawyers or Lawyer Criminals? Ethics of the Criminal Defense Bar Under Attack' [1998], https://www.floridabar.org/news/tfb-journal/?durl=%2FDIVCOM%2FJN%2Fjnjournal01.nsf%2FArticles%2F2B90FFA8FDFA911885256ADB005D619FD. Middleton and M. Levi, 'Let Sleeping Lawyers Lie: Organized Crime, Lawyers and the Regulation of Legal Services' [2015] The British Journal of Criminology 55 (4).
8. G. Sakalauskas, *et. al.* 'Registruotas ir latentinis nusikalstamumas Lietuvoje: tendencijos, lyginamieji aspektai ir aplinkos veiksniai' (Vilnius: Eugrimas 2011).
9. M. Tunick, 'Privacy and Punishment' [2013] Social Theory and Practice 39(4).

Cases:

1. Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12 [2014].
2. NT1 & NT2 v Google LLC, Case No. Q15X04127,HQ15X04128 [2018].
3. The Supreme Court of Lithuania's decision was rendered on 28 December 2010 in criminal case No. 2K-645/2010.
4. The Supreme Court of Lithuania's decision was rendered on 30 October 2007 in criminal case No. 2K-660/2007.
5. The Supreme Court of Lithuania's decision was rendered on 14 June 2011 in criminal case No. 2K–254/2011.
6. The Supreme Court of Lithuania's decision was rendered on 30 June 2011 in criminal case No. 2K-346/2011.
7. The Supreme Court of Lithuania's decision was rendered on 7 February 2012 in criminal case No. 2K-24/2012.
8. The Court of Appeal of Lithuania's decision was rendered on 3 February 2014 in criminal case No. 1A-139/2014.
9. The Supreme Court of Lithuania's decision was rendered on 10 February 2015 in criminal case No. 2K–86-895/2015.
10. The Supreme Court of Lithuania's decision was rendered on 9 June 2015 in criminal case No. 2K-345-507/2015.
11. The Supreme Court of Lithuania's decision was rendered on 29 October 2015 in criminal case No. 2K-430-746/2015.
12. The Supreme Court of Lithuania's decision was rendered on 16 June 2016 in criminal case No. 2K-239-303/2016.
13. The Supreme Court of Lithuania's decision was rendered on 24 October 2016 in criminal case No. 2K-290-699/2016.
14. The Supreme Court of Lithuania's decision was rendered on 19 December 2016 in criminal case No. 2K-450-697/2016The Supreme Court of Lithuania's decision was rendered on 13 March 2018 in criminal case No. 2K-33-303/2018.

Other sources:

1. Chart of signatures and ratifications of Treaty 173. Criminal Law Convention on Corruption, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/173/signatures?p_auth=5u0z8Cen.
2. J. Gumbis 'Diskusijos apie etiką nuolatos privalo būti dienotvarkėje' [2009], https://www.infolex.lt/portal/start.asp?act=news&Tema=50&str=32390.
3. Kyšininkavimas Lietuvoje: bylų analizė ir asmens, teisiamo už kyšininkavimą, prekybą poveikiu ir papirkinėjimą, sociologinis portretas [2016], http://www.transparency.lt/wp-content/uploads/2016/02/Kysininkavimas_Lietuvoje_2006-2013.pdf.

4. Statistical data from http://prokuraturos.lt/lt/administracine-informacija/planavimo-dokumentai-ataskaitos/ataskaitos/138.
5. 'The Role of Lawyers in the Fight against Corruption. A Summary Report' [2013], https://www.trust.org/contentAsset/raw-data/af585d7d-6a7f-4c65-9b5c-3b5534118c74/file.

WTO LAW V 2.0: RETHINKING THE ROLE OF THE WTO DSB IN E-COMMERCE CASES

Karolina Mickute[1]

Abstract

Recent years have shown a gross increase in electronic cross-border delivery of digital goods and services, however there seems to be little progress in the World Trade Organization (WTO) on regulating international e-commerce as WTO Member States have yet to reach any substantial agreement on matter. Being the key player in regulating international trade and consisting of the majority of states engaging in cross border e-commerce, the WTO is in dire need to seek both short and long term solutions for restating its role in the digital economy. Given that the recent WTO negotiations on regulating e-commerce ended up giving no substantial results and the chances of reaching a binding multilateral agreement on e-commerce in the near future are non-existent, the article suggests revisiting current WTO rules that were created for an analogue world.

Keywords: WTO, e-commerce, WTO DSB, GATT

INTRODUCTION

The more facilitated access to electronic delivery have added new dimensions to the international market.[2] As digital products and electronically traded services play a significant role in the WTO legal framework, the general acknowledgment that the existing GATT[3] and GATS[4] rules and obligations unambiguously apply to digital trade transactions must be secured.[5] Having emphasized the importance of cross-border e-commerce and adopted the Work Programme on Electronic Commerce back in 1998[6], the WTO Member States have yet to reach any substantial agreement on regulating global digital trade. Since the recent WTO Ministerial Conference ended up giving no substantial results in the field of e-commerce, the chances of reaching a binding multilateral agreement on e-commerce in the near future are non-existent. Thus the field of international e-commerce is not coherently regulated as there is no legally binding and uniform standard setting instrument at the international level. Consequently states engage in bilateral or multilateral agreements with different standards. Thus the field of international e-commerce is not left for self regulation. Concluding separate agreements and subsequently applying different standards lead to a fragmented regulation of e-commerce and not ensuring at least the minimal standard leading to possible barriers to the free flow of international trade.

Being the key player in regulating international trade and consisting of the majority of states engaging in cross border e commerce, the WTO is in need to seek both short and long term solutions for restating its role in the digital economy. Moreover, WTO has the capacity to provide comprehensive multilateral regulation of e-commerce since as it is often referred to as the most convenient institutional umbrella for multilateral commitments for e-commerce related issues[7].

---

[1] The author is a PhD candidate and junior researcher at the Faculty of Law of Vilnius University, specializing in International Trade law, Public International law, European Union law.

[2] BRAGA, C. A. P. *E-Commerce Regulation: New Game, New Rules?* in *A Handbook of International Trade in Services* 459, 471 (Aaditya Matto et al. eds, 2008).

[3] General Agreement on Tariffs and Trade 1994, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, 1867 U.N.T.S. 187, 33 I.L.M. 1153 (1994) (hereinafter – GATT).

[4] General Agreement on Trade in Services, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M. 1167 (1994) (hereinafter – GATS).

[5] BRAGA, C. A. P., *E-Commerce Regulation* <…>, p. 459.

[6] WTO. Work Programme on Electronic Commerce Adopted by the General Council on 25 September 1998, WT/L/274 (hereinafter – Work programme).

[7] WUNSCH-VINCENT, S. *The WTO, the Internet and Trade in Digital Products* (2006), p. 13-32.

Considering the latter the article suggests revisiting current WTO rules that were created for an analogue world. Accordingly the purpose of the article is to determine the possible short-term solutions in the WTO legal system to ensure the smooth flow of international e-commerce and create an enabling environment for cross-border digital trade going forward. The article primarily suggests to rely on the WTO Dispute settlement body (hereinafter – the WTO DSB) for ensuring the free and smooth flow of cross-border e-commerce in providing relevant reinterpretations of WTO Agreements and settling international disputes. The article refrains from analyzing the limitations of current WTO legal regulation and does not aim to propose new legal provisions.

The **objective** of the research is to determine the role of the WTO DSB in ensuring the free flow of e-commerce under WTO law. Accordingly the **tasks** of the research are as follows:

1. To analyze the current state of regulation of e-commerce under WTO law.
2. To distinguish the peculiarities of WTO law and the role of the WTO DSB that precondition its engagement in modernizing WTO law.
3. To analyze the WTO DSB reports in recent e-commerce cases before the WTO DSB.

The research object is not analyzed by Lithuanian scholars. Studies on the role of WTO DSB in ensuring e-commerce regulation is fragmented, e.g. particular WTO Member State cases are studied[8], overviews of most recent negotiations are provided[9], the regulation of e-commerce under separate multilateral agreement are analyzed[10], separate WTO DSB reports in e-commerce cases are analyzed[11]. Thus the article is scientifically relevant as it engages in the ongoing discourse on the role of WTO in the digital age and provides possible short term adjustments to rely on the WTO DSB to ensure the free flow of digital economy by linking the role of WTO DSB with the peculiarities of regulating e-commerce under WTO law.

The following theoretical and empirical scientific research methods are applied. The document analysis method is employed to collect primary data, to analyze the provisions of relevant WTO agreements, reports of the WTO DSB and relevant positions of authoritative scientists. The linguistic method is used to determine the content of the provisions used and their meaning in relevant sources. The teleological method is used to distinguish the content and scope of the provisions of the WTO Treaties. The method of systemic analysis and classification is employed to divide the object of the research, its purpose and tasks into components, as well as to assess the internal structure of relevant documents, their interaction with each other in order to identify the complexity of the topic and the its most significant aspects. The logical analysis method is used to identify, associate and generalize the material of the research, to evaluate the relevant aspects of legal documents, its interpretation possibilities and the reasonableness and consistency of the research problem.

The first part of the article discusses the current progress of negotiations on WTO law of e-commerce. The second section provides preconditions for the necessity to not only reinterpret current WTO Agreements in order to reaffirm WTO's role in regulating global trade but also the peculiarities of WTO law and the WTO DSB by emphasizing its capacity to exceed its interpretative functions. The third part of the article is the empirical analysis of the most recent relevant WTO DSB reports in the field of e-commerce. This analysis provides not only insights on the reinterpretation of WTO Agreements, but also emphasizes the role and peculiarities of the WTO DSB in ensuring the free flow of trade under WTO law in the field of regulating e-commerce.

---

[8] *See, e.g.* KAMEL, R. *Emerging Markets and E-Commerce in Developing Economies*, 2008; PANAGARIYA, A. E-Commerce, WTO and Developing Countries. *The World Economy,* 2000, Vol 23, No 8, pp. 959-978; FARROKHNIA, F., RICHARDS, C. The accountability challenge to e-commerce: The need to overcome the developed-developing country divide in WTO e-commerce polices, in LEONARD, L., GONZALEZ-PEREZ, M., (eds.), *Principles and Strategies to balance ethical, social and environmental concerns with corporate requirements*, 2013, Emerald Books.

[9] *See, e.g.* WUNSCH-VINCENT, S. *The WTO, the internet and trade in digital products: EC-US perspectives,* 2006, Bloomsbury Publishing; WUNSCH-VINCENT, S. *WTO, E-commerce, and Information Technologies,* 2004.

[10] *See, e.g.* MONTEIRO, J. A.; TEH, R. Provisions on Electronic Commerce in Regional Trade Agreements. WTO Working Paper ERSD-2017-11, 2017.

[11] *See, e.g.* WUNSCH-VINCENT, S. The Internet, cross-border trade in services, and the GATS: lessons from US-Gambling. *World Trade Review*, 2006, Vol 5, No 3, 319-355; HAYER, J. D. The Trade of Cross-Border Gambling and Betting: The WTO Dispute between Antigua and the United States. *Duke Law & Technology Review,* 2004, Vol 13.

1. Current regulation of e-commerce under WTO law

The issue of regulating e-commerce[12] under WTO law has been a relevant topic over the recent decades. However initially WTO Agreements were adopted without taking into account the phenomenon of e-commerce thus such services are not directly covered by the WTO law[13].

The importance regulating electronic commerce was first emphasized in the Declaration of 1998 adopted by the Geneva Ministerial Conference, according to which the WTO Member States committed themselves to introducing a coherent mechanism for regulating of e-commerce[14]. Soon after the WTO General Council adopted a note to assist WTO Members in their deliberations on trade-related issues pertaining to global electronic commerce pursuant to the Declaration of 1998 (hereinafter – Note)[15]. The Note containes recommendations and basic guidelines of interpreting the existing WTO rules on trade in cases of e-commerce until a coherent mechanism under the Declaration of 1998 will be enacted. Given the recommendatory nature of the Note, the only obligation the WTO Members committed to continue their current practice of not imposing customs duties on electronic transmissions[16].

Accordingly in 1999 the WTO Work Programme on Electronic Commerce[17] (hereinafter – Work Programme) was introduced. It was expected to cover the issues related to e-commerce trade, however, the only substantial agreement the parties achieved was the agreement not to charge import duties on electronic transmissions.[18]

At the Ninth Ministerial Conference in 2013, Members reaffirmed their willingness to reinvigorate the Work Programme, but the States reached a mere agreement to continue their current practice of not imposing customs duties on electronic transmissions.[19] The most recent Eleventh WTO Ministerial Conference held in 2017 ended up giving no binding results on regulating e-commerce, thus the Declaration of 1998 and the subsequent Note are the primary sources of guidelines of reinterpreting WTO law for regulating e-commerce.

Initially electronic commerce was defined by the nature of the production, distribution, sale or delivery of goods or services, i.e. it has to be operated by electronic means[20] meaning that the determinant factor are the means of operations. However the concept developed by distinguishing the nature of the service or produce, and the means of distributing the service or goods[21] thus the concept of e-commerce also encompasses processes when the entire transaction takes place electronically[22].

Given the current state of WTO negotiations on entering a multilateral agreement on regulating e-commerce, the role of WTO as the key player in the international trade arena may crumble. Having expressed their ambition to regulate electronic commerce, it becomes evident that certain short-term measures must be applied to ensure the smooth flow of electronic trade. Whilst the multilateral negotiations are at a standstill, the Member States have already addressed the WTO DSB to settle cases on e-commerce related issues. Therefore the inevitable role of the WTO DSB to engage in the regulatory process via litigation must be analyzed.

---

[12] E-commerce and electronic commerce are interchangeable terms in the context of the article.

[13] WEBER, R. H., *Digital Trade in WTO-Law – Taking Stock and Looking Ahea*d, Asian Journal of WTO & International Health Law and Policy, 2010, Vol. 5, No. 1, pp. 1–24, p. 10

[14] WTO. Declaration on Global Electronic Commerce adopted on 20 May 1998 by the Ministerial Conference, WT/MIN(98)/DEC/2 (hereinafter – Declaration of 1998).

[15] WTO. WTO Agreements and Electronic Commerce adopted on 15 July 1998 by the General Council, WT/GC/W/90 (hereinafter – Note).

[16] Declaration of 1998.

[17] Work Programme on Electronic Commerce, Progress Report to the 45 General Council, adopted by the Council for the Trade in Services on 19 Jul. 1999, S/L/74.

[18] Doha WTO Ministerial 2001: Ministerial Declaration adopted on 20 November 2001, WT/MIN(01)/DEC/1.

[19] Ninth WTO Ministerial Conference. Draft Work Programme on Electronic Commerce – Draft Ministerial Decision adopted on 28 November 2013, WT/MIN(13)/DEC/W/1/Rev. 1.

[20] Work programme, para. 1.3.

[21] According to the Note e-commerce can be defined as comprising three different types of transactions: (i) the provisions of Internet access services themselves, (ii) the electronic delivery of services (products are delivered to the customer in the form of digitized information flows), (iii) (c) the use of the Internet as a channel for distribution services (goods and services are purchased over the net but delivered to the consumer in non-electronic form (Note, para. 2). Due to the limit of the research, internet access-related and intellectual property right - related issues are not further analyzed.

[22] Note, para. 10.

2. The role of the WTO DSB under WTO law

Historically WTO Agreements[23] emerged as a means of eliminating protectionism and ensuring the liberalization of the international market to substantially restore the pre-Second World War economic situation[24]. Gradually in order to maximize the benefits of WTO Agreements the system of separate agreements was institutionalized. The creation of the WTO created preconditions for shaping the predictability and clarity of international trade, as the organization not only acts as a platform for the WTO Member States to negotiate the conclusion of international treaties, but also establishes a compulsory judicial dimension[25] to resolve disputes between Member States on the interpretation of the provisions of the WTO Agreements.

WTO Agreements are incomplete contracts thus WTO "courts" have the duty to "complete" said agreements and to add the missing information[26]. The WTO function of dispute settlement and accordingly the function of interpreting WTO Agreements is formally delegated to the WTO DSB, which has the authority to establish panels, adopt panel and Appellate Body reports.[27] Despite the latter, the political role of the WTO DSB does not influence the essence of the dispute settlement process[28] nor does it formally create substantial legal consequences[29], thus the panels and Appellate Body act independently in the legal interpretation of WTO Agreements. Even though WTO panels and the Appellate Body are not called "courts" but *de facto* this is what they are, thus the actual function performed by the WTO panels and the Appellate Body is the judicial interpretation of WTO Agreements.[30]

The following sections emphasize the status of the WTO panels and Appellate Body as "court-like" institutions[31] and the peculiarities of the procedures of dispute settlement under WTO law.

2.1. The binary function of WTO law and WTO DSB

The binary nature of WTO Agreements are relevant to their interpretation. Said agreements may be deemed as multilateral contracts between certain parties, with the intent to regulate relations and trade related aspect that will arise in the future. On the other hand, WTO law encompasses provisions of both primary and secondary importance, meaning that the Agreements are not aimed at particular trade relations between states, but at providing general guidelines for economic cooperation between states. Furthermore, with the establishment of the WTO DSB as the judiciary arbiter, the WTO legal system may

[23] The WTO legal system consists of a variety of agreements, of which the following are relevant to the research: Marrakesh Agreement Establishing the World Trade Organization, Apr. 15, 1994, 1867 U.N.T.S. 154, 33 I.L.M. 1144 (1994) (hereinafter – Marrakesh Agreement); GATT; GATS; Dispute Settlement Rules: Understanding on Rules and Procedures Governing the Settlement of Disputes, Marrakesh Agreement Establishing the World Trade Organization, Annex 2, 1869 U.N.T.S. 401, 33 I.L.M. 1226 (1994) (hereinafter – DSU). For the purposes of the research the key WTO agreements are referred to as "WTO Agreements".

[24] BOWN, C. P. *Self-Enforcing Trade: Developing Countries and WTO Dispute Settlement*. Washington, D.C.: Brookings Institution Press, 2009, p. 11, 21 [accessed 2018-04-13]. Available online: <http://www.jstor.org/stable/10.7864/j.ctt127wbd.5>.

[25] WEILER, J. H. H. The Rule of Lawyers and the Ethos of Diplomats – Reflections on the Internal and External Legitimacy of WTO Dispute Settlement. *Journal Of World Trade,* 2001, Vol 35, p. 191, 200-201 [accessed 2018-04-11]. Available online: <https://www.kluwerLawonline.com/abstract.php?area=Journals&id=337899>.

[26] HORN, H., MAGGI, G., STAIGER, H. W. The GATT/WTO as an Incomplete Contract. 2006, p. 1, 10 [accessed 2018-04-11]. Available online: <ftp://www.cemfi.es/pdf/papers/Seminar/Giovanni06.pdf>; MAVROIDIS, P. C. Licence to Adjudicate: a Critical Evaluation of the Work of the WTO Appellate Body so far *in* HARTIGAN, J. C. *Trade Disputes and the Dispute Settlement Understanding of the WTO: An Interdisciplinary Assessment (Frontiers of Economics and Globalization, Volume 6).* Emerald Group Publishing Limited, 2009, p. 75-76; MAVROIDIS, P. C, HORN, H. Still Hazy after All These Years: The Interpretation of National Treatment in the GATT/WTO Case-Law on Tax Discrimination. *European Journal of International Law,* 2004, Vol 15, p. 54-55 [accessed 2018-04-11]. Available online: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=803822>.

[27] Art. 2(1) DSU.

[28] DAVEY, W. J. WTO Dispute Settlement: Segregating the Useful Political Aspects and Avoiding Over-Legalization *in* BRONCKERS, M., QUICK, R. *New Directions In International Economic Law: Essays in Honor of Jack H. Johnson.* Great Britain: Kluwer Law International, 2000, p. 291, 297.

[29] ROESSLER, D. Are the Judicial Organs of the WTO Overburdened? *in* PORTER, R. B. SAUVE, P. SUBRARNANIAN, A., and BEVIGLIA-ZAMPETTI A. *Efficiency, Equity, Legitimacy: The Multilateral Trading System at the Millennium*. Washington, D.C.: Brookings Institution Press, 2001, p. 323.

[30] WEILER, J. H. H. The Rule of Lawyers <...>, p. 200-201. For the purpose of the research, the judicial dimension of the WTO, consisting of panels, the Appellate body and DSB, is collectively referred to as "WTO Courts" or "Court(s)" when speaking generally.

[31] BOSSCHE, P. *The Law and Policy of the World Trade Organization,* 2008*,* p. 169–235.

be deemed as a modern independent legal system[32]. Accordingly in interpreting WTO Agreements WTO Courts must carry out their binary function. The Courts must not only interpret the Agreements so that the rights and obligations of concrete parties of the dispute would be protected[33] but they must also ensure the security and predictability to the multilateral trading system[34]. This leads to the conclusion that WTO DSB must not only merely settle the dispute between concrete parties, but in doing that the Courts must also reach such a decision that would if not promote, than at least not diminish the security and predictability of the trading system.

2.2. Legal sources under WTO law

WTO law does not foresee an exhaustive list of legal sources applicable to the interpretation of WTO Agreement and dispute settlement. Under the DSU, WTO Courts must follow the customary rules of interpretation of public international law[35] which in the context of WTO law are the rules laid down in the Vienna Convention on the Law of Treaties[36] (hereinafter – the Vienna Convention). However, the Convention does not provide an exhaustive list of possible legal sources of treaty interpretation so it can also be considered an incomplete contract[37] placing the WTO Courts in an "inconvenient" position of interpreting one incomplete contract with another incomplete contract[38]. Moreover, the Vienna Convention provides preconditions to apply supplementary means of interpretations without describing what these means could be.[39] Thus WTO Courts can decide on the means of interpretation of their choosing.[40] This WTO Agreement interpretation methodology presupposes that WTO Agreements should not be interpreted in isolation[41] and that the discretion of WTO Courts to decide on the means of treaty interpretation are not *a priori* limited by law[42].

Some authors argue that under Article 7 of the Dispute Settlement Understanding (hereinafter – DSU)[43] WTO Courts are only allowed to employ sources of WTO law[44]. Others state that Article 7 DSU provides the scope of legal sources applicable to WTO disputes and enables the Courts to apply sources beyond the WTO legal system.[45] Article 7 DSU provides, that the Court may also apply any agreements cited by the parties to the dispute, and the systemic analysis of paragraphs 1 and 3 Article 7 DSU it may be assumed that in certain cases the Court may be granted non-standard mandates to apply not only the WTO covered agreements but also other relevant sources of law. Moreover, in the practice of WTO DSB it is established that the set terms of reference under Article 7 DSU are not aimed at limiting the scope of

[32] See, *e.g.* PALMETER, D., MAVROIDIS, P. C. The WTO Legal System: Sources of Law. *The American Journal of International Law*, 1998, Vol 92, No 3, p. 466-467, 469, 471 [accessed 2018-04-12]. Available online: <http://www.jstor.org/stable/2997915>.
[33] Art. 3(2) DSU, second sentence.
[34] Art. 3(2) DSU, first sentence.
[35] Art. 3(2) DSU.
[36] Appellate Body report in *United States - Standards for Reformulated and Conventional Gasoline* adopted on 29 April 1996 WT/DS2/AB/R (hereinafter – *US-Gasoline).* United Nations, *Vienna Convention on the Law of Treaties*, 23 May 1969, United Nations, Treaty Series, vol. 1155, p. 331 (hereinafter – Vienna Convention).
[37] Appellate Body report in *US-Gasoline*.
[38] *Ibid.*
[39] Art. 32 Vienna Convention.
[40] Appellate Body report in *European Communities - Customs Classification of Frozen Boneless Chicken Cuts* adopted on 12 September 2005, WT/DS269/AB/R (hereinafter – *EC-Chicken Cuts*), para. 283.
[41] Appellate Body report in *US-Gasoline,* p. 17.
[42] Appellate Body report in *EC-Chicken Cuts,* para. 283
[43] Art. 7(2) DSU states that *Panels shall address the relevant provisions in any covered agreement or agreements cited by the parties to the dispute.*
[44] TRACHTMAN, J. P. The Domain of WTO Dispute Resolution. *Harvard International Law Journal*, 1999, t. 40, p. 342 [accessed 2018-04-12]. Available online: <https://ssrn.com/abstract=149348>. According to the author, Art. 7 DSU implies only the application of WTO law; see also MARCEAU, G. Z. Call for Coherence in International Law: Praises for the Prohibition Against "Clinical Isolation: in WTO Dispute Settlement. *Journal of World Trade*, 1999, Vol. 33, No. 5, p. 110 [accessed 2018-04-13]. Available online: <https://archive-ouverte.unige.ch/unige:28978>. G. Z. Marceau argues that the WTO DSB are prohibited from applying other sources of law than the WTO law since the jurisdiction of the WTO DSB is limited.
[45] PALMETER, D., MAVROIDIS, P. C. The WTO Legal System <...>, p. 399. The authors argue that in interpreting Art. 7 DSU legal sources of the WTO DSB can be prior GATT and WTO DSB reports, international customs and general principles of international law..

applicable sources of law and they are not aimed to exclude reference to the broader rules of customary international law in interpreting a claim.[46]

Moreover, WTO Law provides the WTO DSB with the right to seek information and technical advice from any individual or body which it deems appropriate[47] and the ability to seek information from any relevant sources[48]. The latter shows that the Courts are not limited to the isolated interpretation of WTO Agreements, but may also seek additional information and apply it in considering a particular case. *Amicus curiae*[49] briefs may be considered as one of the means of obtaining the necessary information in the case. The court reserves the right to either request an *amicus curiae* brief or to decide to accept the presented brief on the initiative of the subject when it deems it necessary[50]. The right of WTO DSB to obtain information and consultations is not limited thus providing the Court discretion to deciding on the relevant sources of WTO Agreement interpretation.

In practice the aforementioned right to obtain information and necessary consultations together with the right to determine the working procedural rules[51] may been applied, firstly, as enabling WTO Courts to depart from the proscribed procedural rules with the consent of the parties of the dispute and, secondly, as enabling the discretion of the Court to decide on the admissibility of any information or statement provided by parties of the dispute and third parties.[52] Accordingly the Courts obtain discretion to decide on applying a wider span of arguments in cases where it is deemed necessary[53] as long as it is not contrary to the WTO Agreements[54].

Many have criticized that the WTO DSB is allegedly engaging in judicial law-making.[55] Just like domestic courts, WTO Courts frequently make laws in the course of resolving disputes.[56] The main arguments of critics are that the DSB is unilaterally expanding its authority leading not only to judicial activism, but to a violation of WTO law[57] and that the activities of the WTO DSB are overlapping with the competencies of the WTO Member States in rule-making[58] accordingly undermining the basic values of the WTO[59] such as the rule of consensus in the decision making process.

In this context it must be emphasized that, firstly, judicial law-making is inherent to systems where the main treaties to interpret are incomplete in their essence[60]. Moreover, the WTO DSB has the sole discretion to adopt (or dismiss) a panel or Appellate Body report[61] thus the WTO DSB consisting of all of the WTO Member States[62] actually makes decisions on cases by adopting the reports. According to the general rule, the WTO DSB shall adopt a report unless WTO Member States reach a "negative

---

[46] Panel report in *Korea – Measures Affecting Government Procurement*, WT/DS163/R, para. 7.101, footnote No 755.
[47] Art. 13(1) DSU.
[48] Art. 13(2) DSU.
[49] Lot. *Amicus curiae* – "friends of the court". *Amicus Curiae* briefs are statements provided by subjects that are not parties of the dispute, but show a certain interest in it. The briefs may be provided at the subject's own initiative or at the request of the WTO court.
[50] Appellate Body report in *United States – Imposition of Countervailing Duties on Certain Hot-Rolled Lead and Bismuth Carbon Steel Products Originating in the United Kingdom* adopted on 10 May 2000, WT/DS138/AB/R, para. 42.
[51] Art. 12(1) DSU.
[52] Appellate Body report in *United States - Import Prohibition of Certain Shrimp and Shrimp Products* adopted on 12 October 1998, WT/DS58/AB/R, para. 105-108.
[53] Appellate Body report in *United States – Imposition of Countervailing Duties on Certain Hot-Rolled Lead and Bismuth Carbon Steel Products Originating in the United Kingdom* adopted on 10 May 2000, WT/DS138/AB/R, para. 42.
[54] *Ibid*, para. 43.
[55] WTO Dispute Settlement Body, Overview of the State of Play of WTO. Available online: <http://www.wto.org/english/tratop_e/dispu_e/dispu_e.htm>
[56] GINSBURG, T. *Bounded Discretion in International Judicial Lawmaking*, Virginia Journal of International Law, Vol 45, No 631, 2004 [accessed 2018-03-15]. Available online: <https://chicagounbound.uchicago.edu/journal_articles/1437/>.
[57] Minutes of the Meeting, WT/DSB/M/83, 7 July 2000, para. 15.
[58] Minutes of the Meeting, WT/DSB/M/258, 4 February 2009, para. 9.
[59] KELLY, P. J. *Judicial Activism at the World Trade Organization: Developing Principles of Self-Restraint,* Northwestern Journal of International Law & Business, Vol. 22, 2002, p. 355 [accessed 2018-04-15]. Available online: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1103508>.
[60] ZEITLER, H. E. *Good Faith in the WTO Jurisprudence: Necessary Balancing Element or an Open Door to Judicial Activism?* Journal of International Economic Law, Vol 8, No 721, 2005, p. 14.
[61] Art. 20 DSU.
[62] The WTO DSB consists of all the WTO member-states. WTO Agreement, Art. IV.2.

consensus" on not approving the report.[63] Therefore under certain circumstances all of the WTO Member States engage in the judicial decision-making.

Given that a certain level of judicial law-making is inherent to the WTO legal system and thus inevitable, the only possibility seems to be to create certain safeguards. The article does not intend to provide suggestions on the possible safeguards, however for the sake of the further discussion, the article notes that the aforementioned binary function of WTO DSB and the rule of "negative consensus" in dismissing panel reports could be considered such safeguards to limit judicial activism of the courts for it not to overlap with the decision-making process among the WTO Member States. However it must be emphasized, that due to the expanding digital trade market an increase in the number of disputes before the WTO DBS are likely, the WTO DSB seems to have at least the theoretical capacity to facilitate regulation of digital trade via litigation.

3. Recent WTO DSB reports in e-commerce cases

As mentioned before, the phenomenon of e-commerce was not practically relevant during the negotiations of concluding WTO Agreements[64], these services are not explicitly covered by WTO law.[65] However the WTO Member States agreed to engage in regulating e-commerce multilaterally thus stressing the importance of the Organization in regulating digital trade.

Taking into consideration of the particular state of e-commerce under WTO law becomes quite obvious that the role of WTO DSB is of crucial significance in ensuring the basic values of the WTO in the short-term until a comprehensive agreement is reached. The analysis of the WTO DSB functions and limits of its discretion provided in Section 2 of the article shows that the WTO DSB has both the duty and capacity to engage in completing an incomplete contract which the WTO Agreements. However in cases of e-commerce it becomes unclear as to the limits of the discretion of WTO Courts. Generally the WTO DSB has the duty to interpret WTO Agreements that were intentionally drafted to regulate certain aspects of trade that are presented before the DSB. However it is a quite different obligation to "interpret" treaties and in a way "insert" content into them that was not there before. Thus it is necessary to empirically analyze whether the Courts practice judicial restraint or engage in judicial law-making in e-commerce cases.

3.1. Regulating electronic gambling under WTO rules

The first dispute before the WTO DSB on e-commerce related issues was the *US-Gambling*[66] case. This dispute concerned various US measures limiting trans-border gambling and betting services. US noted that it has consistently imposed tight regulations on the remote supply of gambling[67] and the US expanded the regulatory regime for the remote supply of gambling so that it now addresses the Internet.[68] However, the dispute revolved about the US opening the gambling market in its GATS Schedule[69]. The US argued that restrictions on remote gambling services are not "quantitative limits" within the ambit of Article XVI:2[70] that was the substance of the case. US also argued that there is no reason why its nationality-neutral limitations should violate its commitments under GATS[71]. The base of the dispute was the question as to whether a prohibition on cross-border electronic supply of gambling services is a

[63] Art. 6(1), 16(4), 17(14), 22(6) DSU. The Draft Report is submitted to all WTO Member States thus the report can be dismissed is all Member States agree on the dismissal, i.e. the Member States can refuse the interpretation of the WTO DSB is they unilaterally disagree with it.

[64] Rolf H. Weber, *Digital Trade in WTO-Law – Taking Stock and Looking Ahea*d, Asian Journal of WTO & International Health Law and Policy,Vol. 5, No. 1, pp. 1–24 (2010).

[65] *Ibid.*

[66] Appellate Body Report, United States – *Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WT/DS285/AB/R (7 Apr. 2005)

[67] Appellant Submission of the United States, *US-Gambling*, pp. 2–6,

[68] *Ibid.*

[69] Appellate Body Report in *US-Gambling*, paras 84–89

[70] Scheduling Guidelines, para. 6.

[71] Appellate Body Report in *US-Gambling,* para. 83.

limitation within GATS. The Panel concluded that the prohibition, amounting to a zero quota, is a quantitative limitation and, therefore, constitutes a "limitation on the number of service suppliers in the form of numerical quotas within the meaning of Article XVI:2".[72] In addition, by prohibiting the supply of services in respect of which a market access commitment has been taken, the US measures at issue amount to a zero quota on service operations or output with respect to such services. The Appellate Body upheld the panel's finding that a measure prohibiting the supply of certain services where specific commitments have been undertaken is a limitation[73]. The stance of the Appellate Body in the case may be determined as its role in "modernizing" the WTO legal system and adopting new concepts to ensure proper interpretation of applicable Agreements in e-commerce cases[74].

3.2. Regulating online music downloads in *China-Audiovisual*

The *China-Audiovisual* case[75] concerned the online transactions of music. In its GATS Schedule China made both market access and national treatment commitments for facilitating sound recording distribution services[76] by enabling foreign suppliers to engage in joint ventures with national partners. So technically foreign subjects should enjoy national treatment, however Chinese national law[77] significantly limits the ability of foreign-invested enterprises to engage in the distribution of sound recordings by prohibiting these enterprises from engaging in their electronic distribution via the internet. China argued that online music services are a new type of service, which emerged after its accession and is different in kind from the "sound recording distribution services" committed by China, thus, not being covered by its commitments.[78]

US argued that GATS is technologically neutral as it does not contain any provisions that distinguish between the different technological means through which a service may be supplied[79]. This would mean that regardless the peculiarities of e-commerce, any provisions of WTO law may be applicable in relevant cases. US also referred to the report in the *US-Gambling* where the panel stated that a market access commitment implies the right of other Members' service suppliers to supply a service through all means of delivery, e.g. the Internet.[80] In this case the US invoked the principle of technological neutrality, however the Panel did not address or further elaborate on this issue[81]. The Appellate Body analyzed China's commitments as being formulated in generic terms arguing that Member States assume that such generic terms as sound recording and their distribution may develop through time[82].

3.3. Regulating electronic payment services

In the dispute[83] raised by US against China on regulating electronic payments US claimed that China undertook to provide both market access and national treatment for all payment and money transmission services, including credit, charge and debit cards[84]. However allegedly under the measures of China WTO Member States could only supply such services for payment card transactions

[72] Panel Report in *US-Gambling*, paras 6.338, 6.355.
[73] Appellate Body Report, *US-Gambling*, paras 258–267.
[74] PENG, S. *Regulating New Services through Litigation? Electronic Commerce as a Case Study on the Evaluation of 'Judicial Activism' in the WTO,* Journal of World Trade, Vol 48, No 6, 2014, pp. 1189–1222, p. 1210-1211.
[75] Appellate Body Report in *China-Audiovisual Services* adopted on 19 January 2010, WT/DS/363.
[76] Panel Report, *China-Audiovisual Services*, paras 7.1300–7.1311.
[77] First Written Submission of the United States of America, *China-Audiovisual Services,* para. 357
[78] First Written Submission of the People's Republic of China, *China-Audiovisual Services*, paras 389–403.
[79] First Oral Statement of the United States of America in *China-Audiovisual Services,* para. 54
[80] Appellate Body Report in *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WT/DS285/AB/R. Panel Report on *US-Gambling*, para. 6.285.
[81] Panel Report in *China-Audiovisual Services,* para. 7.1258
[82] GARDINER, R. *Treaty Interpretation,* Oxford University Press, 2008, p. 172–173.
[83] Panel report in *China – Certain Measures Affecting Electronic Payment Services* adopted 31 August 2012, WT/DS413/R (hereinafter – *China-Electronic Payment*).
[84] Panel report in *China-Electronic Payment*.

denominated in foreign currencies.[85] China also required all card-payment devices to be compatible with that entity's system[86], thus leading to the possible infringement of the commitments of China under WTO law.

In its textual analysis the Panel provided a broad definition of "all payment and money transmission service" by including the electronic payment services supplied in connection with credit, charge and debit cards, and other payment card transactions.[87] Moreover the scope of "electronic payment services" encompasses payment, money and transmission and all kinds of activities which manage, facilitate or enable the act of making a payment.[88] Thus regardless of China's arguments of its limited scope of obligations under WTO law schedules, the Panel decided on a broad definition (and thus expansion) of China's commitments.

The analysis of relevant disputes and the stance of the WTO DSB in said disputes shows that in cases of e-commerce the WTO DSB even though not fully consistently, but vigorously engages in the role of not only interpreting WTO law but also at modernizing it. In *US-Gambling* the Appellate Body exceeded its interpretative function and as it created new rights and imposed new obligations on Members, contrary to Article 3.2 of the DSU.[89] In *China-Audiovisual Services* the WTO DSB took a necessary position on the issue of whether the definition of "sound recording distribution services" is alterable and evolutionary through time. Even though lacking in legal reasoning the Appellate Body decided that the object and purpose of the GATS is to embrace all new technologies.[90] Lastly, in *China-Electronic Payments* the WTO DSB created an integrated service by reconciling the classification of electronic payment services with the commercial reality of those services. The Panel once again stressed that such an interpretation is based on the objective of progressive liberalization contained in the Preamble to the GATS[91].

Conclusions

1. During the initial negotiations of WTO Agreements e-commerce issues were not considered. Thus WTO Law formally does not cover electronic commerce. Despite the latter, WTO Member States have confidently reaffirmed their willingness to regulate e-commerce matters. However reaching a coherent multilateral agreement under the consensus of all WTO Member States is impossible in the near future. Therefore current WTO law must be applied and adapted to regulating e-commerce.

2. WTO Agreements are incomplete contracts meaning that judicial law making is inherent to the system. The analysis provides that the WTO DSB has the necessary tools and capacity to engage in modernizing WTO law by engaging in judicial-activism. The binary nature of WTO law and WTO DSB (*i.e.* to settle the dispute and to settle in such a manner that the security and predictability of the trading system would be ensured) preconditions the dispute settlement process being aimed at not only settling a concrete dispute among parties, but also at reaching a decision that is coherent and beneficial to the whole WTO legal system. Moreover, when necessary WTO DSB bodies employ legal sources that are relevant to the case and that go beyond WTO law making the law itself up to date.

3. The analysis shows that the WTO DSB is not only an instrument of dispute settlement between the parties, but also shows that WTO DSB engages in the modernization of WTO Agreements by employing means of developing or in times even expanding their discretion when needed. Given the particular state of e-commerce (as it is not generally included in WTO Agreements) the WTO DSB should be relied upon to ensure not only the just settlement of disputes, but also with ensuring the free and smooth flow of electronic trade my reinterpreting or modernizing WTO law. The WTO DSB often exceeds

[85] WEBER, R. *Electronic Payment Services – New Classifications in GATS Classification Issues*, *sic!*, 2012 [accessed 2018-04-15]. Available online: <https://www.ivr.uzh.ch/dam/jcr:ffffffff-bd6d-22cc-ffff-ffffcbb8e3f1/text_24_rolf_h_weber.pdf>.
[86] *Ibid.*
[87] Panel report in *China-Electronic Payment,* paras 7.75-7.122.
[88] WEBER, R. *Electronic Payment Services* <…>, p. 606-608.
[89] PENG, S. *Regulating* <…>, p. 1217.
[90] *Ibid,* p. 1218.
[91] Panel report in *China-Electronic Payment,* paras 7.195–7199.

its interpretative functions and relies on the "objective of progressive liberalization contained in the Preamble to the GATS" and its purpose to embrace all new technologies.

Bibliography

1. Appellate Body Report in *China-Audiovisual Services* adopted on 19 January 2010, WT/DS/363.
2. Appellate Body report in *European Communities - Customs Classification of Frozen Boneless Chicken Cuts* adopted on 12 September 2005, WT/DS269/AB/R.
3. Appellate Body report in *United States - Import Prohibition of Certain Shrimp and Shrimp Products* adopted on 12 October 1998, WT/DS58/AB/R.
4. Appellate Body report in *United States – Imposition of Countervailing Duties on Certain Hot-Rolled Lead and Bismuth Carbon Steel Products Originating in the United Kingdom* adopted on 10 May 2000, WT/DS138/AB/R.
5. Appellate Body Report in *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services* adopted on 7 April 2005, WT/DS285/AB/R.
6. Appellate Body Report in *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WT/DS285/AB/R.
7. Appellate Body report in *United States - Standards for Reformulated and Conventional Gasoline* adopted on 29 April 1996 WT/DS2/AB/R.
8. ARDINER, R. *Treaty Interpretation,* Oxford University Press, 2008.
9. BOSSCHE, P. *The Law and Policy of the World Trade Organization,* 2008.
10. BOWN, C. P. *Self-Enforcing Trade: Developing Countries and WTO Dispute Settlement*. Washington, D.C.: Brookings Institution Press, 2009, p. 11, 21 [accessed 2018-04-13]. Available online: <http://www.jstor.org/stable/10.7864/j.ctt127wbd.5>.
11. BRAGA, C. A. P. *E-Commerce Regulation: New Game, New Rules?* in *A Handbook of International Trade in Services* 459, 471 (Aaditya Matto et al. eds, 2008).
12. DAVEY, W. J. WTO Dispute Settlement: Segregating the Useful Political Aspects and Avoiding Over-Legalization *in* BRONCKERS, M., QUICK, R. *New Directions In International Economic Law: Essays in Honor of Jack H. Johnson.* Great Britain: Kluwer Law International, 2000.
13. Dispute Settlement Rules: Understanding on Rules and Procedures Governing the Settlement of Disputes, Marrakesh Agreement Establishing the World Trade Organization, Annex 2, 1869 U.N.T.S. 401, 33 I.L.M. 1226 (1994).
14. Doha WTO Ministerial 2001: Ministerial Declaration adopted on 20 November 2001, WT/MIN(01)/DEC/1.
15. FARROKHNIA, F., RICHARDS, C. The accountability challenge to e-commerce: The need to overcome the developed-developing country divide in WTO e-commerce polices, in LEONARD, L., GONZALEZ-PEREZ, M., (eds.), *Principles and Strategies to balance ethical, social and environmental concerns with corporate requirements*, 2013, Emerald Books.
16. General Agreement on Tariffs and Trade 1994, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, 1867 U.N.T.S. 187, 33 I.L.M. 1153 (1994).
17. General Agreement on Trade in Services, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M. 1167 (1994).
18. GINSBURG, T. *Bounded Discretion in International Judicial Lawmaking*, Virginia Journal of International Law, Vol 45, No 631, 2004 [accessed 2018-03-15]. Available online: <https://chicagounbound.uchicago.edu/journal_articles/1437/>.
19. H. WEBER, R. H. *Digital Trade in WTO-Law – Taking Stock and Looking Ahea*d, Asian Journal of WTO & International Health Law and Policy, Vol. 5, No. 1, 2010, pp. 1–24.
20. HAYER, J. D. The Trade of Cross-Border Gambling and Betting: The WTO Dispute between Antigua and the United States. *Duke Law & Technology Review,* 2004, Vol 13.
21. HORN, H., MAGGI, G., STAIGER, H. W. The GATT/WTO as an Incomplete Contract. 2006 [accessed 2018-04-11]. Available online: <ftp://www.cemfi.es/pdf/papers/Seminar/Giovanni06.pdf>.
22. KAMEL, R. *Emerging Markets and E-Commerce in Developing Economies*, 2008; PANAGARIYA, A. E-Commerce, WTO and Developing Countries. *The World Economy,* 2000, Vol 23, No 8, pp. 959-978.
23. KELLY, P. J. *Judicial Activism at the World Trade Organization: Developing Principles of Self-Restraint,* Northwestern Journal of International Law & Business, Vol. 22, 2002 [accessed 2018-04-15]. Available online: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1103508>.

24. MARCEAU, G. Z. Call for Coherence in International Law: Praises for the Prohibition Against "Clinical Isolation: in WTO Dispute Settlement. *Journal of World Trade*, 1999, Vol. 33, No. 5 [accessed 2018-04-13]. Available online: <https://archive-ouverte.unige.ch/unige:28978>.
25. Marrakesh Agreement Establishing the World Trade Organization, Apr. 15, 1994, 1867 U.N.T.S. 154, 33 I.L.M. 1144 (1994).
26. MAVROIDIS, P. C, HORN, H. Still Hazy after All These Years: The Interpretation of National Treatment in the GATT/WTO Case-Law on Tax Discrimination. *European Journal of International Law,* 2004, Vol 15, p. 54-55 [accessed 2018-04-11]. Available online: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=803822>.
27. MAVROIDIS, P. C. License to Adjudicate: a Critical Evaluation of the Work of the WTO Appellate Body so far *in* HARTIGAN, J. C. *Trade Disputes and the Dispute Settlement Understanding of the WTO: An Interdisciplinary Assessment (Frontiers of Economics and Globalization,* Vol 6. Emerald Group Publishing Limited, 2009.
28. Minutes of the Meeting, WT/DSB/M/258, 4 February 2009.
29. Minutes of the Meeting, WT/DSB/M/83, 7 July 2000.
30. MONTEIRO, J. A.; TEH, R. Provisions on Electronic Commerce in Regional Trade Agreements. WTO Working Paper ERSD-2017-11, 2017.
31. Ninth WTO Ministerial Conference. Draft Work Programme on Electronic Commerce – Draft Ministerial Decision adopted on 28 November 2013, WT/MIN(13)/DEC/W/1/Rev. 1.
32. PALMETER, D., MAVROIDIS, P. C. The WTO Legal System: Sources of Law. *The American Journal of International Law*, 1998, Vol 92, No 3 [accessed 2018-04-12]. Available online: <http://www.jstor.org/stable/2997915>.
33. Panel report in *China – Certain Measures Affecting Electronic Payment Services* adopted 31 August 2012, WT/DS413/R
34. Panel report in *Korea – Measures Affecting Government Procurement*, WT/DS163/R.
35. PENG, S. *Regulating New Services through Litigation? Electronic Commerce as a Case Study on the Evaluation of 'Judicial Activism' in the WTO,* Journal of World Trade, Vol 48, No 6, 2014, pp. 1189–1222, p. 1210-1211.
36. ROESSLER, D. Are the Judicial Organs of the WTO Overburdened? *in* PORTER, R. B. SAUVE, P. SUBRARNANIAN, A., and BEVIGLIA-ZAMPETTI A. *Efficiency, Equity, Legitimacy: The Multilateral Trading System at the Millennium*. Washington, D.C.: Brookings Institution Press, 2001.
37. TRACHTMAN, J. P. The Domain of WTO Dispute Resolution. *Harvard International Law Journal*, 1999, t. 40 [accessed 2018-04-12]. Available online: <https://ssrn.com/abstract=149348>.
38. United Nations, *Vienna Convention on the Law of Treaties*, 23 May 1969, United Nations, Treaty Series, vol. 1155.
39. WEBER, R. H., *Digital Trade in WTO-Law – Taking Stock and Looking Ahea*d, Asian Journal of WTO & International Health Law and Policy, 2010, Vol. 5, No. 1, pp. 1–24.
40. WEBER, R. *Electronic Payment Services – New Classifications in GATS Classification Issues*, *sic!*, 2012 [accessed 2018-04-15]. Available online: <https://www.ivr.uzh.ch/dam/jcr:ffffffff-bd6d-22cc-ffff-ffffcbb8e3f1/text_24_rolf_h_weber.pdf>.
41. WEILER, J. H. H. The Rule of Lawyers and the Ethos of Diplomats – Reflections on the Internal and External Legitimacy of WTO Dispute Settlement. *Journal Of World Trade,* 2001, Vol 35, p. 191, 200-201 [accessed 2018-04-11]. Available online: <https://www.kluwerLawonline.com/abstract.php?area=Journals&id=337899>.
42. Work Programme on Electronic Commerce, Progress Report to the 45 General Council, adopted by the Council for the Trade in Services on 19 Jul. 1999, S/L/74.
43. WTO Dispute Settlement Body, Overview of the State of Play of WTO. Available online: <http://www.wto.org/english/tratop_e/dispu_e/dispu_e.htm>
44. WTO. Declaration on Global Electronic Commerce adopted on 20 May 1998 by the Ministerial Conference, WT/MIN(98)/DEC/2.
45. WTO. Work Programme on Electronic Commerce Adopted by the General Council on 25 September 1998, WT/L/274.
46. WTO. WTO Agreements and Electronic Commerce adopted on 15 July 1998 by the General Council, WT/GC/W/90.

47. WUNSCH-VINCENT, S. The Internet, cross-border trade in services, and the GATS: lessons from US-Gambling. *World Trade Review*, 2006, Vol 5, No 3, 319-355.
48. WUNSCH-VINCENT, S. *The WTO, the Internet and Trade in Digital Products* (2006).
49. WUNSCH-VINCENT, S. *The WTO, the internet and trade in digital products: EC-US perspectives,* 2006, Bloomsbury Publishing; WUNSCH-VINCENT, S. *WTO, E-commerce, and Information Technologies,* 2004.
50. ZEITLER, H. E. *Good Faith in the WTO Jurisprudence: Necessary Balancing Element or an Open Door to Judicial Activism?* Journal of International Economic Law, Vol 8, No 721, 2005, p. 14.

TERRESTRIAL REGULATION FOR CELESTIAL SPHERE

Milto Yuliya[92]

Abstract

The time of space exploration moved ahead from its discovery to exploitation.

This transition has at its core the marketization of space.

In the heart of the moment, the attempt to take place in the fast growing competitive space market leads to increasing amount of private commercial entities changing the outer space scene, originally being public. Together with the lack of technological security it caused some outer space disturbances. As a result, the capability to respond effectively on cyberattacks is weakening because the traditional understanding of threats and security has changed. There is no firm understanding of the interrelation between space and cyber fields. The cyber vulnerability in space put into risk the earth – based critical infrastructure, its integrity and availability.

Creation of coherent flexible space and cyber security regime gives strategic opportunities to manage risks and to balance regulation especially in the absence of a global umbrella organization dealing with cyber security in space.

The emphasis in the article is made on the analysis of outer space regime and creation of a mechanism having the deterrent effect on misconduct in the abovementioned fields.

Keywords: cybersecurity, outer space framework, satellite

Introduction

For almost six decades legal scholars have been enthusiastically relishing issues arisen from the encounter of outer space.

Nowadays, when the usage of outer space and cyber space has become ubiquitous satellite industry has become a rapidly growing sector of the global economy. The article describes the role of satellites in modern life and some aspects of their regulation in the light of outer space legal framework. In addition, the article addresses the key issues of cybersecurity in conjunction with space activities.

It is an irony but there is no unitary understanding neither of outer space nor cybersecurity concepts. Bearing this in mind, the article identifies the outer space tendencies in law and international approaches to respond the deviant behavior in cyber domain.

1. "Houston, we have a problem"

The first problem is absence of explicit legal understanding of what does outer space mean.

The second problem is absence of holistic outer space regime.

During the Cold War the possible expansion of national sovereignty to outer space provoked fears that it would lead to outer space monopolization. That is why in contrary to *jus cogens* rules on complete and exclusive sovereignty over the air space of every State above its territory as declared by the Chicago Convention of 1944[93], the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (Outer Space Treaty) signed in January 1967[94] prohibits any forms of national appropriation.

Outer space has non-sovereign status and is equalized to the high seas regime, it is international in scope with no national sovereignty prevailing. Supposed, that the exemption from national appropriation would protect outer space from national colonization. Nevertheless, states did not come to an agreement concerning the limits of national sovereignty, *i.e.,* where the air space boundary is. Neither the

[92] *PhD in European Law from the University of Bologna, Italy*

[93] Convention on International Civil Aviation [1944], https://www.icao.int/publications/Documents/7300_orig.pdf.

[94] UN Treaties and Principles on Outer Space, http://www.unoosa.org/pdf/publications/STSPACE11E.pdf.

fundamental space law treaties nor the Chicago Convention provided the demarcation of states' vertical border or defined the outer space.

In a nutshell, legal debates on defining and delimitating of outer space led to development of "spatialists" and "functionalists" theoretical approaches.

The "spatialists" define that delimitation of the boundary between air space and outer space should be physically measurable. The "functionalists" doubting that air space and outer space have any natural vertical border define that the determinant is the nature of space activities and not the location.

The approach of the "functionalists" presumes that space activities should be governed by space law in all circumstances as the raison d'être of the mission has priority over the space object's geographical location at any given time. Space object from the moment it has been put in motion by a launching vehicle falls under the scope of space and not the air law even if it reached a few meters above the sea level[95].

The "spatialists" approach provides the 100km above sea level standard. This altitude has been chosen because there is a residual part of the Earth's atmosphere, where space objects can hold an orbital position around the planet. There exists a general consensus among states in relation to the region at and above the line determined by the lowest perigees of satellites placed in orbit (100 (+/ -10) km above the sea level). It is not subject to the sovereignty of underlying states and, thus, is outer space. This altitude is a flexible measure and there is no clear natural boundary between air space and outer space because the vertical demarcation follows the natural specifies of the planet's surface and the Earth is not a perfect sphere. It is a pear shaped ovoid, with the Southern hemisphere slightly bigger than the Northern one and an equatorial zone having a radius superior to polar one[96].

The description of factors to be taken into account when delimitating air and space border reveals that it cannot be defined solely by means of law, albeit it is possible to connect law with the characteristics and nature of space objects paying into account the altitude they can reach and the real purpose and circumstances of their usage. The demarcation of outer space creates legal security necessary to avoid international disputes concerning aeronautical and space activities, in particular, when using spy satellites or for the safety of national air space eventually crossed by space objects.

As early as 1967 the scientific and technological subcommittee of the United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS) conducted research on possible criteria for definition and delimitation of outer space. The conclusion was quite depressing, as stated it was not possible to identify scientific or technical criteria allowing to define precisely the outer space. Nowadays the situation has not moved too much ahead. Since none of the approaches triumphed, just in case, the legal subcommittee of the UNCOPUOS accepted the terms and positions of both "spatialists" and "functionalists".

The next problem appeared when the USSR launched the first artificial satellite in October 1957. Absence of outer space regime heated political debates concerning the outer space status. In a hurry, the international community "launched" the first set of outer space legal acts.

At the core of *corpus juris spatialis* are five fundamental binding space treaties[97]. But is there a good branch of international law without soft law provisions? Since the United Nations General Assembly adopted the resolution concerning the recognition of common interest of mankind in outer space and its use for peaceful purposes in December 1958, the peaceful use of outer space has become a benchmark for the forthcoming outer space regulation. The resolution stressed the importance of international cooperation for study and utilization of outer space considering that it promotes mutual understanding and

[95] J. N. Pelton Jr., 'Defining the Limits of Outer Space for Regulatory Purposes' (Switzerland: Springer International Publishing 2015) pp. 32-37.

[96] *Ibid*, pp. 79-82.

[97] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies entered into force on 10 October 1967; Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space entered into force on 3 December 1968; Convention on International Liability for Damage Caused by Space Objects entered into force on 1 September 1972; Convention on Registration of Objects Launched into Outer Space entered into force on 15 September 1976; Agreement Governing the Activities of States on the Moon and Other Celestial Bodies entered into force on 11 July 1984.

strengthen friendly relations among people[98]. Later the Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space of 1963 proclaimed cooperation and mutual assistance to be a principle for conducting space activities. The provisions of the Declaration detailed in the Outer Space Treaty[99], the first binding treaty of such a kind creating a general framework for space exploration, are the following.

Outer space and celestial bodies are free for exploration on a basis of equality and in accordance with international law. The activities of States in the exploration and use of outer space shall be carried on in accordance with international law, including with the Charter of the United Nations. States bear international responsibility for national activities in outer space carried on by governmental and non-governmental entities, and for assuring that national activities are in conformity with the Declaration. The activities of non-governmental entities in outer space require authorization and supervision by the State concerned. When activities are carried on by an international organization, responsibility for compliance with the principles shall be borne by the international organization and by the States participating in it. The State on whose registry an object is launched into space shall retain jurisdiction and control over such object while in outer space. Ownership of objects and their component parts launched into outer space is not affected by their passage through outer space or by their return to the Earth. Each State which launches or procures the launching of an object into outer space, and each State from whose territory or facility an object is launched is internationally liable for damage to a foreign State or to its natural or juridical persons by such object or its component parts on the Earth, in air space, or in outer space.

Since the times of adoption of the Outer Space Treaty when only states were empowered to conduct space activities, outer space appetites have grown. Geopolitical and military interests dominated at the dawn of outer space exploration gave way to commercial ones. Private entities interested in the commercial benefits the space activities could bring caught up the states in the space race.

Involvement of private actors blurred the outer space regulation as the commercialization of outer space could cause the application of private norms to outer space, originally regulated by public law. In spite of timid efforts taken by the UNIDROIT Space Protocol in 2012, they were neither enough nor effective since the Protocol, presenting a coordinated attempt of governments and private sector to attract financing to space-based services, has not been enforced[100]. Nevertheless, adoption of legal provisions by Intelsat, a globalized network, former intergovernmental satellite organization privatized in 2001, or Inmarsat established in 1979 by International Maritime Organization, another privatized international satellite organization, or by the International Telecommunication Union (ITU), has changed the outer space policy and framework. The United Nations remained no longer the leitmotif for creating the outer space regulation in spite of its universality.

The ITU legal framework differs from the United Nations' one. Developed long before the space treaties and having no focus on space, it spread its mandate to celestial field and appeared to be crucial for space activities. In 1947 by the agreement, formally enforced in 1949, the newly created United Nations recognized the ITU as its specialized agency for telecommunications.

Before coming to the description of the ITU framework one remark should be made.

Privatization and commercialization of outer space, and increasing number of emerging space technologies raising concern of cybersecurity, are crucial when analyzing the legal outer space framework. However, these phenomena do not require elaboration of new areas of law or outer space regulation. The most efficient way is to analyze general rules applicable to special regulation of outer space assets. To illustrate this statement is given an example concerning the appropriateness of a separate branch of law for regulating deals with horses. "Only by putting the law of the horse in the context of broader rules about commercial endeavors could one really understand the law about horses. Lots of cases deal with sales of horses; others deal with people kicked by horses; still more deal with the licensing

[98] UN General Assembly Resolution on peaceful use of outer space 1348(XIII) [1958], http://www.unoosa.org/pdf/gares/ARES_13_1348E.pdf.

[99] UN Treaties and Principles on Outer Space, http://www.unoosa.org/pdf/publications/STSPACE11E.pdf.

[100] UNIDROIT Protocol to Convention on International Interests in Mobile Equipment on Matters specific to Space Assets [2012], https://www.unidroit.org/overview-2012-space-assets#a1.

and racing of horses, or with prizes at horse shows. Any effort to collect these strands into a course on "The Law of the Horse" is doomed to be shallow and to miss unifying principles"[101].

Law is a conservative practice, drawing heavily on analogy and history[102]. Not underestimating the significance of outer space achievements, regulation of space objects and issues of their cybersecurity does not require revolution in legal sphere or adoption of totally new norms. In this sense, space objects as satellites do not differ too much from horses.

2. *Per aspera ad astra*

The International Telecommunication Union (ITU) currently has a membership of 193 countries and almost 800 private entities and academic institutions. The Union has legal capacity in the territory of each Member State necessary to exercise its functions and fulfill its purposes.

The International Telegraph Convention first signed in 1865, today the Constitution and Convention adopted in 1992, are binding instruments of the ITU. Member States are bound to impose the observance of these acts. According to the Preamble to the Constitution the Union fully recognizes the sovereign right of each State to regulate its telecommunication with regard to the growing importance to telecommunication for the preservation of peace and economic and social development of all States.

Since the moment it was established in 1865 as the International Telegraph Union, the organization has evolved significantly from the telegraph communication regulation to regulation of radio frequencies for space communications and direct broadcasting by satellites. This transition was caused by the increasing impact of telecommunications/ICTs that have become critical infrastructure, supporting not only communications for citizens and organizations, but other integral services as power supply, healthcare and financial services.

The ITU estimated that there were 6.8 billion mobile-cellular subscriptions by the end of 2013, almost as many as people on the planet, with a mobile-cellular penetration rate of 96%[103].

ICTs, in particular, fast access to Internet enhance economic growth, especially in less developed countries[104].

The telecommunications/ICTs[105] are used not only to bridge the digital divide and to build an inclusive information society but, *inter alia*, for global flight tracking for civil aviation[106] and monitoring and management in emergency and disaster situations[107]. In the area of climate change radio and telecommunication technologies and equipment are used for weather and climate-change monitoring. Remote-sensing applications on board satellites and other radiocommunication systems are important tools for detection of illegal deforestation, and improvement of energy efficiency[108].

---

[101] F.H. Easterbrook, 'Cyberspace and the Law of the Horse' [1996] University of Chicago Legal Forum, pp. 207-20.

[102] J. H. Sommer, 'Against Cyberlaw' [2000] Berkeley Technology Law Journal 3 Volume 15 pp. 1147-1148.

[103] 'Collection of the basic texts of the ITU' [2015] ITU Plenipotentiary Conference, http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/5.21.61.en.100.pdf.

[104] See for ex., SMART Africa Manifesto of 2013 adopted by the African Union General Assembly highlighting the need to place ICT at the centre of national socio-economic development agenda. ITU Plenipotentiary Conference Resolution 195 on implementation of Smart Africa Manifesto [2014]; 'Collection of the basic texts of the ITU' [2015] ITU Plenipotentiary Conference, http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/5.21.61.en.100.pdf.

[105] Broadcasting Service: A radiocommunication service in which the transmissions are intended for direct reception by the general public, may include sound transmissions, television transmissions or other types of transmission. Telecommunication: Any transmission, emission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems. 'Collection of the basic texts of the ITU' [2015] ITU Plenipotentiary Conference, http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/5.21.61.en.100.pdf.

[106] Determination of the position of aircraft and reporting this information to air traffic control centres. 'Resolution 185 on global flight tracking for civil aviation' [2014] ITU Plenipotentiary Conference, 'Collection of the basic texts of the ITU' [2015] ITU Plenipotentiary Conference, http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/5.21.61.en.100.pdf.

[107] 'Resolution 136 on the use of telecommunications/ICTs for monitoring and management in emergency and disaster situations for early warning, prevention, mitigation and relief' [2014] ITU Plenipotentiary Conference, 'Collection of the basic texts of the ITU' [2015] ITU Plenipotentiary Conference, http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/5.21.61.en.100.pdf.

[108] 'Resolution 182 on the role of telecommunications/ICTS in regard to climate change and the protection of the environment' [2014] ITU Plenipotentiary Conference, Collection of the basic texts of the ITU [2015] ITU Plenipotentiary Conference, http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/5.21.61.en.100.pdf.

After Sputnik I launch, it became evident that telecommunications would use satellites as part of their networks. In 1959, in response to the swift advances in radio engineering and emergence of new radio services the Administrative Radio Conference incorporated into the ITU's Radio Regulations several new definitions, including of space and earth-space services[109].

The technological progress provoked a number of political and legal problems, amid: the status of the geostationary orbit, and efforts of some equatorial states to obtain special rights to certain parts of that orbit. Besides, direct broadcasting by satellite scared many developing countries with "cultural imperialism" besiege[110]. Because of this, development of satellite communication forced the international community to elaborate adequate control measures over outer space activities.

In 1963 the Global Communications Satellite System (Intelsat) consortium started negotiations to gain international cooperation for the promulgation of arrangements for a global communications satellite commercial system. The Agreement Establishing Interim Arrangements for a Global Commercial Communications Satellite System of 1967 with more than 50 states signed it, applied to space segment of satellite communication system while earth stations remained under control and ownership of the participating states. The Agreement repeated principles of the United Nations Resolution No. 1721(XVI) providing that satellite communication should be available to the nations as soon as practicable on a global and non-discriminatory basis. The Intelsat or its successor was given competence to solve financial problems while the technical problems of orbit allocation and frequency allocation fell within the primary responsibility of the ITU[111].

The ITU was empowered to register radio-frequency assignments and space services, any associated orbital position in the geostationary-satellite orbit, and any associated characteristics of satellites in other orbits, in order to avoid harmful interference between radio stations of different countries[112].

According to Article 44 of the ITU Constitution radio frequencies and any associated orbits, including the geostationary-satellite orbit, are limited natural resources.

They must be used rationally, efficiently and economically, so that countries have equitable access to those orbits and frequencies, taking into account special needs of developing countries and the geographical situation of particular countries. The Member States shall endeavour to limit the number of frequencies and spectrum used to the minimum essential to provide in a satisfactory manner the necessary services and to apply the latest technical advances as soon as possible.

Satellite communications require coordination of physical position of satellites in outer space because there is an inherent relationship between the usage of frequencies by satellites and the positions they occupy: using the same frequency in neighboring positions results in white noise for both operators, but if satellites find themselves on opposite ends of the geostationary orbit[113] there is no risk to interference.

---

[109] Administrative Radio Conference (Geneva 1959), https://www.itu.int/en/history/Pages/RadioConferences.aspx?conf=4.85.

[110] F. von der Dunk and F. Tronchetti, 'Handbook of Space Law' (Cheltenham, UK • Northampton, MA, USA: Edward Elgar Publishing 2015) pp. 493-494.

[111] D. D. Smith, 'The Legal Ordering of Satellite Telecommunication: Problems and Alternatives' [1969] Indiana Law Journal 3 Volume 44 pp. 337-351.

[112] The ITU shall: a) effect allocation of bands of the radio-frequency spectrum, the allotment of radio frequencies and the registration of radio-frequency assignments and, for space services, of any associated orbital position in the geostationary-satellite orbit or of any associated characteristics of satellites in other orbits, in order to avoid harmful interference between radio stations of different countries; b) coordinate efforts to eliminate harmful interference between radio stations of different countries and to improve the use made of the radio-frequency spectrum for radiocommunication services and of the geostationary-satellite and other satellite orbits (Article 1 of the ITU Constitution).

[113] Geostationary orbit is circular orbit 35 786 km above the equator where satellites could remain stationary from a terrestrial perspective. If an object circles Earth faster than about 8 km/s, it becomes a satellite. It still falls under Earth's gravitational attraction but the drop is matched by the planet's curvature as the satellite moves along. It is falling but never reaches the ground. Satellites in geostationary orbit allow permanent communication links to be established by transmitting radio-frequency signals from fixed antennas. These signals are not very different from the signals used to broadcast terrestrial television, but usually have a frequency 3–50 times higher. The signal is received by a satellite, amplified and transmitted back to Earth, it can be picked up by antennas anywhere in the satellite's coverage area: a country, a region, a continent, or an entire hemisphere. Anyone with an antenna, sometimes as small as 40–50 cm in diameter, can become a direct user of the satellite. [European Space Agency, 'Orbits' [2013], https://www.esa.int/Our_Activities/Telecommunications_Integrated_Applications/Orbits.

This sophisticated coordination of frequencies and orbit resources requires a high level of international cooperation, and one of the principal ITU tasks is to facilitate intergovernmental negotiations to develop legally binding agreements between states that are later embodied into the Radio Regulations, the World's and regional plans adopted for different space and terrestrial services.

The ITU regime for coordinating satellite frequencies and orbits has undeniable worked rather well so far, but it came under pressure from various angles as a result of involvement of increasing numbers of, in particular, private commercial entities and commercialization of their activities that cause mounting pressure on the gentleman's arrangement of the ITU regime. The overcrowding of certain geostationary regions led to increasing temptation for states and other operators to short-cut or bypass the ITU coordination process in view of the political, economic and commercial interests at stake. An emerged problem is the "paper satellites" problem when states start to file requests before the final decisions before constructing a satellite in order to take an early place in the "queue". In response, the ITU implemented "administrative due diligence" regime. The proposal for allotment/assignment allows all the ITU member states other than the one requesting it to report threats of possible interference with their respective systems or those of operators falling within their jurisdiction. If such potential interference was reported, the requesting state had the primary obligation to accommodate, that usually means that it had to propose alternative frequencies (and the process could basically start all over again) or other methods by which the interference would be avoided[114].

Another consequence of outer space commercialization, *i.e.*, the increase of turnover[115] revealed the necessity to apply the WTO international trade rules to space related services. In 1994, the General Agreement on Trade in Services (GATS) extended WTO's mandate to trade in commercial services. With the establishment in 1997 of an Agreement on Basic Telecommunications Services under the Fourth Protocol to the GATS, the WTO and its GATS regime for global free trade in services started to legally impact the international satellite communications environment. Key GATS issues for satellite industry include non-discriminatory market access, open borders for competitive access, and advancing transparency in telecommunications regulation.

Satellite communication is treated as public good and public service. The Intelsat originally established this approach to offer a global public satellite communications infrastructures as it were offering an international public good and international public service in one go.

Another problem discussed further has a more technical character; it is the vulnerability of space assets to cyberthreats.

3. Falling from the clouds

Much of the World's critical infrastructure - communications, air transport, maritime trade, financial services, weather and environmental monitoring and defence systems - depends on space infrastructure. Satellites and other space assets, like any other parts of digitized infrastructure, are vulnerable to cyberattack that poses serious risks for ground-based critical infrastructure.

Cyberattacks on satellites can include jamming, spoofing and hacking attacks on communication networks; targeting control systems or mission packages; and attacks on ground infrastructure such as satellite control centres. Possible cyberthreats against space-based systems include military actions; well-resourced organized criminal elements seeking financial gain; terrorist groups wishing to promote their causes, even up to the catastrophic level of cascading satellite collisions; and individual hackers who want to fanfare their skills[116].

---

[114] F. von der Dunk and F. Tronchetti, 'Handbook of Space Law' (Cheltenham, UK • Northampton, MA, USA: Edward Elgar Publishing 2015) pp. 483-485.

[115] For ex., the annual economic benefit of the mobile Internet will be between USD 3.7 trillion and USD 10.8 trillion globally by 2025., 'Collection of the basic texts of the ITU' [2015] ITU Plenipotentiary Conference, http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/5.21.61.en.100.pdf.

[116] D. Livingstone and P. Lewis, 'Space, the Final Frontier for Cybersecurity?' [2016] International Security Department, https://reader.chathamhouse.org/space-final-frontier-cybersecurity.

In 1999, the Telegraph published that a group of hackers was suspected of seizing control of a British military communications satellite using a home computer.

In 2007, rebel independence fighters in Sri Lanka, identified by the US government as a terrorist organization in 1997, had been pirating the services of a US satellite to send radio and television broadcasts to other countries. The satellite belongs to Intelstat and its officials had to meet with technical experts and Sri Lanka's Ambassador to the US to discuss measures the company was taking to prevent the satellite's unauthorized use[117].

The US National Oceanographic and Atmospheric Administration took its Satellite Data Information System offline in September 2014 after a hacking incident, which kept weather agencies around the World from receiving forecasting data for 48 hours[118].

Technical solutions are effective means to give a timely response to space cyberthreats. Some satellite operators like Intelsat, use traditional security monitoring tools and those uniquely designed for satellites[119].

China moved further and launched the World's first quantum communications satellite into the orbit in 2016[120].

A danger foreseen is half avoided, but the international legal approach to enhance cyber security is not so forward-thinking. One of the explanations for this is blindness to the potential of nascent today technologies. "The blindness comes in two forms, one from the techies who give us the machines upon which cyberspace gets built; and the other from the regulators, who have their own special blindness to exactly what their regulation would take a way". The decisive point is timing to achieve the balance between technologies and regulation[121].

The pace at which technology evolves makes it hard, or even impossible, to devise a timely response to space cyberthreats. Humans are affected by "digital ageing". Youngers use space-based and cyber communications in ways that make it difficult for older generation and some senior decision-makers to fully understand technologies and threats. Among other factors, this leads to insufficiency of internationally agreed definitions of key terminology in cyber and space domains. This, in turn, impedes the development of multilateral arms control agreements. A blurring line between non-military and military roles in cyber and space sectors is raising dual-use technologies. Asymmetric threats in cyber and space domains, *i.e*., "offence is easier and cheaper than defence" make advanced countries vulnerable to attacks from less developed states, as well as from terrorist groups[122].

The situation is aggravated by the fact, that the established governance of cyber domain is based on traditional Westphalian sovereignty, and, though, there is a general consensus about the need for cooperation, it is difficult for nations to reach an agreement[123].

Under these circumstances, the ITU has elaborated its own approach to cybersecurity. It strengthened its role in building confidence and security in the use of ICTs and adopted ICTs security standards focusing on those areas of cybersecurity within its core mandate, notably the technical and development spheres, not including areas related to Member States' application of legal or policy principles related to national defence, national security, and cybercrime, which are within their sovereign rights, although this does not exclude ITU from developing technical recommendations.

---

[117] S. Northcutt, 'Are Satellites Vulnerable to Hackers?' SANS Technology Institute, https://www.sans.edu/cyber-research/security-laboratory/article/satellite-dos.

[118] A. Newcomb, 'Hacked in Space: Are satellites the Next Cybersecurity Battleground?' [2016] NBC News, https://www.nbcnews.com/storyline/hacking-in-america/hacked-space-are-satellites-next-cybersecurity-battleground-n658231.

[119] M. Reynaud, 'Cyber Security for Satellite Systems' [2017], https://www.observatoire-fic.com/cyber-security-for-satellite-systems-by-secgate/.

[120] Quantum entanglement is kind of sending a message in a soap bubble. If a wrong person pops it, the message goes away. A. Newcomb, 'Hacked in Space: Are satellites the Next Cybersecurity Battleground?' [2016] NBC News, https://www.nbcnews.com/storyline/hacking-in-america/hacked-space-are-satellites-next-cybersecurity-battleground-n658231

[121] L. Lessig, 'The Path of Cyberlaw' [1995] The Yale Law Journal 7 Volume 104 pp. 1747-1752.

[122] D. Livingstone and P. Lewis, 'Space, the Final Frontier for Cybersecurity?' [2016] International Security Department, https://reader.chathamhouse.org/space-final-frontier-cybersecurity.

[123] K. E. Eichensehr, 'The Cyber-Law of Nations' [2015] Georgetown Law Journal 103 pp. 321-355.

Conclusions

There are no binding acts directly regulating cybersecurity issues when conducting outer space activities. The question is: Are they necessary?

If to imagine that such an agreement would be adopted, what a time span its adoption would take?

To compare, the first binding outer space treaty, in spite of urgency in it, was adopted in about ten years since the moment states realized its necessity. It took five years for Intelsat to adopt an agreement for a global commercial communications satellite system since negotiations started.

Even if we assume that such an act would finally be enforced, would it really stop terrorist groups or hackers from cyberattacks? Instead of promoting punitive cybersecurity laws it would be more effective to modernize investigation and judicial procedures in a way allowing to speed them up.

"At the center of any lesson about cyberspace is an understanding of the role of law. We must make a choice about life in cyberspace-about whether the values embedded there will be the values we want"[124].

Cybersecurity and outer space regulation in great extent is based on values of maintaining peace and security of those domains. This idea reflects the existing framework on transparency and confidence-building measures in outer space. The United Nation Resolution on creation of a global culture of cybersecurity recognized that effective cybersecurity is not the matter of government or law enforcement, it must be achieved through prevention and supported by society[125]. Gaps in access to and use of information technologies by states can diminish effectiveness of cooperation in combating criminal misuse of information technology and in creating a global culture of cybersecurity[126].

As a bonus, cybersecurity will increase competitiveness of space assets and establish more equitable relations between producers and consumers, as it is expected to reach 60% level of individual Internet users by 2020 worldwide[127].

Bibliography

1. F. von der Dunk and F. Tronchetti, 'Handbook of Space Law' (Cheltenham, UK • Northampton, MA, USA: Edward Elgar Publishing 2015)
2. F.H. Easterbrook, 'Cyberspace and the Law of the Horse' [1996] University of Chicago Legal Forum.
3. K. E. Eichensehr, 'The Cyber-Law of Nations' [2015] Georgetown Law Journal 103.
4. L. Lessig, 'The Law of the Horse: What Cyberlaw Might Teach' [1999] Harvard Law Review 2 Volume 113.
5. L. Lessig, 'The Path of Cyberlaw' [1995] The Yale Law Journal 7 Volume 104.
6. D. Livingstone and P. Lewis, 'Space, the Final Frontier for Cybersecurity?' [2016] International Security Department, https://reader.chathamhouse.org/space-final-frontier-cybersecurity.
7. A. Newcomb, 'Hacked in Space: Are satellites the Next Cybersecurity Battleground?' [2016] NBC News, https://www.nbcnews.com/storyline/hacking-in-america/hacked-space-are-satellites-next-cybersecurity-battleground-n658231.
8. S. Northcutt, 'Are Satellites Vulnerable to Hackers?' SANS Technology Institute at https://www.sans.edu/cyber-research/security-laboratory/article/satellite-dos.
9. 'Orbits' [2013] European Space Agency, https://www.esa.int/Our_Activities/Telecommunications_Integrated_Applications/Orbits.
10. J. N. Pelton Jr., 'Defining the Limits of Outer Space for Regulatory Purposes' (Switzerland: Springer International Publishing 2015).

[124] L. Lessig, 'The Law of the Horse: What Cyberlaw Might Teach' [1999] Harvard Law Review 2 Volume 113 p. 548.

[125] 'Resolution on creation of a global culture of cybersecurity 57/239' [2003] UN General Assembly, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf.

[126] 'Resolution on creation of a global culture of cybersecurity and protection of critical information infrastructures 58/199' [2004] UN General Assembly, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf.

[127] 'Collection of the basic texts of the ITU' [2015] ITU Plenipotentiary Conference, http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/5.21.61.en.100.pdf.

11. M. Reynaud, 'Cyber Security for Satellite Systems' [2017], https://www.observatoire-fic.com/cyber-security-for-satellite-systems-by-secgate/
12. D. D. Smith, 'The Legal Ordering of Satellite Telecommunication: Problems and Alternatives' [1969] Indiana Law Journal 3 Volume 44.
13. J. H. Sommer, 'Against Cyberlaw' [2000] Berkeley Technology Law Journal 3 Volume 15.

Legislation

1. 'Collection of the basic texts of the ITU' [2015] ITU Plenipotentiary Conference, http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/5.21.61.en.100.pdf
2. Convention on International Civil Aviation [1944] at https://www.icao.int/publications/Documents/7300_orig.pdf.
3. 'Protocol to Convention on International Interests in Mobile Equipment on Matters specific to Space Assets' [2012] INIDROIT, https://www.unidroit.org/overview-2012-space-assets#a1.
4. 'Resolution 136 The use of telecommunications/information and communication technologies for monitoring and management in emergency and disaster situations for early warning, prevention, mitigation and relief' [2014] ITU Plenipotentiary Conference, 'Collection of the basic texts of the ITU' [2015] ITU Plenipotentiary Conference, http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/5.21.61.en.100.pdf.
5. 'Resolution 182 on the role of telecommunications/ICTS in regard to climate change and the protection of the environment' [2014] ITU Plenipotentiary Conference, 'Collection of the basic texts of the ITU' [2015] ITU Plenipotentiary Conference, http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/5.21.61.en.100.pdf.
6. 'Resolution 185 on global flight tracking for civil aviation' [2014] ITU Plenipotentiary Conference, 'Collection of the basic texts of the ITU' [2015] ITU Plenipotentiary Conference, http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/5.21.61.en.100.pdf.
7. 'Resolution on creation of a global culture of cybersecurity 57/239' [2003] UN General Assembly, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf.
8. 'Resolution on creation of a global culture of cybersecurity and protection of critical information infrastructures 58/199' [2004] UN General Assembly, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf.
9. 'Resolution on peaceful use of outer space 1348(XIII)' [1958] UN General Assembly, http://www.unoosa.org/pdf/gares/ARES_13_1348E.pdf.
10. UN Treaties and Principles on Outer Space, http://www.unoosa.org/pdf/publications/STSPACE11E.pdf

LIABILITY FOR MEDICAL MALPRACTICE AFTER IMPLEMENTATION OF ELECTRONIC HEALTH RECORD SYSTEM

Morkūnaitė Monika[1]

Abstract

We entered into the era of digitalization. Digitalization has affected many different areas, the health care sector is not an exception. The European Commission, the Government of the Republic of Lithuania emphasise that information and communication technologies, including electronic health records, applied to health and healthcare systems, can increase their efficiency, improve quality of life and unlock innovation in the health care sector. However, looking at these indicated aims, it has to be recognised that the implementation and use of electronic health records have raised many legal questions. At present, legal questions widely addressed in the jurisprudence are related to the privacy and the ownership of health data issues. Nevertheless, little attention is devoted to the dilemma of will and how the use of electronic health records will affect the application of civil liability for medical malpractice. In Lithuanian context, this question has never been analysed. Therefore, the purpose of this conference paper is to analyse whether any changes will arise in the application of civil liability for medical malpractice after implementation of electronic health record system, what quite new questions it will raise. In order to achieve the mentioned goal, first of all, the general system of electronic health records is presented, including its aim and functioning in Lithuania. Secondly, the paper analyses whether the use of electronic health records will affect the application of civil liability for medical malpractice, its assessment in courts, what quite new legal issues it will raise. Having analysed the abovementioned issue, based on the opinions of legal scholars and on the conducted researches, the paper concludes that the use of electronic health records will definitely affect the application of civil liability for medical malpractice. Two main aspects have been identified: firstly, it will provide better documentation of clinical findings. Therefore, it will allow courts to better identify the precise sequence of events in the provision of health care services. Secondly, courts will have to address quite new legal issues in applying civil liability.

Keywords: electronic health records, medical malpractice, clinical findings, diagnosis

Introduction

Digitalization has affected many different areas[2], the health care sector is not an exception. A. Skaržauskienė, V. Stokaitė, M. Mačiulienė also note that healthcare in the meantime is becoming more and more dependent on information and communication technologies **(**hereinafter, **ICTs)**[3]. **ICTs in health care sector** covers different areas: information and data sharing between patients and health service providers, hospitals, health professionals and health information networks; electronic health records; telemedicine services; portable patient-monitoring devices; operating room scheduling software; robotised surgery[4]. ICT based systems and solutions, applied in the health sector, are loosely defined as eHealth[5].

---

[1] *PhD in Law, Vilnius University Faculty of Law, with a dissertation on physician's civil liability.*

[2] Such examples can be seen looking at electronic services provision, E-justice, E-Procurement, *etc.*

[3] A. Skaržauskienė, V. Stokaitė and M. Mačiulienė, 'Empowering Patients and Professionals: Case of Lithuanian eHealth System' [2015] International Journal of Business and Management III (1) p. 75.

[4] 'Information Regarding Digital Care and Health' [2018] European Commission, https://ec.europa.eu/health/ehealth/overview_en, accessed 20 April 2018.

[5] K. A. Stroetmann, J. Artmann, J. Dumortier and G. Verhenneman, 'United in Diversity: Legal Challenges on the Road Towards Interoperable eHealth Solutions in Europe' [2012] EJBI 8 (2) p. 3. The same meaning is applied by European Commission (European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. eHealth Action Plan 2012-2020 – Innovative Healthcare for the 21st Century [2012] COM (2012) 736 final 3). For the wider discussion regarding the general eHealth policy see M. Sogomonjan and T. Kerikmäe, 'Challenges in the eHealth Regulatory Policy' [2017] 5th International Conference of PhD Students and Young Researchers, 'How Deep is your Law? Brexit. Technologies. Modern Conflicts.' Conference Papers 367-375.

World Health Organization (hereinafter, WHO), European Union (hereinafter, EU) recognise that **ICTs** provide benefits to the health care sector.

In May 2005, the Fifty-eighth World Health Assembly adopted a resolution establishing the eHealth strategy for WHO. World Health Assembly noted that advances in **ICTs** could have the impact on health-care delivery, public health, research and health-related activities for the benefit of both – low and high-income countries. World Health Assembly urged member states: (1) to consider drawing up a long-term strategic plan for developing and implementing eHealth services in various areas of the healthcare sector, including health administration, which would encompass an appropriate legal framework and infrastructure, encourage public and private partnerships; (2) to develop the infrastructure for **ICTs** for health as deemed appropriate in order to promote equitable, affordable and universal access to their benefits, and to continue to work with information and telecommunication agencies and other partners in order to reduce costs and make eHealth successful; (3) to consider establishing and implementing national electronic public-health information systems and to improve, by means of information, the capacity for surveillance of, and rapid response to, disease and public-health emergencies[6].

EU has also emphasised the need to use **ICTs in the provision of health care services. It has been stated that ICTs,** applied to health and healthcare systems, can increase their efficiency, improve quality of life and unlock innovation in health markets[7]. European Commission has adopted eHealth Action Plan 2012-2020[8], which covers the wide range of measures for utilising and developing eHealth system in EU in order to strengthen effective prevention and health promotion practices, to foster cross-border healthcare, health security, solidarity, universality and equity[9].

These mentioned plans and intentions are not only declarative. Looking at the present situation, we can see their real implementation. Many countries around the world have implemented eHealth policies, strategies and took the measures to implement eHealth systems in their countries in order to improve the provision of medical care not only in the national states, but also in all world[10]. The Republic of Lithuania is not an exemption. In 2011 Lithuania has made the amendment to the Law on Health System of the Republic of Lithuania and adopted the legal regulation establishing eHealth system in Lithuania[11]. Lithuanian Health Strategy for 2014-2025 indicates that one of the tasks of Lithuania is to develop

---

[6] 'WHA58.28 eHealth' [2005] Fifty-eighth World Health Assembly, Preamble, para. 1, 2, 7.

[7] European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. eHealth Action Plan 2012-2020 – Innovative Healthcare for the 21st Century [2012] COM (2012) 736 final 3. European Parliament has welcomed this action plan and emphasised that eHealth has great potential and could be of benefit to the professionals involved in healthcare, to patients, informal carers and to the competent authorities themselves (European Parliament resolution of 14 January 2014 on the eHealth Action Plan 2012-2020 – Innovative healthcare for the 21st century [2014] (2013/2061(INI)) OJC 482 para. 1, 2).

[8] The first eHealth Action Plan was adopted in 2004 (European Commission. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. e-Health – Making Healthcare Better for European Citizens: An Action Plan for a European e-Health Area [2004] COM (2004) 356 final). Since then, the European Commission has been developing policy initiatives aimed at fostering widespread adoption of eHealth throughout the EU. The adoption in 2011 of the Directive on the Application of Patients' Rights in Cross Border Healthcare and its Article 14 establishing the eHealth Network, marked a further step towards formal cooperation on eHealth, with the aim to maximise social and economic benefits through interoperability and the implementation of eHealth systems. Cited: European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. eHealth Action Plan 2012-2020 – Innovative Healthcare for the 21st Century [2012] COM (2012) 736 final 3.

[9] European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. eHealth Action Plan 2012-2020 – Innovative Healthcare for the 21st Century [2012] COM (2012) 736 final 6.

[10] According to the 2016 WHO report, "From Innovation to Implementation – eHealth in the WHO European Region" 70 percent of European Member States report having a national eHealth policy or strategy. 'From Innovation to Implementation eHealth in the WHO European Region' [2016] World Health Organization Regional Office for Europe, XI. For detailed policies and strategies see: http://www.euro.who.int/en/health-topics/Health-systems/e-health/policy-and-tools/e-health-policies-and-strategies-in-the-who-european-region, accessed 20 April 2018.

[11] 13^1 Article of the Law on Health System of the Republic of Lithuania *inter alia* states that the implementation of the eHealth system of the Republic of Lithuania is coordinated and supervised by the Ministry of Health. In implementing the measures of the electronic health system of the Republic of Lithuania, State Electronic Health Services and Cooperation Infrastructure Information System is established. The manager of this information system is the Ministry of Health. All entities of national health promotion activities and enforcement, persons providing or receiving health care services and other persons, in performing statutory functions or providing services related to health activities, must use State Electronic Health Services and Cooperation Infrastructure Information System and according to the legal provisions to provide and receive data. Law on Health System of the Republic of Lithuania [1994] Valstybės žinios no. 63-1231 [1998] Valstybės žinios no. 112-3099 [dated 1 January 2018]. This provision has entered into force 1 August 2011.

Lithuanian eHealth system infrastructure and solutions and integration of the Lithuanian eHealth system into the EU eHealth area in order to ensure high quality and efficient health care oriented towards the needs of the population[12]. Now this system started to function, however many other works will have to be done[13].

eHealth system is wide and thus the object of this conference paper is devoted to a fundamental part of eHealth system – electronic health records. Such electronic health records have to change the paper based medical records and make electronic health records accessible to all health care institutions[14]. Looking at the mentioned initiatives we can see that WHO, the European Commission, the Government of the Republic of Lithuania emphasise that information and communication technologies, including electronic health records, applied to health and healthcare systems, can increase their efficiency, improve quality of life and unlock innovation in the health care sector. *A. Skaržauskienė*, *V. Stokaitė, M. Mačiulienė* also emphasise that the deployment of new ICTs has the potential to increase organisational efficiency of healthcare providers, change the processes of work organisation and create the conditions for electronic patient information exchange between healthcare providers according to the nationally agreed standards[15].

However, despite the promised mentioned benefits, there are many currently unanswered legal and ethical questions regarding the adoption and use of electronic health records[16]. Legal dilemmas widely addressed in the jurisprudence are related to the privacy and the ownership of health data issues[17]. But little attention is devoted to the dilemma of will and how the use of electronic health records will affect the application of civil liability for medical malpractice[18]. In Lithuanian context this question has never been analysed.

The purpose of this paper is to address the basic question whether any changes will arise in the application of civil liability for medical malpractice after implementation of electronic health record system, what quite new questions it will raise. In order to achieve the mentioned goal, first of all, the general system of electronic health records is presented, including its aim, functioning in Lithuania. Secondly, the paper analyses whether the use of electronic health records will affect the application of civil liability for medical malpractice, its assessment in courts, what quite new legal issues it will raise.

When writing this paper, the main research methods were comparative, systematic and analytical.

1. Electronic health record system

Before starting to analyse the impact of electronic health record system to litigation process, it is necessary to emphasise the concept of electronic health record, to look what were the main intentions

[12] Lithuanian Health Strategy for 2014-2025, Approved by Parliament of the Republic of Lithuania in 26 June 2014, decree no. XII-964 [2014] Teisės aktų registras no. 9403 para. 96.5.

[13] This can be seen from the adopted actions plans regarding implementation of eHealth system. For example: Lithuanian Health Strategy for 2014-2025, Approved by Parliament of the Republic of Lithuania in 26 June 2014, decree no. XII-964 [2014] Teisės aktų registras no. 9403, *etc.*

[14] The importance of electronic health record system in eHealth functioning is also emphasised by European Commission. Commission Recommendation (notified under document number C(2008) 3282) (2008/594/EC) on cross-border interoperability of electronic health record systems [2008] OJ L190/37 Preamble para. 2.

[15] A. Skaržauskienė, V. Stokaitė and M. Mačiulienė, *Ibid*., p. 75.

[16] D. F. Sittig and H. Singh, 'Legal, Ethical, and Financial Dilemmas in Electronic Health Record Adoption and Use' [2011] Pediatrics 127 (4) pp. 1042-1047.

[17] Not the implementation and the use of electronic record *per se* create the privacy concerns, but the possibility that these data would be assessed illegally by other individuals. The privacy issue is analysed by M. Carter, 'Integrated Electronic Health Records and Patient Privacy: Possible Benefits but Real Dangers' [2000] Med J Aust 172 (1) p. 28-30; V. L. Raposo, 'Electronic Health Records: Is it a Risk Worth Taking in Healthcare Delivery?' [2015] GMS Health Technol Assess p. 11; S. Hoffman and A. Podgurski, 'E-Health Hazards: Provider Liability and Electronic Health Record Systems' [2009] Berkeley Technology Law Journal 24:4 p. 1555-1561; K. A. Stroetmann, J. Artmann, J. Dumortier and G. Verhenneman, *Ibid*., p. 3-10; L. Zurita and C. Nohr, 'Patient Opinion: EHR Assessment from the Users Perspective' [2004] Stud Health Technol Inform 107(2) p. 1333-1336. Ownership of health data issues are analysed by MA Hall, 'Property, Privacy, and the Pursuit of Interconnected Electronic Medical Records' [2010] Iowa Law Rev. 95 pp. 631-663; *etc.*

[18] S. Hoffman and A. Podgurski, *op. cit*., p. 1527. This issue also was analysed by B. Carter, 'Electronic Medical Records: a Prescription for Increased Medical Malpractice Liability?' [2011] Vanderbilt J. of Ent. and Tech Law p. 385; S. S. Mangalmurti, L. Murtagh and M. M. Mello, 'Medical Malpractice Liability in the Age of Electronic Health Records' [2010] The New England Journal of Medicine p. 2060-2067, *etc.*

that encouraged the implementation of electronic health record system and to investigate the functioning of this system.

While looking at the legal acts and legal doctrine, it can be stated that there is no single universally accepted definition of an electronic health record[19]. In EU legal acts, the electronic health record is described as a comprehensive medical record or similar documentation of the past and present physical and mental state of health of an individual in electronic form, and providing for ready availability of these data for medical treatment and other closely related purposes. An electronic health record system is understood as the system aimed for recording, retrieving and manipulating information in electronic health records[20]. In Lithuanian legal acts, an electronic health record is emphasised as the electronic record about patient's physical or mental health status and the acts of health care services. Electronic health history is considered as a collection of patients' electronic health records from all heath care providers[21]. K. A. Stroetmann, J. Artmann, J. Dumortier, G. Verhenneman also note that when it comes to the term, the electronic health record, it is much less clear what it means, but they proposed that the electronic health record should be understood to be a shared, integrated or interlinked (virtual) record of all patients' clinically relevant health and medical data independent of when, where and by whom the data were recorded. However, in some cases, an electronic health record is understood to contain a patient's health summary as one of its core elements or artefacts[22]. Despite the different definitions, an electronic health record is generally understood as a medical record or similar documentation in electronic form and these records form the electronic health history of the patient. In the electronic health record system, medical records can be seen by all health care providers.

The aim to create the electronic medical records system and refuse paper-based documentation was the intention to ensure more effective and better treatment to the patients. European Commission recognises that such systems have the potential to achieve greater quality and security in health information than the traditional forms of health records. Interoperability of electronic health record systems should make access easier and enhance the quality and safety of a patient's care throughout the Community by providing patients and health professionals with relevant and up-to-date information while ensuring the highest standards of protection of personal data and confidentiality[23]. S. Hoffman, A. Podgurski also state that electronic health record systems can facilitate access to patients' medical records, improve the quality of care and the accuracy of treatment decisions, achieve cost savings, and promote clinical research[24]. Their use could also promote complete documentation and timely access to patient information, facilitating sound clinical decision making. Moreover, the use of electronic intermediaries may decrease transcription errors, improve communication among providers and limit the duplication of tests. Clinical-decision support systems may offer a safety net by reminding harried providers of clinical guidelines and catching errors before they cause harm[25]. The carried out studies even demonstrate that the use of electronic health records are able to reduce the amount of claims for medical malpractice[26]. Thus, it is claimed that the use of electronic health records has the potential to contribute to the safety of the patients[27]. These mentioned benefits, provision of health care services not only in one

[19] K. A. Stroetmann, J. Artmann, J. Dumortier and G. Verhenneman, *Ibid*., p. 5.

[20] Commission Recommendation (notified under document number C(2008) 3282) (2008/594/EC) on cross-border interoperability of electronic health record systems [2008] OJ L190/37 para. 3 c), d).

[21] Regulations of Electronic Health Services and Cooperation Infrastructure Information System, Approved by the Government of the Republic of Lithuania in 7 September 2011, decree no. 1057 [2011] Valstybės žinios no. 113-5318 [dated 1 January 2016] para. 4.1, 4.2.

[22] K. A. Stroetmann, J. Artmann, J. Dumortier and G. Verhenneman, *Ibid*., p. 5.

[23] Commission Recommendation (notified under document number C(2008) 3282) (2008/594/EC) on cross-border interoperability of electronic health record systems [2008] OJ L190/37 Preamble para. 3.

[24] S. Hoffman and A. Podgurski, *Ibid*., p. 1526.

[25] S. S. Mangalmurti, L. Murtagh and M. M. Mello, *Ibid*., p. 2062.

[26] Electronic health records may improve patient safety and health care quality, but the exact relationship between their adoption and settled malpractice claims is unknown. Survey of 1884 physicians in Massachusetts, using electronic health records functions, during June 1, 2005, and November 30, 2005, revealed that physicians with electronic health records appear less likely to have paid malpractice claims. A. Virapongse, DW. Bates, P. Shi, *et. al.* 'Electronic Health Records and Malpractice Claims in Office Practice' [2008] Arch Intern Med. 168 (21) p. 2362-2367. Cited according to: S. S. Mangalmurti, L. Murtagh and M. M. Mello, *Ibid*., p. 2062.

[27] S. S. Mangalmurti, L. Murtagh, M. M. Mello, *Ibid*., p. 2062.

particular health care institution or in single state, have influenced the implementation of the electronic health record system in many countries around the world. Lithuania is also implementing this system.

Talking about the situation in Lithuania, it is necessary to state that before the implementation of the electronic health record system, there was no central or unified national database of patients' medical records in Lithuania. However, for this moment in Lithuania electronic health record system is implemented as a part of the State Electronic Health Services and Cooperation Infrastructure Information System (hereinafter, ESPBI IS). The structure of the ESPBI IS consists of separate databases of patients' electronic health records, medical devices, classifiers, medical images, ePrescriptions, as well as reports and statistical information. ESPBI IS was created as a single data centre, which electronically stores medical records of each resident of the state and integrate all internal IS of healthcare institutions into a unified system. Such integration allows the creation, storage and transfer of electronic health records according to the principle "one resident – one electronic health record"[28]. In such system patient-identifiable and main data regarding patient health is provided: information on overdue illnesses, surgical procedures, allergies, demographic data, other information required by law to be provided in case of emergency care. This mentioned system allows the users of the system (patient, health service specialist, *etc.*) to see all patients' arrivals to health care institutions, their registration, medical history, manage electronic medical history, send announcements, issue parcels, manage the calendar of vaccine, introduce and review medical images, tests. This system also allows the patient to review his own, his child's and foster's medical records[29].

As it can be seen, this system is aimed to create the single data base of healthcare information and to ensure the exchange of such information among patients, healthcare professionals and institutions[30]. The medical data will be stored in one data base and therefore the information about the patient will be accessible more. Thus it can help to solve problems, that existed before implementation of electronic system, when patient applied to another health care institution and it was necessary carry out tests in order to verify patient's allergenic reactions, his/her state of health, to collect other necessary information. This electronic system creates the possibility to see necessary information about the patient, collected from all health care institutions. In such way it could contribute to cost saving, to save time of physicians and ensure more effective treatment provision to the patients as it could effectively provide health care institutions with the information needed to provide health services or to ensure the continuity of health care[31].

Looking at the present situation, it can be seen that health care institutions, serving 90 percent of all Lithuania's patients, are connected to eHealth system and can handle medical records electronically. Others are urged to connect to eHealth as soon as possible. From the 1 March 2018 in eHealth system must be handled data relating to the description of the patient's visit to health care institution, epicrisis, issuance of e. prescription, birth certificate, medical certificate of death, medical certificate of driver's medical examination[32]. Thus the functioning of the electronic health record system (eHealth system) in Lithuania is at the initial stage: now the national health care providers implement this system, the next step will be the integration of Lithuanian eHealth system into EU eHealth area[33]. That means for now the

[28] Milieu Ltd and Time Lex, 'Overview of the National Laws on Electronic Health Records in the EU Member States. National Report for Lithuania' [2014], https://ec.europa.eu/health//sites/health/files/ehealth/docs/laws_lithuania_en.pdf, accessed 20 April 2018.

[29] Procedure on the Use of Electronic Health Services and Cooperation Infrastructure Information System, Approved by the Minister of Health of the Republic of Lithuania in 26 May 2015, order no. V-657 [2015] Teisės aktų registras no. 2015-08275 [dated 20 April 2018] para. 1, 5, 54.

[30] Milieu Ltd and Time Lex, *Ibid*.

[31] Legal acts indicate and other aims of eHealth system, e.g. by using information to improve public health, quality assessment, training and research, statistics, health system management analysis. Explanatory Note of Legislative Project on the Supplement of Article 2 and Supplement I Part by III Section of Law on Health System of the Republic of Lithuania, no. 10-4863-03 [2011] Teisės aktų registras no. 10-4863-03. Lithuanian eHealth system Development Program for 2017-2025 repeats the same purposes. It indicates that the aim is also to install eHealth analytics tools that would improve the results of patient treatment, the quality of health services, the efficiency of health professionals and promote biomedical research (Article 6 of Lithuanian eHealth System Development Program for 2017-2025, Approved by Minister of Health of the Republic of Lithuania in 17 July 2017, order no. V-878 [2017] Teisės aktų registras no. 12345).

[32] 'Health Care Providers are Ready to Handle Data of Patients Electronically' [2018] Health Ministry of the Republic of Lithuania, http://sam.lrv.lt/lt/naujienos/gydymo-istaigos-jau-pasiruosusios-tvarkyti-pacientu-duomenis-elektroniniu-budu, accessed 20 April 2018.

[33] Lithuanian Health Strategy for 2014-2025, Approved by Parliament of the Republic of Lithuania in 26 June 2014, decree no. XII-964 [2014] Teisės aktų registras no. 9403 para. 117.

data can be used by Lithuanian physician and later – certain information about the patient can be obtained from the physicians in other EU countries.

Looking at the mentioned changes and functioning of the electronic health record system, it can be presumed that electronic health record systems have the potential to transform the health care system from a mostly paper-based industry to one that utilizes clinical and other pieces of information in electronic form in order to assist providers in delivering higher quality of care to their patients[34]. However, looking at the mentioned new system and its functioning, we can wonder whether any changes will arise in the application of civil liability for medical malpractice after implementation of electronic health record system, what quite new questions it will raise.

2. *Status quo* or possible changes?

Looking at the aim of electronic health record system, its functioning we have to agree with S. Hoffman, A. Podgurski who indicate that, along with the potential to enhance health outcomes, electronic health records technology may bring novel responsibilities, burdens, and complexities for medical practices[35]. This parallel can be done by looking at the history. S. Hoffman, A. Podgurski indicate that historically, medical innovations, such as anesthetics and x-rays, have generated an increased tort litigation as patients quickly came to expect better care while physicians struggled to perfect their use of challenging technologies[36] and the same phenomenon may well occur with electronic health record systems[37]. N. Menachemi, T. H. Collum also have identified potential disadvantages associated with this technology[38]. S. Hoffman, A. Podgurski emphasise that in future physicians may face medical malpractice claims that would have never emerged in the past[39]. In such context it can be wondered whether and how the introduction of electronic health records will impact application of civil liability for medical malpractice?

It can be claimed that the use of electronic health records will cause changes in applying civil liability for medical malpractice. Two main aspects can be identified: firstly, it will provide better possibilities for the courts to investigate medical malpractice claims, and secondly, courts may face quite new legal issues: questions regarding reliance on other‘s physician diagnosis, treatment decisions, questions regarding the responsibility of provision of health care services in case of malfunction of electronic health record system, *etc.* These two aspects will be discussed separately.

Firstly, looking at the present-day process of establishing civil liability for medical malpractice, it can be noted that, before the use of the electronic health record system, medical records were paper based. *V. L. Raposo indicates that* the paper file allows various kind of manipulation, since it is easy to wipe documents, delete notes in the margins or, rather, add them, as some sad judicial episodes have shown. Sometimes these manipulations are relatively easy to identify. e.g., if the handwriting of a note is different from the rest of the document, or it is written with a different colour, those facts soon generate doubts as to its veracity or the timing of the respective insertion. However, in the clinical process on paper many manipulations may go overlooked and even when identified it is almost impossible to ascertain the author, the time[40].

The same situation can also be identified in Lithuania. Lithuanian case-law gives instances when some of legally essential information about the patient’s health is missing in medical documents[41] or this

[34] N. Menachemi and T. H. Collum, 'Benefits and Drawbacks of Electronic Health Record Systems' [2011] 4 Risk ManagHealthc Policy pp. 47-55.

[35] S. Hoffman and A. Podgurski, *Ibid.*, p. 1527.

[36] J. C. Mohr, 'American Medical Malpractice Litigation in Historical Perspective' [2000] J. AM. MED. ASS‘N 283 p. 1731, 1733-34; M. F. Grady, 'Why Are People Negligent? Technology, Nondurable Precautions, and the Medical Malpractice Explosion' [1988] Nw. U. L. Rev. 82 pp. 293, 297-301, 314-15.

[37] S. Hoffman and A. Podgurski, *Ibid.*, p. 1527.

[38] N. Menachemi and T. H. Collum, *Ibid*., pp. 47-55.

[39] S. Hoffman and A. Podgurski, *Ibid*., p. 1528.

[40] V. L. Raposo, *Ibid.*

[41] G. K. v Respublikinė Panevėžio ligoninė, Case 3K-3-288/2014 [2014] Supreme Court of Lithuania; G. V. v „Šeškinės poliklinika“, Case 2A-911-464/2016 [2016] Court of Appeal of Lithuania; A. A. v Centro poliklinika, Lietuvos Respublikos sveikatos apsaugos ministerija, Case 2A-556-798/2017 [2017] Court of Appeal of Lithuania; A. B. v Alytaus apskrities S. Kudirkos ligoninė, Case 2-699-230/2015 [2015] Kaunas Regional Court; V. K., G. K., E. K., represented by V. K., v Vilkaviškio ligoninė, AAS „Gjensidige Baltic“, Case 2-1144-221/2017 [2017]

information is indicated later when it is established in the legal acts[42]. There are instances when medical records corrections are made even after the patient's death or after the provisions of health care services when the real diagnosis is known[43]. These aspects cause difficulties for the courts to evaluate whether the health care services were provided according to the standard of care, whether the civil liability should be applied for medical malpractice[44].

It can be presumed that, in part, the introduction of electronic health records could contribute to the solution of this problem. Looking at electronic health record system it can be seen that, in contrast to paper-based records, in which incomplete or illegible information is not unusual[45], electronic health record system can store virtually unlimited amounts of perfectly legible and instantly accessible records that include nearly every aspect of care, regardless of where or when it took place, all of which is "discoverable"[46]. S. S. Mangalmurti, L. Murtagh, M. M. Mello also indicate that electronic health record system records all electronic transactions, from the input of orders to time stamps of clinical activity. This information, called metadata, provides a permanent electronic footprint that can be used to track physician activity[47]. V. L. Raposo emphasises that after the implementation of electronic health record system the court will have the greater information regarding knowledge that was available to the physician. These technological possibilities of electronic health record system would allow identifying the exact time when the corrections of medical documents were made, to identify who made the changes[48]. Typically, this should bolster the defendant's ability to rely on the electronic health records when defending against a malpractice claim[49]. It could also help the plaintiff to prove this claim. It such situation the availability of metadata changes the game[50]. Thus it can be indicated that electronic health record system will provide better possibilities to evaluate the exact conduct of physician, it will allow courts to identify better the precise sequence of events in provision of health care services. Moreover, it can discourage the physician to make any corrections to medical documentation.

However, for such benefits it is essential that eHealth system would function effectively. Lithuanian Health Strategy for 2014-2025, approved by Parliament of the Republic of Lithuania, declares that one of the aim of eHealth system is to provide health practitioners with access to patient information and health information at the right place and at the right time[51]. However, there is no guarantee that such system would work effectively in all cases, particularly in transition period[52]. This possibility is also recognised by Lithuanian institutions. Lithuanian legal acts provide that in case of malfunctioning of the health care

Kaunas Regional Court; Lietuvos sveikatos mokslų universiteto ligoninės Kauno klinikos v L. K., Case 2-766-230/2017 [2017] Kaunas Regional Court; K. M. v UAB „Ortodontologika", Case 2A-1081-186/08 [2008] Vilnius Regional Court.

[42] D. P., A. P., U. P. v Centro poliklinika, Case 2A-1251/2014 [2014] Court of Appeal of Lithuania.

[43] D., A. ir U. v Centro poliklinika, Case 3K-3-299-611/2015 [2015] Supreme Court of Lithuania.

[44] G. K. v Respublikinė Panevėžio ligoninė, Case 3K-3-288/2014 [2014] Supreme Court of Lithuania; L. P. v Vilniaus universiteto ligoninės Santaros klinikos, Vilniaus miesto klinikinė ligoninė, Case 2A-733-464/2017 [2017] Court of Appeal of Lithuania.

[45] D. F. Sittig and H. Singh, *Ibid*., p. 1042-1047. For more information see: E. B. Devine, J. L. Wilson-Norton, N. M. Lawless, et al., 'Characterization of Prescribing Errors in an Internal Medicine Clinic' [2007] Am J Health Syst Pharm 64 (10) pp. 1062-1070.

[46] A. R. Millera and C. E. Tucker, 'Electronic Discovery and Electronic Medical Records: Does the Threat of Litigation Affect Firm Decisions to Adopt Technology?' (Washington DC: Federal Trade Commission 2009), www.ftc.gov/be/seminardocs/090430amiller.pdf. Cited according to: D. F. Sittig and H. Singh, *Ibid*., pp. 1042-1047.

[47] S. S. Mangalmurti, L. Murtagh and M. M. Mello, *Ibid*., pp. 2063-2064.

[48] V. L. Raposo, *Ibid*.

[49] S. S. Mangalmurti, L. Murtagh and M. M. Mello, *Ibid*., p. 2064. For example, M. M. Vigoda, D. A. Lubarsky note that the timing of entries on a paper-based record is not identifiable by a time stamp, however electronic systems time stamp all entries made to the record. Implementing electronic medical records is not simply a matter of replacing a paper form with an electronic copy. The issue of access to all of the electronic elements within the database is likely to become a highly charged issue from two perspectives: (a) accessibility of the data to the plaintiff and (b) discoverability of the data in court. In other article they note that sometimes incomplete documentation is considered as fraud, also it can be used to determine what treatment was provided. M. M. Vigoda, D. A. Lubarsky, 'The Medicolegal Importance of Enhancing Timeliness of Documentation When Using an Anesthesia Information System and the Response to Automated Feedback in an Academic Practice' [2006] AnesthAnalg 103 (1) pp. 131-136.

[50] S. S. Mangalmurti, L. Murtagh, M. M. Mello, *Ibid*., p. 2064.

[51] Lithuanian Health Strategy for 2014-2025, Approved by Parliament of the Republic of Lithuania in 26 June 2014, decree no. XII-964 [2014] Teisės aktų registras no. 9403 para 117.1.

[52] Such conclusion can be made by looking at present functioning of eHealth System ('National Audit Report 'Establishment of eHealth System' [2017] National Audit Office of Lithuania, no. VA-2017-P-900-3-12, https://www.vkontrole.lt/audito_ataskaitos.aspx?tipas=2, accessed 20 April 2018). Moreover, some parallel can be made by looking at the establishment in Lithuania the possibility to provide documents for legal procedures by using Lithuanian e-services portal "e.teismas.lt" (https://e.teismas.lt/lt/public/home/), the use of electronic cases in the courts system and looking at other instances.

institution information system and ESPBI IS, due to which it is not possible to process patient data electronically, the health care institution must ensure the recording of patient health data in written form in accordance with the procedure established by legal acts. After eliminating the malfunctions of the information system of health care institution or ESPBI IS, the patient's health records recorded in written form must be entered into the information system of health care institution or ESPBI IS, indicating that the data is presented from the equivalent of the paper document. According to the legal regulation, the data link from the paper document to the corresponding health facility is organized by the healthcare institution in the prescribed manner[53]. Looking at such possibility it can be noted that legal safeguards have to exist that in case of malfunctioning of this system physicians would not misuse their powers when transferring the information from the written form to electronic system. Only in such case the mentioned better possibility to investigate the real conduct of physician in case of possible medical malpractice situation would have the real and long-term effect.

Secondly, it can be identified that the use of electronic health records will not only impact the investigation of claims of medical malpractice, but also raise for the courts quite new legal issues.

The mentioned functioning of eHealth system reveals that all electronic health data will be held in this system: information regarding patients' diagnosis, prior tests or other information, and there is no absolute guarantee that this system will function perfectly, especially in the transition period. In legal doctrine it is identified that such amount of information and functioning of electronic system can lead to few main medical malpractice situations[54]:

I. Accessible amount of information can lead health care service providers to overlook key findings despite reliable access to documentation and lead health specialists in providing inappropriate treatment to patient and cause him damage[55].

II. As the system is quite new it can be the instances when the incorrect information appear in the medical records because of negligent health care specialists' actions; moreover, copy-and-paste mistakes can lead to misplaced information in the medical records, it can be instances when medical records are impossible to access at the necessary time because of the malfunctioning of the system[56]. Such cases can cause the negative impact to the provision of health services.

III. According to this system, all data of the patient's health will be stored in one system and this could raise another medical malpractice situation when physicians in all cases will rely on other physicians' prior test results and diagnosis and continue the medical treatment of the patient. In such cases courts will have to face the question of evaluation of the physician's overreliance on other physician's findings or opinion, and not verification of their diagnoses in the light of current findings. S. Hoffman, A. Podgurski admit that greater access to the existing diagnostic data and increased economic pressure to avoid duplication of tests could lead to errors which result from inappropriate reliance on outdated or inadequate prior testing[57]. Such cases can arise where the technician who was sloppy or not sufficiently skilled may have conducted the prior test, or the patient's condition could have changed in the intervening time[58]. Reliance on the prior test results can lead to misdiagnoses or sub-optimal treatment decisions. In such context, it would mean that physicians will face difficult decisions regarding whether to re-order expensive tests to verify diagnoses, i.e. repeat tests[59]. S. S. Mangalmurti, L. Murtagh, M. M. Mello also

[53] Procedure on the Use of Electronic Health Services and Cooperation Infrastructure Information System, Approved by the Minister of Health of the Republic of Lithuania in 26 May 2015, order no. V-657 [2015] Teisės aktų registras no. 2015-08275 [dated 20 April 2018] para. 10.

[54] Although it is necessary to recognise that some of these cases to some extent could arise and before the implementation of electronic health record system.

[55] D. F. Sitti and H. Singh, *Ibid*., pp. 1042-1047.

[56] V. L. Raposo, *Ibid*.

[57] S. Hoffman and A. Podgurski, *Ibid*., p. 1537.

[58] *Ibid.,* p. 1543. In doing such conclusion these authors refer to the conducted researches, e. g. R. J. Brenner, et al., 'Radiology and Medical Malpractice Claims: A Report on the Practice Standards Claims Survey of the Physician Insurers Association of America and the American College of Radiology' [1998] AM. J. ROENTGENOLOGY 171 pp. 19, 20-21.

[59] *Ibid.,* pp.1543-1544.

recognise that the potential medical liability risk in this situation is the temptation to copy and paste patient histories instead of taking new histories, that causes the risk of missing new information and perpetuates previous mistakes[60].

Thus courts may face these quite new legal questions regarding overlooking the essential information, reliance on other physician's diagnosis, treatment decisions, questions regarding the division of civil liability when the medical malpractice in part was caused by malfunctioning of eHealth system. Thus, how these legal issues should be solved?

The real answer to these questions will be provided by the courts when they face these legal challenges. However, some insights can be proposed.

It can be suggested that, despite the fact the electronic health record system provides the large amount of available data, it does not alter the requirements for the standard care provided by the physician. In all these instances, it is essential that the physician has his/her own responsibility in provision of health care services, thus he/she has the full responsibility to evaluate data of the patient's health: medical history, diagnoses, prior tests, and applied treatment methods. In making such analysis the courts have to take into account that the information provided to them could not have been accessible to the physician at the time of delivery of health care services. Thus, it has to be ensured that in applying civil liability for medical malpractice, the courts would evaluate only that information which was available to the physician at the time when the health care services were provided. Moreover, despite the fact that one of aims of this system is to save financial costs and make the medical documents accessible, it cannot outweigh the main aim – help the patient and secure the patient's health. Thus, in case of relying upon prior tests, it has to be evaluated whether the physician correctly relied on prior tests and diagnosis, whether it was any circumstances to repeat the test and verify the diagnosis, before continuing to provide health care services. In case of malfunctioning of eHealth system, it is necessary to draw the line between obligations of the physicians and health care institution and legal entity which are responsible for the functioning of eHealth system. The civil liability for the physicians' act or omission can be applied only in case they did not act according to the standard of care in the given situation but not for the circumstances that they could not change[61].

To sum it up, it should be noted that the electronic health record system would make health care records more accessible, enhance the quality of patient care throughout the national states and later EU by providing patients and health care providers with all relevant information. Electronic health record system will definitely make the impact on the litigation processes of medical malpractice: provide relevant documentation of health care provision process, better possibilities to identify the real conduct of the physician in case of possible medical malpractice. However, the application of electronic health record system in health care sector might also raise quite new legal issues which have to be solved by the courts. These new questions will require in applying civil liability *inter alia* to evaluate the conduct of physicians, health care institutions, and fulfilment of responsibilities of legal entities responsible for the proper functioning of eHealth system. This would require establishing the fair balance between these subjects' responsibilities.

Conclusions

WHO, the European Commission, the Government of the Republic of Lithuania emphasise that information and communication technologies, including electronic health records, applied to health and healthcare systems, can increase their efficiency and improve quality of life. It can encourage the better provision of health care services not only in the national states but worldwide.

However, despite the benefits that bring the implementation of eHealth system, we also have to recognise that the use of information and communication technologies in health care sector would also make influence to litigation of medical malpractice, raise quite new legal issues which will have to be solved by the courts.

[60] S. S. Mangalmurti, L. Murtagh and M. M. Mello, *Ibid*., p. 2062.
[61] *Ibid*., pp. 2065-2066.

Looking at the functioning of eHealth system, it can be recognised that in cases of medical malpractice the electronic health record system will provide the courts with better possibilities to identify every step of health care delivery process, identify whether and what corrections were made to medical documents, and what the real conduct of the physician was. It can contribute to better evaluation whether actions of the physician complied with the applicable standard of care.

Moreover, it can be identified that the use of electronic health records not only will make the impact for the investigation of claims of medical malpractice, but also raise quite new legal issues for the courts. The functioning of eHealth system reveals that all electronic health data will be held in this system: information regarding patients' diagnosis, prior tests or other information and there is no absolute guarantee that this system will function perfectly, especially in the transition period. Such amount of information and functioning of electronic system can lead to few quite new medical malpractice situations: when the physician will overlook certain information regarding the patient's health in the system or the physician might over rely on previously recorded patient histories, tests and diagnosis and not to collect new data, also it can raise the new legal issues of dividing liability between the physician, health care institutions and legal entities that are responsible for administration of electronic heath record system in case of malfunctioning of eHealth system. So how these issues should be solved?

One of the possibilities is to recognise that despite the fact the electronic health record system provides the greater access to the medical data, it does not alter the requirements for the standard of care applicable to the physician. In all these instances, it is essential that the physician has his/her own responsibility in provision of health care services, thus he/she has the full responsibility to evaluate data of the patient's health: medical history, diagnoses, prior tests and applied treatment methods. The fact of the available amount of information cannot change this obligation. However, it is important that in applying civil liability for medical malpractice caused in part by not evaluation certain information about the patient's health, courts would evaluate only that information which was available to the physician at the time when the health care services were provided.

Despite the fact that one aims of this system is to save financial costs and make the medical documents accessible, it cannot outweigh the main aim – provide high quality health care services. Thus, in case of relying on the prior tests, it has to be evaluated whether the physician correctly relied on the prior tests, diagnosis, whether it were any circumstances to repeat test, to verify the diagnosis before the continuing to provide health care services.

In case of malfunctioning of eHealth system, it is necessary to draw the line between obligations of the physicians, their health care institutions and legal entities that are responsible for the functioning of eHealth system. The civil liability for the physicians' act or omission can be applied only in case they did not act according to the standard of care in the given situation, but not for the circumstances that they could not change. Thus, the courts should be brave and in necessary circumstances raise the liability question of legal entities that are responsible for administration and functioning of eHealth system.

Bibliography

Legislation

1. Commission Recommendation (notified under document number C (2008) 3282) (2008/594/EC) on cross-border interoperability of electronic health record systems [2008] OJL190/37.
2. European Commission. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. e-Health – Making Healthcare Better for European Citizens: An Action Plan for a European e-Health Area [2004] COM (2004) 356 final.
3. European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. eHealth Action Plan 2012-2020 – Innovative Healthcare for the 21st Century [2012] COM (2012) 736 final.
4. European Parliament resolution of 14 January 2014 on the eHealth Action Plan 2012-2020 – Innovative healthcare for the 21st century [2014] (2013/2061(INI)) OJC 482.

5. Explanatory Note of Legislative Project on the Supplement of Article 2 and Supplement I Part by III Section of Law on Health System of the Republic of Lithuania, no. 10-4863-03 [2011] Teisės aktų registras no. 10-4863-03.
6. Fifty-eighth World Health Assembly. WHA58.28 eHealth [2005].
7. Law on Health System of the Republic of Lithuania [1994] Valstybės žinios no. 63-1231 [1998] Valstybės žinios no. 112-3099.
8. Lithuanian eHealth System Development Program for 2017-2025, Approved by Health Minister of the Republic of Lithuania in 17 July 2017, order no. V-878 [2017] Teisės aktų registras no. 12345.
9. Lithuanian Health Strategy for 2014-2025, Approved by Parliament of the Republic of Lithuania in 26 June 2014, decree no. XII-964 [2014] Teisės aktų registras no. 9403.
10. Regulations of Electronic Health Services and Cooperation Infrastructure Information System, Approved by the Government of the Republic of Lithuania in 7 September 2011, decree no. 1057 [2011] Valstybės žinios no. 113-5318.
11. Procedure on the Use of Electronic Health Services and Cooperation Infrastructure Information System, Approved by the Health Minister of the Republic of Lithuania in 26 May 2015, order no. V-657 [2015] Teisės aktų registras no. 2015-08275.

Books, articles, other publications

1. R. J. Brenner, et al., 'Radiology and Medical Malpractice Claims: A Report on the Practice Standards Claims Survey of the Physician Insurers Association of America and the American College of Radiology' [1998] AM. J. ROENTGENOLOGY 171.
2. B. Carter, 'Electronic Medical Records: a Prescription for Increased Medical Malpractice Liability?' [2011] Vanderbilt J. of Ent. and Tech Law.
3. M. Carter, 'Integrated Electronic Health Records and Patient Privacy: Possible Benefits but Real Dangers' [2000] Med J Aust 172 (1).
4. E. B. Devine, J. L. Wilson-Norton, N. M. Lawless, et al., 'Characterization of Prescribing Errors in an Internal Medicine Clinic' [2007] Am J Health Syst Pharm 64 (10).
5. M. F. Grady, 'Why Are People Negligent? Technology, Nondurable Precautions, and the Medical Malpractice Explosion' [1988] Nw. U. L. Rev. 82.
6. M. A. Hall, 'Property, Privacy, and the Pursuit of Interconnected Electronic Medical Records' [2010] Iowa Law Rev 95.
7. 'Health Care Providers are Ready to Handle Data of Patients Electronically' [2018] Health Ministry of the Republic of Lithuania, http://sam.lrv.lt/lt/naujienos/gydymo-istaigos-jau-pasiruosusios-tvarkyti-pacientu-duomenis-elektroniniu-budu, accessed 20 April 2018.
8. S. Hoffman and A. Podgurski, 'E-Health Hazards: Provider Liability and Electronic Health Record Systems' [2009] Berkeley Technology Law Journal 24:4.
9. 'Information Regarding Digital Care and Health' [2018] European Commission, https://ec.europa.eu/health/ehealth/overview_en, accessed 20 April 2018.
10. S. S. Mangalmurti, L. Murtagh and M. M. Mello, 'Medical Malpractice Liability in the Age of Electronic Health Records' [2010] The New England Journal of Medicine.
11. N. Menachemi and T. H. Collum, 'Benefits and Drawbacks of Electronic Health Record Systems' [2011] 4 Risk ManagHealthc Policy.
12. Milieu Ltd and Time Lex, 'Overview of the National Laws on Electronic Health Records in the EU Member States. National Report for Lithuania' [2014], https://ec.europa.eu/health//sites/health/files/ehealth/docs/laws_lithuania_en.pdf, accessed 20 April 2018.
13. A. R. Millera and C. E. Tucker, 'Electronic Discovery and Electronic Medical Records: Does the Threat of Litigation Affect Firm Decisions to Adopt Technology?' (Washington DC: Federal Trade Commission 2009), www.ftc.gov/be/seminardocs/090430amiller.pdf.
14. J. C. Mohr, 'American Medical Malpractice Litigation in Historical Perspective' [2000] J. AM. MED. ASS'N 283.
15. National Audit Office of Lithuania, 'National Audit Report 'Establishment of eHealth System' [2017] no. VA-2017-P-900-3-12 https://www.vkontrole.lt/audito_ataskaitos.aspx?tipas=2.
16. V. L. Raposo, 'Electronic Health Records: Is it a Risk Worth Taking in Healthcare Delivery?' [2015] GMS Health Technol Assess.

17. D. F. Sittig and H. Singh, 'Legal, Ethical, and Financial Dilemmas in Electronic Health Record Adoption and Use' [2011] Pediatrics 127 (4).
18. A. Skaržauskienė, V. Stokaitė and M. Mačiulienė, 'Empowering Patients and Professionals: Case of Lithuanian eHealth System' [2015] International Journal of Business and Management III (1).
19. M. Sogomonjan, T. Kerikmäe, 'Challenges in the eHealth Regulatory Policy' [2017] 5th International Conference of PhD Students and Young Researchers. How Deep is your Law? Brexit. Technologies. Modern Conflicts. Conference Papers.
20. K. A. Stroetmann, J. Artmann, J. Dumortier and G. Verhenneman, 'United in Diversity: Legal Challenges on the Road Towards Interoperable eHealth Solutions in Europe' [2012] EJBI 8 (2).
21. M. M. Vigoda, D. A. Lubarsky, 'The Medicolegal Importance of Enhancing Timeliness of Documentation When Using an Anesthesia Information System and the Response to Automated Feedback in an Academic Practice' [2006] AnesthAnalg 103 (1).
22. A. Virapongse, D. W. Bates, P. Shi, et. al. 'Electronic Health Records and Malpractice Claims in Office Practice' [2008] Arch Intern Med. 168 (21).
23. World Health Organization, 'Information regarding eHealth policies and strategies in WHO European Region' [2016] http://www.euro.who.int/en/health-topics/Health-systems/e-health/policy-and-tools/e-health-policies-and-strategies-in-the-who-european-region.
24. World Health Organization Regional Office for Europe, 'From Innovation to Implementation eHealth in the WHO European Region' [2016].
25. L. Zurita and C. Nohr, 'Patient Opinion: EHR Assessment from the Users Perspective' [2004] Stud Health Technol Inform 107 (2).

Cases

1. A. B. v Alytaus apskrities S. Kudirkos ligoninė, Case 2-699-230/2015 [2015] Kaunas Regional Court.
2. A. v Centro poliklinika, Lietuvos Respublikos sveikatos apsaugos ministerija, Case 2A-556-798/2017 [2017] Court of Appeal of Lithuania.
3. D., A. ir U. v Centro poliklinika, Case 3K-3-299-611/2015 [2015] Supreme Court of Lithuania.
4. D. P., A. P., U. P. v Centro poliklinika, Case 2A-1251/2014 [2014] Court of Appeal of Lithuania.
5. G. K. v Respublikinė Panevėžio ligoninė, Case 3K-3-288/2014 [2014] Supreme Court of Lithuania.
6. G. V. v „Šeškinės poliklinika“, Case 2A-911-464/2016 [2016] Court of Appeal of Lithuania.
7. K. M. v UAB „Ortodonto logika“, Case 2A-1081-186/08 [2008] Vilnius Regional Court.
8. L. P. v Vilniaus universiteto ligoninės Santaros klinikos, Vilniaus miesto klinikinė ligoninė, Case 2A-733-464/2017 [2017] Court of Appeal of Lithuania.
9. Lietuvos sveikatos mokslų universiteto ligoninės Kauno klinikos v L. K., Case 2-766-230/2017 [2017] Kaunas Regional Court.
10. V. K., G. K., E. K., represented by V. K., v Vilkaviškio ligoninė, AAS „Gjensidige Baltic“, Case 2-1144-221/2017 [2017] Kaunas Regional Court.

LEGAL AND CRIMINOLOGICAL ASPECTS OF CYBERCRIMES IN POLAND – SELECTED ISSUES

Narodowska Joannna PhD[1] and Duda Maciej PhD[2]

Abstract

In the recent years, the cybercrimes have been deemed as one of the most developing types of crime. The binding Polish Penal Code at the time of adoption in 1997 did not criminalize many of acts violating the security of cyberspace. It should also be noted that there is no legal definition of cybercrimes in Polish penal law and these types of crimes are forbidden on the ground of many different legal acts. The representatives of Polish law doctrine have divided cybercrimes into three groups: crimes against the security of digitally processed information, crimes related to the content of information and crimes related to instrumental use of networks and computer systems. New forms of *modus operandi* of perpetrators associated with the use of the Internet, have forced the legislator to criminalize these types of behaviours. Examples of neocriminalization in Polish criminal law are grooming or cyberstalking. In addition, there is a large group of crimes in the Polish Criminal Code that can be committed both in the virtual and real world, such as hate speech, fraud or theft. The aim of the paper is to present selected issues of cybercrimes which are the most often committed in Poland. The authors analyze cybercrimes from the perspective of criminal law and criminology. The attention is paid to crimes such as hate speech, child pornography, grooming, cyberstalking, identity theft, online fraud, money laundering, online gambling. The paper indicates issues of etiology, phenomenology and possibilities of counteracting cybercrimes, as well as presents the criminal liability for cybercrimes on the ground of Polish legislation.

Keywords: cyberspace, cybercrimes, criminal liability, Polish penal code, criminology

Introduction

The phenomenon of cybercrimes has escalated at the turn of 20th and 21st century with the development of network and technology, in particular the Internet, and is a serious threat to the internal security of states. It requires a reaction to this pathology at the level of criminal law legislation and criminal policy. The disruption of the functioning of cyberspace can have a significant impact on economic and social relations in the public and private sectors. The risks of infringement in cyberspace might come from various sources, including deliberate attacks, in the form of distribution of malware, hacking ICT systems or blocking service provision. The perpetrators of the cybercrimes can be both individuals and criminal groups acting for financial gains, for terrorist motives or other personal purposes as well as the groups that are supported by foreign states. The aim of cybercrimes is to obtain certain information, cause political or economic destabilisation, or to induce social discontent.

The first definition of cybercrime (called then "computer crime") was formulated in 1973 by R. von zur Mühlen, who described it as deeds in which a computer is either a tool or an object of an attack. The other expressions that are commonly used for this phenomenon are: cybercrimes, computer crimes, computer-related crimes, high-tech crimes, Internet crimes. It is obvious, that not only computers are used for communication in cyberspace. Therefore, it was necessary to update the definition of cybercrimes.

It should be highlighted that the Polish criminal law does not provide a legal term of such crimes. At the same time, there are many definitions of cybercrimes created by representatives of doctrine. In the Polish criminological literature, the general definition of cybercrimes refers to the acts associated with the

[1] Holds PhD in Criminal Law with dissertation on „Crimes of poaching in inland waters. A legal and criminological study" (2015). Assistant Professor at Department of Criminology and Criminal Policy at the Faculty of Law and Administration at the University of Warmia and Mazury in Olsztyn. E-mail: joanna.narodowska@uwm.edu.pl.

[2] Holds PhD in Criminology with a dissertation on „Hate crimes. A legal and criminological study" (2015). Assistant Professor at Department of Criminology and Criminal Policy at the Faculty of Law and Administration at the University of Warmia and Mazury in Olsztyn. E-mail: maciej.duda@uwm.edu.pl.

use of IT systems or networks in order to violate any goods protected by criminal law. The continuous technological development is not conducive to formulate a stable, holistic definition of cybercrimes. It shall be agreed that because of changing *modus operandi* of perpetrators, the legislator has been forced to penalize new forms of illegal acts committed in the cyberspace[3]. The other divisions of cybercrimes might refer to: object of illegal acts (the similar groups of crimes are included in a particular chapter of the Polish Penal Code e.g. offences: against the Republic of Poland, against the public safety, against the sexual liberty and decency, against honour and personal inviolability, against the protection of information, against the credibility of documents, against property ect.)[4], crimes associated with use of violence (e.g. cyberterrorism, cyberstalking, cyberbullying, child pornography) or without use of violence (e.g. cybertheft, cyberfraud, cyberforgery, cyberintrusion, cyberdestruction)[5].

Currently, the main directions of cybersecurity in Poland are indicated in the program entitled "National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022"[6]. The government document was prepared by the group composed of representatives of the Minister of Digital Affairs, Minister of Defence and Minister of the Interior and Administration and representatives of the Internal Security Agency, the Government Centre for Security and the National Security Bureau. The aim of this program is to ensure a high level of security of the public sector, private sector and citizens in a process of the provision or use of essential services and digital services. According to strategy, in 2022 Poland shall be more resilient to attacks and threats from the cyberspace. In the field of international cooperation for the security of cyberspace, the program emphasizes the partnerships with the countries of the region, including the Visegrad Group and the Baltic Sea States as well as with organizations such as the European Union (EU), The North Atlantic Treaty Organization (NATO), the United Nations (UN) and the Organization for Security and Co-operation in Europe (OSCE). The program defines the „cyberspace" as the space of processing and exchanging information created by ICT systems, including relations between them and relationships with the users. In addition, the basic terms referring to cyberspace were defined in pervious, non-binding strategy for 2011-2016[7]. The notion of „cybercrime" should have been understood as the prohibited act committed in the cyberspace and term „cyberattack" as the intentional disturbance in proper functioning of the cyberspace.

The quoted definitions are very general and do not specify exactly what types of deeds can be included in the category of cybercrimes. Undoubtedly, the common element of them is the place of their committing, which is the cyberspace. However, due to the cross-border character of these crimes, there might be some difficulties in locating the place of their commitment. The place of acting of perpetrator may be different than the result of his behaviour. On the basis of article 6 of the Polish Penal Code, a prohibited act is deemed to have been committed at the place where the offender acts or fails to perform an action that the offender is obliged to perform, or where the results of the prohibited act take place, or are intended by the offender to take place. The determination of the place is significant for procedural rules as it decides which jurisdiction would apply to perpetrator of cybercrime. It should be noted that there is no uniform model in the global dimension. In Polish doctrine, the prevailing opinion is that, in case of cybercrimes, the important role in determining the jurisdiction performs criteria: where the perpetrator acts and where is located the computer system (system as the object of attack or system as *instrumenta sceleris*)[8].

[3] M. Siwicki, 'Podział i definicja cyberprzestępstw' [2012] Prokuratura i Prawo 7-8 pp. 241-251.

[4] S. Kotecka, 'Strategie i dobre praktyki dotyczące bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych i ochrony przed ich nieuprawnionym ujawnieniem' in J. Gołaczyński (red.), 'Wybrane dobre praktyki w zakresie usług elektronicznych' (Warszawa: C.H. Beck 2016) pp. 449-459.

[5] B. Hołyst and J. Pomykała, 'Cyberprzestępczość, ochrona informacji i kryptologia' [2011] Prokuratura i Prawo 1, p. 11.

[6] Ministerstwo Cyfryzacji, 'Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022' (Warszawa: Ministerstwo Cyfryzacji 2017) p. 28.

[7] Ministerstwo Spraw Wewnętrznych i Administracji, 'Rządowy program ochrony cyberprzestrzeni na lata 2011-2016' (Warszawa: Ministerstwo Spraw Wewnętrznych i Administracji 201) p. 6.

[8] See more in: M. Nawrocki, 'Miejsce popełnienia czynu zabronionego' (Warszawa: C.H. Beck 2016) and M. Sowa, 'Odpowiedzialność karna sprawców przestępstw internetowych' [2002] Prokuratura i Prawo 4 pp. 74-75.

A division of cybercrimes is consisted in the Council of Europe Convention on Cybercrime and distinguishes four groups of crimes[9]:

- offences against confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, data interference, system interference, misuse of devices),
- computer-related offences (computer-related forgery, computer-related fraud),
- content-related offences (offences related to child pornography),
- offences related to infringement of copyright and related rights.

Analogously to above definition, the Polish doctrine has divided cybercrimes into three main groups[10]:

- crimes against the security of digitally processed information,
- crimes related to the content of information (content-related offences),
- crimes related to instrumental use of networks and computer systems.

Due to continuous development of the phenomenon of cybercrime as well as the necessity of implementing international and EU laws, the Polish legislator has been forced to amend the criminal law and neocriminalize new forms of behaviours[11]. On the ground of the Polish criminal law, the crimes committed in the cyberspace are penalized in more than hundred legal acts. However, the basic regulations are stipulated in: Penal Code[12], Personal Data Protection Act[13], Law on Copyright and Related Laws[14].

Crimes against the security of digitally processed information

The first group of cybercrimes is crimes against the security of digitally processed information, also called computer crimes *sensu stricto*. These crimes are gathered in chapter XXXIII of Polish Penal Code entitled "Offences against the Protection of Information". Not every crime included in this chapter can be classified as a computer crime *sensu stricto* (i.e. article 265 k.k. and 266 k.k.). Nevertheless, if they are committed in cyberspace, it would be possible to assign them to other groups of cybercrimes. These cybercrimes are generally the equivalent of the acts identified in the first group of the Convention on Cybercrimes against confidentiality, integrity and availability of computer data and systems. According to Polish regulations, the offences against the security of digitally processed information are:

- illegal access to information and computer system (article 267 § 1 and 2 k.k),
- illegal access to information with the use of audio, visual or other special equipment, (article 267 § 3 k.k.),
- data interference (article 268 k.k., 268a k.k.),
- system interference (article 269 k.k., 269a k.k.),
- misuse of devices (article 269b k.k.).

It should be noted, that most of these crimes came into the force after Poland's accession into the European Union in 2004. The latest regulation was introduced to criminal legislation just one year ago, in 2017 and is called unpunishability clause. This principle refers to the perpetrator who performs "non-contractual security test" of computer system. In accordance with article 269c k.k., anyone who accesses to computer system or sabotage computer system, in order to secure computer system or telecommunication network, or in order to develop such method of protection shall not be punished under criminal law. In addition, the perpetrator must promptly inform the disposer of the system or network about detection of threats. Furthermore, his action could not have caused any damage[15].

[9] Council of Europe Convention on Cybercrime, Budapest 23.11.2001, Council of Europe, European Treaty Series No. 185.
[10] M. Siwicki, 'Cyberprzestępczość' (Warszawa: C.H. Beck 2013) p. 5.
[11] M. Zbrojewska, S. Biedroń, T. Pański and K. Bajon-Stolarek, 'Prawnokarne aspekty zjawiska cyberprzestępczości' [2016] Palestra 34 p. 264.
[12] Act of 6.06.1997 – Penal Code, Journal of Laws, 2017, No. 2204 with amendments, further quoted also as "k.k.".
[13] Act of 29.08.1997 – Personal Protection Data, Journal of Laws, 2016, item 922 with amendments.
[14] Act of 4.02.1994 – Law on Copyright and Related Rights, Journal of Laws, 2017, item 880 with amendments.
[15] A. Grześkowiak and K. Wiak (ed.), 'Kodeks karny. Komentarz' (Warszawa: C.H. Beck 2018) p. 1270.

The illegal access to information and computer system is also called "hacking" (article 267 § 1 and § 2 k.k.). The legislator penalized acts of unauthorised access to any information or to any part of a computer system by breaching electronic, magnetic or other special protection. The criminal provisions of above article do not determine what kind of information is protected. Generally, it can be any information which is not designed for knowledge of the perpetrator, e.g. personal data (name, address of residence, identity number), computer passwords, access codes, number of bank account, confidential commercial or corporate information, provided that they are encrypted or secured. Even a free use of paid services displays the characteristic of hacking. *Modus operandi* of the offender consists in physical interaction with computer or remote connection with computer systems. There might be different purposes of illegal access to information. As a curiosity, it can be added that criminologists have introduced to literature new notion "hacktivism" which is politically motivated hacking[16].

Another form of illegal access to information is sniffing (article 267 § 2). Anyone who installs or uses any audio, visual or other special equipment in order to acquire information is liable to penalty. The criminal liability does not depend on whether the perpetrator managed to acquire the information. Forbidden is even installing and using spy equipment and programs. Examples of spy programs are: sniffer, keyloggers, cookies, web bug, browser hijacker, web crawler. Nevertheless, there are some exceptions to this prohibition. On the basis of law, indicated government services are allowed to track user's of computer systems[17].

The acts against data interference consist of different types of *modus operandi* of the offender. The difference between them refers to the object of violation, which is either essential information (article 268 k.k.) or database (article 268a k.k.). The penalized ones are intentional, unauthorised acts of destroying, damaging, deleting, altering of the above objects, as well as preventing the automatic collection and transmission of data.

The provisions of the Polish Penal Code distinguish two types of acts against system interference. Article 269 k.k. concentrates on particular objects, that are important for the functioning of the state. Criminal liability concerns for destroying, deleting, changing the records on computer storage that are crucial for national defence, transport safety, operation of the government authority or local government, as well as for interfering or preventing the automatic collection and transmission of such information. Whereas provisions of the article 269a k.k. penalize significant, unauthorised disruption of computer system or telecommunications network by transmitting, damaging, deleting, destroying or altering information data.

The last prohibition of this group is associated with misuse of devices (article 269b k.k.). Forbidden are acts of creating, obtaining, transferring, allowing the access to hardware or software, including also computer passwords, access codes or other data enabling access to the information collected in the computer system or telecommunications network, adapted to commit offences against the security of digitally processed information.

According to criminal statistics, crimes included in this group are committed relatively seldom. In 2016, there were: article 267 k.k. – 2718 crimes, article 268 k.k. and article 268a k.k. – 789 crimes, article 269 k.k. – 6 crimes, article 269a k.k. – 38 crimes, article 269b k.k. – 39 crimes.

Crimes related to the content of information

The second group of cybercrimes are computer-related offences. The feature of them is the content of information which is forbidden by law. The most often committed cybercrimes of this group are: child pornography, grooming, slander, insult, as well as propagating racism, fascism, xenophobia and discrimination of group or individuals because of their national, ethnic, race or religious affiliation[18].

Pursuant to Convention on Cybercrime (2001) the term „child pornography" refers to pornographic material that visually depicts: a) a minor engaged in sexually explicit conduct, b) a person appearing to

[16] F. Radoniewicz, 'Odpowiedzialność karna za przestępstwo hackingu' [2013] Prawo w działaniu 13 pp. 121-173.
[17] M. Szmit, I. Politowska, 'O artykule 267 Kodeksu Karnego oczami biegłego' [2007] e-biuletyn CBKE, pp. 1-13.
[18] See: M. Siwicki, 'Nielegalna i szkodliwa treść w Internecie' (Warszawa: Wolters Kluwer 2011).

be a minor engaged in sexually explicit conduct, c) realistic images representing a minor engaged in sexually explicit conduct[19]. Furthermore, the Directive of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography defines such terms as "child", "age of sexual consent", "child pornography", "child prostitution", "pornographic performance"[20].

Generally, in the Polish legal system the pornography is legal. On the other hand, there are some unacceptable behaviours referring to pornography that are penalized in provisions of the Polish Penal Code. According to the article 202 § 1 k.k. anyone who publicly displays pornographic material in such a manner that it is imposed upon a person against their wish is liable to a fine, the restriction of liberty or imprisonment for up to two years. The other types of forbidden acts are: child pornography, pornography associated with the use of an animal or the use of violence (article 202 § 3 k.k.). The Polish criminal law also bears criminal liability for the following acts related to child pornography (pedo-pornography):

- preserving of pornographic material with the participation of a minor under the age of 15 (article 202 § 4 k.k.),
- importing, storing or obtaining access to pornographic materials with the participation of a minor under the age of 15 (article 202 § 4a k.k.),
- producing, distributing, presenting, storing or possessing pornographic materials that present a created or processed image of a minor involved in a sexual act (article 202 § 4b k.k.),
- participating in presentation of pornographic materials with the participation of a minor with the purpose of achieving sexual satisfaction (art. 202 § 4c k.k.).

It should be noted that the term of minor refers to any person under the age of 18. However, there are some interpretative doubts caused by the problem of so-called "sham pornography" (generated, simulated) which is a kind of pornography that presents created or processed image of a minor. The regulations penalizing this kind of pornography have been adopted by the majority of European countries (among others in France, Great Britain, Germany, the Netherlands, Sweden)[21].

The criminal statistics conducted by the Polish Police indicate that in the last decade the number of reported crimes related to child pornography has increased and oscillates at the level between 500 to 2500 per year. The methodology of this statistic does not allow stating what per cent of these crimes is committed in the cyberspace. Nevertheless, in criminological literature, it is deemed that even 20 per cent of all pornography materials accessible online might be the child pornography[22].

Recently, the representatives of criminology have paid attention to so-called "camming", which is popular among the youth. Foregoing phenomenon consists in obtaining material or personal benefits in exchange for making available and distributing through the Internet pornographic material with own participation. Therefore, such act can be considered on the borderline of pornography and prostitution. The particularly popular websites offering the online sex performances are: showup.tv, showcam.com, liveshow.pl. Limited possibilities of verifying online users' identity facilitate access to websites for minors. Therefore, this kind of websites might contain child pornography and might enable pedophiles to contact with potential victims.

The offence of so-called grooming is the example of neocriminalization in the Polish criminal law. This type of cybercrime came into a force in 2009 as consequence of implementation the provisions of Convention on the Protection of the Children against Sexual Exploitation and Sexual Abuse (2007)[23].

In criminological sense the phenomenon of „sexual grooming is a process by which a person or person(s) prepare a child, significant adults and the environment for the abuse of this child. Specific goals

[19] Council of Europe Convention on Cybercrime, Budapest 23.11.2001, European Treaty Series No. 185.

[20] Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (Official Journal of the European Union L 335/1 from 17.12.2011).

[21] Szerzej na ten temat w: M. Skórzewska-Amberg, 'Karalność pornografii dziecięcej w polskim kodeksie karnym' in S. Pikulski and M. Romańczuk-Grącka (ed.), 'Granice kryminalizacji i penalizacji' (Olsztyn: Elset 2013) pp. 333-339.

[22] M. Siwicki, 'Nielegalna i szkodliwa treść w Internecie' (Warszawa: Wolters Kluwer 2011) p. 35.

[23] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse from 25th October 2007 (Journal of Laws 2015, item 608).

include gaining access to the child, gaining the child's compliance and maintaining the child's secrecy to avoid disclosure. The impact of this process exists long after the actual abuse, can affect a child's recovery and it serves to strengthen the offender's abusive pattern, as it may be used as a means of justifying or denying of their action"[24]

The article 200a of Polish Penal Code penalizes two types of behaviour associated with the use of information system or telecommunication network referring to grooming:

- establishing a connection with a minor under the age of 15 in order to commit the offence specified in article 197 § 3 section 2 k.k. (rape of a minor under the age of 15) or article 200 k.k. (sexual intercourse with a minor under the age of consent) as well as for the purpose of producing or preserving pornographic materials, with the intention of using deceit or an illegal threat to meet with him or her (article 200a § 1 k.k.),
- making an offer to a minor under the age of 15 of sexual intercourse, submission or performance to another sexual act, or participation in the production or preservation of pornographic material (article 200a § 2 k.k.).

From the statistical perspective grooming is a crime disclosed relatively seldom. In the years 2010-2016 there were committed accordingly 6, 66, 74, 132, 129, 275, 339. The above criminal statistics indicate that every year, there is a noticeable increase in this crime. It should be emphasized, that grooming because of its characteristics can be committed only in the cyberspace.

The term of „hate speech' is defined in Recommendation no. R 97(20) of the Committee of Ministers to member states on "hate speech" and should be understood as "all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance, including: intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrants and people of immigrant origin"[25].

The Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems of Council of Europe from 2003 determines the notion of "racist and xenophobic material" as "any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors" [26].

Hate speech is a specific form of so-called hate crimes. In the Polish criminal law, there are only three types of crimes recognized as hate crimes *sensu stricto*. These offences can be committed in the form of verbal acts (acts of speech) or in the form of acts (behaviours). The feature of hate crimes committed in cyberspace is that the perpetrator does not have to contact in person with the victim. These acts consist in:

- the use of illegal threats against a group or a person because of its/his/her belonging to national, ethnic, racial, political or religious affiliation or because of the lack of religious denomination (article 119 k.k.),
- propagating fascist or other totalitarian regime or encouraging to hatred against national, ethnic, racial, religious distinctions or the lack of religious denomination (article 256 k.k.),
- public insulting a group or person because of its/his/her belonging to national, ethnic, racial, religious affiliation or because of the lack of religious denomination (article 257 k.k.).

According to criminal statistics of Polish General Prosecutor's Office, in 2016 there were 1631 criminal proceedings conducted against perpetrators of hate speech. It is 0,15 per cent of all criminal proceedings in that year. Unfortunately, the reports say that the dynamics of hate crimes increases. The detection of this type of crime was 24%. Almost one third of them was committed in the capital of the

[24] S. Craven, 'Deconstructing perspectives of sexual grooming: implications for theory and practice' (Coventry: Coventry University 2009) pp. 215-216.

[25] Recommendation no. R 97(20) of the committee of ministers to member states on "hate speech" (Adopted by the Committee of Ministers on 30 October 1997at the 607th meeting of the Ministers' Deputies).

[26] Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, 28.I.2003, Council of Europe, European Treaty Series No. 189.

country – Warsaw. Among all hate crimes committed in Poland in 2016, nearly half of them took place in the cyberspace (701 cases)[27]. Hate crimes in Poland are usually aimed against Muslims, Jews, Roma and Negroes. The criminologists have also observed that the number of offences against Jews and Romes has recently decreased. At the same time, the number of hate crimes against Muslims and refugees has rapidly increased which is undoubtedly related to the phenomenon of migration[28].

The cyberspace has become a new dimension of contemporary society. Its main advantages are relative anonymity and global sphere. It allows propagating hate speech by overcoming geographical and language barriers. The Internet is also particularly attractive for extremist organizations. They use it to propagate radical ideas, communicate with members and recruit new supporters.

The examples of use of the Internet by extremist groups include:

- Redwatch website containing photographs and personal data of " traitors of the white race"[29],
- computer games with racist contents such as "Ethnic cleansing", "Kill the Nigger", "Manager in the concentration camp" [30],
- placing on the social networks recordings and video clips with so-called right-wing music[31],
- Internet sales of radical propaganda materials, e.g. books, CDs, video recordings, clothes, flags, jewellery[32],
- propaganda of Muslim terrorist organizations, such as ISIS, to recruit and radicalize foreign fighters and lone wolf terrorists (newspapers, games, music)[33].

The problem with counteracting hate speech crimes in the cyberspace often results from the constitutional protection of freedom of expression in some countries (e.g. The United States of America)[34]. However, the online hate speech might also be a manifestation of cyberterrorism and the computer system might be a useful tool to support terrorist activities[35].

Crimes related to instrumental use of networks and computer systems

The last group of cybercrimes, entitled crimes related to instrumental use of networks and computer systems, consists of many various types of crimes that can be committed in the cyberspace. Some of them are stipulated in separate articles and sections of legal acts, nevertheless, the vast majority are "traditional" crimes that can be committed both in the real world and the cyberspace. This group of acts include, *among others*: cyberstalking, cyber-fraud, cybertheft, computer-forgery, cyberstalking, money laundering, skimming, cyberspying.

[27] Prokuratura Krajowa, 'Wyciąg ze sprawozdania dotyczącego spraw o przestępstwa popełnione z pobudek rasistowskich, antysemickich lub ksenofobicznych prowadzonych w 2016 roku w jednostkach organizacyjnych prokuratury' (Warszawa: Prokuratura Krajowa 2017) pp. 2-23.

[28] M. Duda, 'Uchodźcy, imigranci i mniejszości jako ofiary przestępstw z nienawiści' in W. Pływaczewski and M. Ilnicki (ed.), 'Uchodźcy – nowe wyzwania dla bezpieczeństwa europejskiego na tle standardów praw człowieka' (Olsztyn: Katedra Kryminologii i Polityki Kryminalnej 2015) pp. 180-189.

[29] M. Duda and J. Narodowska, 'Mowa nienawiści w Internecie' in W. Pływaczewski and M. Ilnicki (ed.), 'Ochrona praw człowieka w polityce migracyjnej Polski i Unii Europejskiej' (Olsztyn: Katedra Kryminologii i Polityki Kryminalnej 2016) pp. 307-308.

[30] A. Lewkowicz, 'Mowa nienawiści w cyberprzestrzeni' in W. Pływaczewski and P. Lubiewski (ed.), 'Współczesne ekstremizmy. Geneza, przejawy, przeciwdziałanie' (Olsztyn: Katedra Kryminologii i Polityki Kryminalnej 2014) p. 84.

[31] *Ibid*.

[32] P. B. Gerstenfeld, D. R. Grant and C. P. Chiang, 'Hate online. A Content Analysis of Extremist Internet Sites' in P. B. Gerstenfeld and D. R. Grant (ed.), 'Crimes of Hate. Selected Readings' (Thousand Oaks: Sage 2004) p. 144-153.

[33] M. Duda, 'Propaganda Państwa Islamskiego (ISIS) jako przejaw mowy nienawiści oraz metoda rekrutacji i radykalizacji' in W. Pływaczewski and M. Duda (ed.), 'Mowa nienawiści a prawo na tle współczesnych zjawisk społeczno-politycznych' (Olsztyn: Katedra Kryminologii i Polityki Kryminalnej 2017) pp. 151-152.

[34] Relation between hate speech crimes and constitutional rights are discuss in: M. Duda, 'Przestępstwa z nienawiści. Studium prawno karne i kryminologiczne' (Olsztyn: Katedra Kryminologii i Polityki Kryminalnej 2016).

[35] See: A. Tymieniecka, 'Przestępczość internetowa – zagadnienia kryminologiczne' in A. Opalska, M. Treder and A. Tymieniecka, 'Social media. Analiza prawnokarna i kryminologiczna. Zagadnienia wybrane' (Szczecin: Volumina 2016) p. 74.

Due to the limited framework of this paper, the authors decided to present only selected types of cybercrimes, which are, in their opinion, the most dangerous for society and indicate increasing dynamics. Additionally, they can take a form of organized crime[36].

The Polish criminal law penalizes in article 190a k.k. a crime of persistent harassment commonly known as stalking. On the ground of Polish legislation, this crime can take two forms of action. The behaviours penalized in § 1 consist in a significant violation of privacy of another person or another person's next of kin or creation of a justified sense of danger to them. Another type of stalking, § 2, occurs in the situation when a perpetrator pretends to be another person and uses his or her image or other personal data, in order to cause property or personal damage. The criminal liability is higher if the above acts result in suicide attempt of the harassed person. The crime of stalking can be committed both in the real world and in the virtual world. If the place of perpetrator activity is the cyberspace the crime of persistent harassment is called "cyberstalking"[37]. What is important, identity theft without a purpose of causing personal or property damage cannot be treated as cyberstalking. In case of illegal use of someone's data, the perpetrator might be accused for violation of Personal Data Protection Act or Law on Copyright and Related Laws.

According to criminological surveys the perpetrator, in order to gain control over the victim, very often display both forms determined in article 190a § 1 and § 2 k.k. Cyberstalking might also take a form of, *inter alia*, false accusations on online forums, submitting sexual proposal, collecting and disseminating confidential personal data, persuading other persons to harm a victim of cyberstalking, blocking the victim's computer or phone. The crime of stalking is the example of neocriminalization and was introduced to the Polish legislation in 2011. The criminal statistics conducted by the Police indicate that dynamics of this phenomenon increases every year. Comparing records from 2012 and 2017, the number of stalking crimes disquietingly has increased from 2700 to 4200 cases. Nevertheless, in the official record, there is no information whether the crime of stalking was committed in the cyberspace. However, it can be assumed that this number is significant.

The criminological researches indicate that the cyberspace is a conducive place to commit „traditional" criminal crimes. Recently, there are many of cases of stealing the objects from the computer games such as avatars (in-game items). It is worth highlighting that the above items might reach at the online auctions the value, even of several-dozen thousand euros[38]. However, the problematic issues are: determining the place of committing a crime (and consequently, indicating the jurisdiction of the court) and determining the value of stolen property (and consequently qualifying the act either as a crime or a misdemeanour). In case of obtaining someone else's computer software, without the permission of an authorised person, in order to gain a material benefit, the penalization is under the provisions of article 278 § 2 k.k. (theft). However, due to definition of moveable item, contained in article 115 § 9 k.k., unlawful seizure of avatar cannot be qualified as a theft (neither article 279 § 1 – traditional theft, nor article 279§ 2 k.k.). According to the doctrine and the judicature, in this case, the criminal liability can be considered on the ground of article 287 k.k. (computer-fraud). The Police statistics indicate that over the last 20 years, the number of detected computer frauds has increased from 160 to over 4,200.

One of the most often committed type of fraud in the cyberspace is so-called "Nigerian fraud" (Nigerian scam, African scam, 419 scam). Its name comes from the article 419 of the Nigerian Penal Code penalizing such act. The first cases of this fraud have appeared in early 80s of the twentieth century[39]. Thiskind of fraud is most frequently initiated by e-mail contact. The scammers also contact through text message or social media. Nowadays, it can be observed that the mailboxes are flooded with spam offering participation in alleged, lucrative investment. The *modus operandi* of perpetrator looks similar. The content of information sent via the Internet in based on the fictitious transfer of large amount

[36] A. Minnaar, 'Malware and data breach cyberattacks and the more organized cybercriminals. How "organised" are they' in E. W. Pływaczewski and E. M. Guzik-Makaruk (ed.), 'Current problems of penal law and criminology' (Warszawa: C.H. Beck 2017) pp. 601-626.
[37] B. Hołyst, 'Cyberstalking as a form of cyberharassment' [2015] Ius Novum pp. 104-129.
[38] W. Kasprzak, 'Kradzież dóbr z gier komputerowych' in J. Karaźniewicz and T. Kuczur (ed.), 'Karnomaterialne i procesowe instrumenty ochrony jednostki przed nadużyciami władzy państwowej' (Toruń: Adam Marszałek 2015) pp. 262-275.
[39] M. Chawki, 'Nigeria Tackles Advance Fee Fraud' [2009] Journal of Information 1, Law & Technology, pp. 1-17.

of money from overseas country. The perpetrator offers the potential victim a share in this amount or a payment on the condition that the person helps to transfer money out of the particular country. Before that, the offender asks a victim to transfer some money to his bank account. After sending the requested payment by the victim, the contact with the offender stops. There are many variations of Nigerian fraud, e.g. "on political refugee from the black land", on the investor", "on winning the lottery", "on the bank account without the owner", "on the internet auction". The emails sent by offender usually contain language errors as they are automatically translated by translators such as Google. Therefore, the potential victims are seeking in non-English speaking countries (mainly Asian countries)[40]. This type of behaviour is penalized in article 286 k.k. as fraud. Pursuant to it, anyone, who intending to achieve a material benefit, causes another person to unfavourably dispose of his or her property, or the properly of a third party, by misleading the person, or by taking advantage of a mistake or an inability to properly understand the action undertaken, will be punished. Similarly to other crimes related to instrumental use of networks and computer systems, the Polish criminal statistics present only general numbers of committed frauds without distinguishing the place of their commitment.

Another type of crime included in this group is money laundering. The main aim of the perpetrator is to introduce into legal turnover the income coming from illegal activity. It consists of three main phases – placement, masking, integration[41]. The perpetrators of money laundering in the cyberspace use, *among others*, the *modus operandi* similar to Nigerian fraud. One of the methods of cybelaundering is so-called "money mule". It consists in using legal bank accounts in order to transfer illegal money, e.g. from one country to another. The perpetrators contact with the victim via email, claiming to be a person from a war-ravaged country or victim of religious/ethnic persecution. They offer to transfer a certain amount of money to the victim's account asking at the same time for sending back the majority of this amount to the indicated account. The victim's benefit from this transaction is a small share in this amount (10-15%), as a commission. Other variations of cyberlaundering are: sending job advertisements, notifications about winning the lottery. The victim is required to provide personal data such as: name, surname, address, gender, age, occupation, telephone number. With this data, the perpetrator can open a new bank account and launder the money[42].

The Polish Penal Code penalizes money laundering in the art. 299 k.k. The criminologists indicate that money laundering in the cyberspace is also possible due to such phenomena as: cybercurrencies and online gambling. It should be noted that the status of cryptocurrencies (e.g. Bitcoin, Ethereum, Iota) is not regulated by Polish law. At the same time the market of cryptocurriencies is huge and there are even so-called "bitcoin minings". The gambling, in Poland, is regulated by the Gambling Act of 2009[43]. In general, gambling games are legal if they take place in licensed casinos, whereas online gambling requires permission of the Ministry of Finance. Due to restricted regulation, online gambling websites moved their servers to countries with more liberal rules (e.g. Czech Republic, Cyprus). According to criminal statistics, in the last decade the number of recorded crimes of cybelaundering in Poland has been relatively stable and oscillates between 300 and 400 per year.

Conclusions

It should be emphasized that because of the continuous development of technology the *modus operandi* of offenders has been changing. There is a large group of acts which from the criminological point of view seem to be social pathology, but do not display characteristics of the particular crimes consisted in the Polish Penal Code. Therefore, these acts do not bear criminal liability and it is not possible to bring a charge against the perpetrator. The examples of such acts are:

- smishing i.e. sending SMS links to malware,

[40] E. Hernandez, D. Regalado and N. Villeneuve, 'An inside look into the world of Nigerian scammers' (Milpitas, Fire Eye 2018) pp. 3-7.
[41] J. Grzywacz and B. Orłowska-Drzewek, 'Pranie pieniędzy w Internecie' [2011] Nauki ekonomiczne 14 p. 8.
[42] M. DeSantis, C. Dougherty and M. McDowell, 'Understanding and Protecting Yourself Against Money Mule Schemes' (Pittsburgh: Carnegie Mellon University 2011) pp. 1-5.
[43] Act of 19.11 2009 r. – Gambling Act, Journal of Laws, 2018, item 165.

- bluebugging i.e. remote access to mobile devices,
- ransomware i.e. encrypting the data of victim in order to extort a charge for unlocking data[44],
- placing on website violent-related *snuff movies*, *mondo* or *gore*[45],
- inducing to suicide or self-injuring through means of computer games, telephone applications, social networks e.g. „Blue whale" (popular game among youth in Poland) [46],
- cyberviolence (cyberbullying) against individuals and social groups[47].

In the context of cybercrimes, the attention should be paid to the issue of dark number of crimes. As indicated by FBI data, the number of unreported cybercrimes in the United States oscillates between 85 and 97 per cent, in the United Kingdom – 85 per cent, in Germany 75 – per cent, in Russia over 90 per cent[48].

On the basis of records, it can be deemed that official criminal statistics referring to cybercrimes do not present a real scope of the phenomenon of cybercrimes. In the criminal literature, it is stated that the main causes of high dark number of cybercrimes might result from: cross-border character, easy access to networks, anonymity of online users, intangible nature of data, lack of centralized control centre as well as discrepancies between the legislation of individual countries[49]. According to the above, it is expected that dynamics of crimes committed in cyberspace will significantly increase.

Bibliography

Articles

1. Budyn-Kulik M., Kulik M., 'Wybrane zagadnienia kryminalizacji tzw. przestępstw seksualnych przeciwko małoletnim' [in:] S. Pikulski, M. Romańczuk-Grącka (ed.), 'Granice kryminalizacji i penalizacji' (Olsztyn: Elset 2013).
2. M. Chawki, 'Nigeria Tackles Advance Fee Fraud' [2009] Journal of Information 1, Law & Technology.
3. S. Craven, 'Deconstructing perspectives of sexual grooming: implications for theory and practice' (Coventry: Coventry University 2009).
4. M. DeSantis, C. Dougherty and M. McDowell, 'Understanding and Protecting Yourself Against Money Mule Schemes' (Pittsburgh: Carnegie Mellon University 2011).
5. M. Duda, 'Propaganda Państwa Islamskiego (ISIS) jako przejaw mowy nienawiści oraz metoda rekrutacji i radykalizacji' in W. Pływaczewski and M. Duda (ed.), 'Mowa nienawiści a prawo na tle współczesnych zjawisk społeczno-politycznych' (Olsztyn: Katedra Kryminologii i Polityki Kryminalnej 2017).
6. M. Duda, 'Przestępstwa z nienawiści. Studium prawno karne i kryminologiczne' (Olsztyn: Katedra Kryminologii i Polityki Kryminalnej 2016).
7. M. Duda, 'Uchodźcy, imigranci i mniejszości jako ofiary przestępstw z nienawiści' in W. Pływaczewski and M. Ilnicki (ed.), 'Uchodźcy – nowe wyzwania dla bezpieczeństwa europejskiego na tle standardów praw człowieka' (Olsztyn: Katedra Kryminologii i Polityki Kryminalnej 2015).
8. M. Duda and J. Narodowska, 'Mowa nienawiści w Internecie' in W. Pływaczewski and M. Ilnicki (ed.), 'Ochrona praw człowieka w polityce migracyjnej Polski i Unii Europejskiej' (Olsztyn: Katedra Kryminologii i Polityki Kryminalnej 2016).

[44] J. Kosiński, 'Cyberprzestępczość' in W. Jasiński, W. Mądrzejowski and K. Wiciak (ed.), 'Przestępczość zorganizowana. Fenomen. Współczesne zagrożenia. Zwalczanie. Ujęcie praktyczne' (Szczytno: Wydawnictwo Wyższej Szkoły Policji 2013) p. 480.

[45] See more in: M. Romańczuk-Grącka, 'Snuff movies and mondo movies. Characteristics of terrorism and organized crime related film productions' in W. Pływaczewski (ed.), 'Organized Crime and Terrorism' (Olsztyn: University of Warmia and Mazury 2011) pp. 207-225.

[46] See also: W. Kasprzak, 'Niebieski wieloryb – studium kryminalistyczne' in W. Pływaczewski and B. Gadecki (ed.), 'Taktyczno-techniczne aspekty przeciwdziałania przestępczości' (Warszawa: Difin 2018) pp. 151-164.

[47] A. Leszczuk-Fiedziukiewicz, 'Między cyberprzemocą a hejtem. Kampanie społeczne związane z agresją w Internecie' in E.W. Pływaczewski, E Jurgielewicz-Delegacz and D. Dajnowicz-Piesiecka (ed.), 'Współczesna przestępczość i patologie społeczne z perspektywy interdyscyplinarnych badań kryminologicznych' (Warszawa: C.H. Beck 2017) pp. 126-135.

[48] D. Sołodow, 'Ślady wirtualne w praktyce ścigania karnego i kryminalistyce rosyjskiej' [2013] Przegląd Policyjny 2 (110) pp. 161-162.

[49] M. Zbrojewska, S. Biedroń, T. Pański and K. Bajon-Stolarek, 'Prawnokarne aspekty zjawiska cyberprzestępczości' [2016] Palestra 34 pp. 265-266.

9. P. B. Gerstenfeld, D. R. Grant and C. P. Chiang, 'Hate online. A Content Analysis of Extremist Internet Sites' in P. B. Gerstenfeld and D. R. Grant (ed.), 'Crimes of Hate. Selected Readings' (Thousand Oaks: Sage 2004).
10. A. Grześkowiak and K. Wiak (ed.), 'Kodeks karny. Komentarz' (Warszawa: C.H. Beck 2018).
11. J. Grzywacz and B. Orłowska-Drzewek, 'Pranie pieniędzy w Internecie' [2011] Nauki ekonomiczne 14.
12. E. Hernandez, D. Regalado and N. Villeneuve, 'An inside look into the world of Nigerian scammers' (Milpitas, Fire Eye 2018).
13. B. Hołyst, 'Cyberstalking as a form of cyberharassment' [2015] Ius Novum.
14. B. Hołyst and J. Pomykała, 'Cyberprzestępczość, ochrona informacji i kryptologia' [2011] Prokuratura i Prawo.
15. W. Kasprzak, 'Kradzież dóbr z gier komputerowych' in J. Karaźniewicz and T. Kuczur (ed.), 'Karnomaterialne i procesowe instrumenty ochrony jednostki przed nadużyciami władzy państwowej' (Toruń: Adam Marszałek 2015).
16. W. Kasprzak, 'Niebieski wieloryb – studium kryminalistyczne' in W. Pływaczewski and B. Gadecki (ed.), 'Taktyczno-techniczne aspekty przeciwdziałania przestępczości' (Warszawa: Difin 2018).
17. J. Kosiński, 'Cyberprzestępczość' in W. Jasiński, W. Mądrzejowski and K. Wiciak (ed.), 'Przestępczość zorganizowana. Fenomen. Współczesne zagrożenia. Zwalczanie. Ujęcie praktyczne' (Szczytno: Wydawnictwo Wyższej Szkoły Policji 2013).
18. S. Kotecka, 'Strategie i dobre praktyki dotyczące bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych i ochrony przed ich nieuprawnionym ujawnieniem' in J. Gołaczyński (red.), 'Wybrane dobre praktyki w zakresie usług elektronicznych' (Warszawa: C.H. Beck 2016).
19. A. Leszczuk-Fiedziukiewicz, 'Między cyberprzemocą a hejtem. Kampanie społeczne związane z agresją w Internecie' in E.W. Pływaczewski, E Jurgielewicz-Delegacz and D. Dajnowicz-Piesiecka (ed.), 'Współczesna przestępczość i patologie społeczne z perspektywy interdyscyplinarnych badań kryminologicznych' (Warszawa: C.H. Beck 2017).
20. A. Lewkowicz, 'Mowa nienawiści w cyberprzestrzeni' in W. Pływaczewski and P. Lubiewski (ed.), 'Współczesne ekstremizmy. Geneza, przejawy, przeciwdziałanie' (Olsztyn: Katedra Kryminologii i Polityki Kryminalnej 2014).
21. Ministerstwo Cyfryzacji, 'Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022' (Warszawa: Ministerstwo Cyfryzacji 2017).
22. Ministerstwo Spraw Wewnętrznych i Administracji, 'Rządowy program ochrony cyberprzestrzeni na lata 2011-2016' (Warszawa: Ministerstwo Spraw Wewnętrznych i Administracji 2010).
23. A. Minnaar, 'Malware and data breach cyberattacks and the more organized cybercriminals. How "organised" are they' in E. W. Pływaczewski and E. M. Guzik-Makaruk (ed.), 'Current problems of penal law and criminology' (Warszawa: C.H. Beck 2017).
24. M. Nawrocki, 'Miejsce popełnienia czynu zabronionego' (Warszawa: C.H. Beck 2016).
25. Prokuratura Krajowa, 'Wyciąg ze sprawozdania dotyczącego spraw o przestępstwa popełnione z pobudek rasistowskich, antysemickich lub ksenofobicznych prowadzonych w 2016 roku w jednostkach organizacyjnych prokuratury' (Warszawa: Prokuratura Krajowa 2017).
26. F. Radoniewicz, 'Odpowiedzialność karna za przestępstwo hackingu' [2013] Prawo w działaniu 13.
27. M. Romańczuk-Grącka, 'Snuff movies and mondo movies. Characteristics of terrorism and organized crime related film productions' in W. Pływaczewski (ed.), 'Organized Crime and Terrorism' (Olsztyn: University of Warmia and Mazury 2011).
28. P. Siemkowicz, 'Przestępstwo oszustwa komputerowego w polskim kodeksie karnym z uwzględnieniem specyfiki działań sprawcy podejmowanych za pośrednictwem sieci Internet' [2011] Gospodarka Rynek Edukacja 2.
29. M. Siwicki, 'Cyberprzestępczość' (Warszawa: C.H. Beck 2013).
30. M. Siwicki, 'Nielegalna i szkodliwa treść w Internecie' (Warszawa: Wolters Kluwer 2011).
31. M. Siwicki, 'Podział i definicja cyberprzestępstw' [2012] Prokuratura i Prawo 7-8.
32. M. Skórzewska-Amberg, 'Karalność pornografii dziecięcej w polskim kodeksie karnym' in S. Pikulski and M. Romańczuk-Grącka (ed.), 'Granice kryminalizacji i penalizacji' (Olsztyn: Elset 2013).
33. D. Sołodow, 'Ślady wirtualne w praktyce ścigania karnego i kryminalistyce rosyjskiej' [2013] Przegląd Policyjny 2 (110).

34. M. Sowa, ‘Odpowiedzialność karna sprawców przestępstw internetowych’ [2002] Prokuratura i Prawo 4.
35. M. Szmit, I. Politowska, ‘O artykule 267 Kodeksu Karnego oczami biegłego’ [2007] e-biuletyn CBKE.
36. A. Tymieniecka, ‘Przestępczość internetowa – zagadnienia kryminologiczne’ in A. Opalska, M. Treder and A. Tymieniecka, ‘Social media. Analiza prawnokarna i kryminologiczna. Zagadnienia wybrane’ (Szczecin: Volumina 2016).
37. M. Zbrojewska, S. Biedroń, T. Pański and K. Bajon-Stolarek, ‘Prawnokarne aspekty zjawiska cyberprzestępczości’ [2016] Palestra 34.

Legal acts

1. Act of 29.08.1997 – Personal Protection Data, Journal of Laws, 2016, item 922 with amendments.
2. Act of 4.02.1994 – Law on Copyright and Related Rights, Journal of Laws, 2017, item 880 with amendments.
3. Act of 6.06.1997 – Penal Code, Journal of Laws, 2017, No. 2204 with amendments.
4. Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, 28.I.2003, Council of Europe, European Treaty Series No. 189.
5. Council of Europe Convention on Cybercrime, Budapest 23.11.2001, Council of Europe, European Treaty Series No. 185.
6. Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse from 25th October 2007 (Journal of Laws 2015, item 608).
7. Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (Official Journal of the European Union L 335/1 from 17.12.2011).
8. Recommendation no. R 97(20) of the committee of ministers to member states on “hate speech” (Adopted by the Committee of Ministers on 30 October 1997at the 607th meeting of the Ministers' Deputies).

"CYBER-TERRORISM: HIJACKING CIVIL AIRCRAFT USING TECHNOLOGICAL MEANS – INTERNATIONAL LAW PERSPECTIVE"

Osiecki Mateusz[1]

Abstract

Doubtlessly civil aviation is the safest mean of transport. For decades, international community has been constantly working on ensuring that air passengers are secured from external hazards. However, airliners were many times targeted for hijacking and lastly performed experiment by American authorities proved that they are exposed to another dangerous offence: cyber-hijackings. Hereby paper aims at analysing this problem from juridical perspective and sharing views on current status of protection of passengers against cyber-attacks. For that purpose first a brief history of aircraft hijacking shall be presented with a focus on mentioned American experiment. Then, an attempt to define the term "cyber-terrorism" is provided, along with overview of key advantages of cyber-attack for a potential terrorist. It is followed with a chapter on legal instruments related to the problem, namely Hague Convention from 1970 and Beijing Protocol from 2010 with presentation of their advantages and disadvantages. The document is closed with some conclusions on efficiency of legal protection of air passengers against cyber-hijacking.

Key words: hijacking, Beijing Protocol, cyber-terrorism, unlawful aircraft seizure, civil aviation.

Introduction

The year 2017 was officially declared as the safest year in civil aviation. According to official reports, just 10 fatal accidents were registered, resulting in 44 casualties. That makes a significant drop from the number of 303 deaths in 2016, and even a larger decrease from 537 fatalities in 2015.[2] Such a tendency only proves that civil aviation, considered for decades as the safest mean of transport, is constantly becoming even safer. Nevertheless, it does not mean that works on further improvement of safety and security in aviation should be halted. With the faster-than-ever development of technology and capabilities of digital devices, legal measures related to civil aviation should be adapted to changing reality. Especially as the technology not only serves aviation, but may also be used against it.

Since civil aircraft became targets of attacks, especially hijackings, the international community has been working hard to protect air passengers. Many international treaties were adopted, aimed at responding to new threats that may endanger safety of air travels. In recent years, technology became even more popular tool in the hands of offenders. Digital hacking was used against government websites, social media, or even databases consisting of protected personal data. Is then civil aviation vulnerable to acts of cyber-terrorism? The hereby article aims at responding to that question, focusing mostly on international law perspective.

1. Aircraft hijacking – a brief history

Aircraft hijacking (sometimes also called "skyjacking") is nearly as old as civil aviation itself, with the first-ever case thereof registered on February 21st, 1931 in Peru. Byron Rickards, having piloted a Ford Tri-motor turboprop was captured by a group of local revolutionists just after landing in Arequipa in

[1] *PhD candidate at the Chair of International Law and International Relations, Faculty of Law and Administration, University of Lodz, Poland. Interests: aviation safety and security law, anti-terorrism law, international public law, European law.*

[2] O. Smith, '2017 was the safest year in aviation history – but which was the deadliest?' [2 January 2018] The Telegraph, https://www.telegraph.co.uk/travel/comment/2017-was-the-safest-year-in-aviation-history, accessed 2 April 2018.

the south of the country.[3] Several years later, in 1948, a first commercial airliner was hijacked in Macao – a plane belonging to Cathay Pacific Airways then crashed in the ocean.[4]

But a true wave of skyjackings had its outbreak at the beginnings of Cold War and was involving primarily citizens of Eastern Europe countries fleeing from their homelands behind Iron Curtain.[5] From 1961 onwards, more and more American planes were captured and commandeered for Cuba. In total, in the period of 1947-1967 registered were 47 cases of aircraft hijacking.[6] The apogee was reached in 1969 – in this single year 82 such acts were recorded worldwide, which nearly doubled the total number of previous twenty years.[7]

At the turn of 1960s and 1970s the world saw the rise of terrorism in civil aviation. Active in that field especially were Arab terrorist groups: on September 6th, 1970 four aeroplanes belonging to BOAC, Swissair, Trans World Airlines and Pan Am were hijacked by members of Popular Front for the Liberation of Palestine (or 'PFLP'). Offenders demanded release of some Palestinian prisoners from jails in Europe and Israel.[8] Then, on May 8th, 1972, a Sabena 707 jet on route to Tel Aviv was captured above Vienna by terrorists from Black September under the similar motive of releasing 30 Palestinian detainees in Israel.[9] More than two decades later, another spectacular attempt of hijacking occurred in Algiers. On December 24th, 1994, an Airbus A300 belonging to Air France was seized by Armed Islamic Group whose members ordered the crew to fly to Paris. After a brave rescue mission of French National Gendarmerie, the plane was secured and all hijackers were killed.

At the end of 20th century, hijackings were occurring far less frequently, as sophisticated security control systems were being implemented at airports across the globe and governments were concentrating their efforts to fight against terrorism. But the nations of the world were again struck by international terrorism on September 11th, 2001, when several American airliners were captured and subsequently directed at Twin Towers of World Trade Center and the building of Pentagon. That event not only forced governments to even strengthen their anti-terrorist policies, but also changed the attitude towards terrorism – ever since, a terrorist attack has been viewed not only as an ordinary crime, but also as *casus belli* (an act justifying war).[10]

Here, a general remark should be made concerning the world politics. M. Dupont-Elleray fairly points out that acts of aerial hijacking strongly reflect current “political climate” on Earth.[11] At the climax of Israel-Palestine conflict rose the activity of PFLP and other similar groups, during the period of rule of communism in Eastern Europe many refugees were capturing the planes etc.

Would terrorists invent an even bolder way of attacking airline passengers? An event that occurred not too long ago proves that it might be possible...

In November 2017, the US Department of Homeland Security revealed that on September 19th, 2016 a Boeing 757 jet was successfully hacked and remotely diverted to land in Atlantic City, New Jersey. Although the operation was planned in advance and performed as an experiment by the United States' authorities, it served one important purpose: to prove that airliners are now vulnerable to skyjacking with the usage of technological methods. And here, the problem is identified: due to immense technological progress, a high-tech device might be a useful tool in terrorists' hands and therefore health or even lives of airlines' passengers may be in danger, if he takes over control of a plane and then directs it to crash.

---

[3] Aviation Safety Network, https://aviation-safety.net/database/record.php?id=19310221-0, accessed: 2 April 2018.

[4] P. Dempsey, 'Aviation Security: the Role of Law in the War against Terrorism' [2003] Columbia Journal of Transnational Law 3 (41) p. 654.

[5] H. Dawson, 'Civil Aviation, Hijacking and International Terrorism - An Historical and Legal Review' [1987] International Business Law 15 p. 57.

[6] T. Aleksandrowicz and K. Liedel, 'Zwalczanie terroryzmu lotniczego. Wybrane zagadnienia i źródła prawa międzynarodowego' (Szczytno: Wydawnictwo Wyższej Szkoły Policji 2010) pp. 11-12.

[7] P. Dempsey, *Ibid*., p. 654, after: P. Wilkinson, 'Weaknesses in Airport Security Must be Fixed' [8 February 2000] The Scotsman p. 16.

[8] M. Dupont-Elleray, 'Géopolitique du terrorisme aérien: de l’évolution de la menace à la diversité de la riposte ' [2005] Stratégique 1 (85) p. 111.

[9] M. Dupont-Elleray, *Ibid*., p. 111.

[10] T. Aleksandrowicz, 'Zamach terrorystyczny w świetle prawa międzynarodowego: przestępstwo czy akt walki zbrojnej? *Ius ad bellum* a współczesne zagrożenia terrorystyczne – uwagi *de lege lata* i *de lege* ferenda', in: E. Mikos-Skuza, K. Myszona-Kostrzewa, J. Poczobut, et al., 'Prawo międzynarodowe – teraźniejszość, perspektywy, dylematy. Księga jubileuszowa Profesora Zdzisława Galickiego' (Warsaw: Wolters Kluwer Polska 2013) p. 566.

[11] M. Dupont-Elleray, *Ibid*., p. 112.

But are we at least on a juridical level protected against such crimes? Does the law secure us from such behaviour? The attempt to answer those questions shall be taken in subsequent chapters.

2. Cyber-terrorism as a new challenge for law-makers

For a complex and accurate analysis of the problem, necessary it is to define the basic term here, namely "cyber-terrorism". The term has multiple definitions and in consequence is difficult to be accurately described. Although the problem has been known by states for many years, the term still lacks pure legal definition. Neither international treaties, nor domestic law acts provide one. If then one conducts research on the subject, he should analyse those definitions that are being used by doctrine or political institutions. However, most of definitions focus on some common and relevant aspects.

First of all, one should decrypt the most important element of the term, namely the "terrorism" itself. If an attack is to be regarded as "terrorist", it must include following elements:

I. use of force or a threat thereof;
II. unlawfulness;
III. harm to persons or damage to property;
IV. aim at realisation of specific goals, either religious or political;
V. spread of fear or threat thereof;
VI. affecting entities such as state or international organisation.[12]

Therefore, if one wants to define "cyber-terrorism", he should pay attention to inclusion of aforementioned elements thereto.

A WordNet lexical database uses a definition of "cyber-terrorism" that reads as follows: an assault on electronic communication networks.[13]

P. Reambauville-Nicolle defines "cyber-terrorism" as usage of cybernetic attacks or threat thereof in order to create fear, with an intent to force states (governments) or societies to realise certain objectives, mostly of political, religious or ideological nature.[14]

- The author further enumerates some most typical forms of cyber-terrorism:
- clandestine seizure of control of a system;
- denial of service providing;
- destruction or steal of sensitive data;
- hacking;
- cracking (breaking software protection);
- phreaking (sabotage, taking control of telephone network).[15]

In turn, Federal Bureau of Investigation prepared its own definition: the premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents.[16]

We should now take a closer look at aforementioned definitions. The one presented by WordNet database does have a particular value, but is definitely too simplified, as it totally lacks the "terrorist" element. As it was mentioned above, if an assault is to be classified as terrorist, it should feature particular traits [see: supra]. And according to the definition in WordNet, cyber-terrorism may include any kind of assault, only if it is directed against electronic communication networks. Therefore, such a definition may serve as some basis for understanding the nature of the phenomenon, but has little role in research, due to its weak accuracy.

---

[12] M. Osiecki, 'Terrorism vs. International Law – Case of Attacks in Brussels' in 5th International Conference of PhD Students and Young Researchers, 'How deep is your law? Brexit. Technologies. Modern conflicts conference papers 27-28 April 2017' (Vilnius, Lithuania Vilnius 2017) p. 282.

[13] wordnetweb.princeton.edu/perl/webwn, accessed 5 April 2018.

[14] P. Rembauville-Nicolle, 'L'effectivite du droit de la securité aérienne' in X. Latour, 'La securité et la sûreté des transports aériens' (Paris: L'Harmattan 2005) p. 37.

[15] *Ibid*., p. 37.

[16] R. Abeyratne, 'Cyber terrorism and aviation—national and international responses' [2011] Journal of Transportation Security 4 (4) p. 338-339, http://www.crime-research.org/Cyber_Terrorism_new_kind_Terrorism, accessed 5 April 2018.

On the contrary, the definition of Reambauville-Nicolle is much better structured. It contains most elements of the definition of terrorism itself plus adapts it to "cybernetic environment". It is then perfectly destined for conducting research on the topic.

Finally, as for the explanation provided by FBI, its interesting element is focus on subject of attack (information, computer systems, computer programs, data) and offenders (sub-national or clandestine agents), with a lesser concentration on purely terrorist traits of attacks. In consequence, that definition should be treated as having rather "operational" purpose, destined for FBI officers and agents, whose job aims at pursuing offenders and identifying targets, and has loose relation with research. Nevertheless, the definition has also a practical nature, as in fact most offenders are clandestine agents or members of sub-national groups, mostly of terrorist character.[17]

The experiment by American authorities discussed in previous chapter only proved that nowadays cyber-attacks on aircraft are possible. It is due to the fact that presently most aeroplanes used in civil service are equipped with sophisticated computer systems that assist pilots in control. What is more, such a form of attack might be quite "convenient" for potential terrorists due to multiple reasons:

- a skilful terrorist that effectively takes over control of aircraft may remain for a long time anonymous, in contrast to a hijacker that rushes into the cockpit and forces pilots to divert aircraft using weapon,
- using software to hack aeroplanes' systems is cheaper than weapons or tools that were "classically" used to seize control of aircraft,
- process of hacking aeroplane's system does not require direct presence on board; an offender then has lower risk of being captured by security forces while on board.[18]

At the same time, such a "cyber-hijacking" still fulfils most roles related to "classical" skyjacking – as most civil flights carry persons of multiple nationalities and civil aviation itself is a symbol of internationalism, seizure of a plane has a potent of spreading fear throughout wide global audience and affects multiple states or societies in general.[19] Conclusively, an effectively performed cyber-attack on an aeroplane resulting in control take over might definitely be regarded as "terrorist" and therefore a given anti-terrorist law would apply thereto.

3. Legal framework

Just as Reambauville-Nicolle explained, cyber-terrorism might have many forms, including clandestine seizure of control of a system, like cockpit computers in a plane. Would such a manoeuvre be regarded as "aircraft hijacking"? Or rather classified as a different form of crime? Responses to those queries shall be given in hereby chapter.

Aircraft hijacking, unlike cyber-terrorism, has its legal definition in multiple international treaties (which is also repeated in domestic law acts). Although conventions dedicated to the problem are numerous, here we shall discuss only the most relevant, namely:

I. Convention for the Suppression of Unlawful Seizure of Aircraft done in Hague 16 December, 1970 ("Hague Convention");
II. Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft done in Beijing, 10 September 2010 ("Beijing Protocol").

Hague Convention stipulates in Article 1(a) that a person commits an offence if he unlawfully, by force or threat thereof, or by any other form of intimidation, seizes, or exercises control of […] aircraft

[17] See also: K. Anderson, 'Cyber terrorism and politically motivated computer crime are a big concern for the real world' [10 October 2010] Prague Post, https://www.praguepost.com/opinion/5996-virtual-hostage.html, accessed 6 April 2018.

[18] Similarly: R. Abeyratne, 'The Beijing Convention of 2010 on the suppression of unlawful acts relating to international civil aviation—an interpretative study' [2011] Journal of Transportation Security 4 (4) pp. 131-143.

[19] M. Lech, 'Ochrona prawna społeczności międzynarodowej wobec zagrożenia terroryzmem' (Gdansk: Wydawnictwo Uniwersytetu Gdańskiego 2014) p. 42, after: K. Indecki, 'Prawo karne wobec terroryzmu i aktu terrorystycznego' (Lodz: Wydawnictwo Uniwersytetu Łódzkiego 1998) p. 19.

[…].[20] Wording of that provision may perfectly serve as a definition of aircraft hijacking.[21] In fact, at time of Hague Convention preparatory works, participants of conference preferred to use an expression of "unlawful aircraft seizure" instead of "hijacking", as the latter one is related mostly to "change of aircraft's primary itinerary", whereas the former one is much wider and may relate to many other situations in which the factual control of aircraft is taken by force. But for hereby article's narrative, both expression may be treated synonymously.[22]

Point (b) of the article 1 criminalises the act of hijacking and thereby assures that a potential terrorist is not left unpunished. However, a protection introduced by the Convention might not be sufficient, when it comes to hijacking with the use of cybernetic methods, (or "cyber-hijacking"). Crucial here is usage of expressions "by force or threat thereof". If we talk about usage of force in attempt to seize control of an aircraft, we take into account both psychical or physical form. A typical situation of applying physical force would be using tools like weapons against pilots, whereas psychical force would be characterised as pointing gun at the head of pilot and ordering him to divert aircraft, or threatening to blow up a machine with a bomb (if a threat is credible). So, an aeroplane is hijacked, when an offender either uses violence to obtain control thereof, or psychically "pushes" crew to follow his orders. Here then, hacking aircraft systems falls outside the scope of any of those categories. An offender thus only remotely seizes control of a plane's system – no violence/physical force is applied. Obviously, there is also no action affecting air crew psychologically. Therefore, a person using cybernetic methods in hacking aircraft would not be held accountable on the grounds of the provision of article 1 of the Hague Convention, due to non-fulfilling all required elements of crime.

On the other hand, Beijing Protocol that is drafted in purpose of supplementing Hague Convention, covers the gap left by the latter one. Its Article II replacing Article 1 of the Convention stipulates that [a]ny person commits an offence if that person unlawfully and intentionally seizes or exercises control of an aircraft […] by force or threat thereof, or by coercion, or by any other form of intimidation, or by any technological means.[23] In contrast to analogical provision of the Hague Convention, this Article of Beijing Protocol does in fact introduce criminalisation of cyber-hijacking in a proper way.

Positive it is that the Protocol uses a general expression "by technological means" that gives a wide leeway for interpretation. Instead of enumerating possible forms of hijacking aircraft using cybernetic tools (like hacking navigation systems, remote control of steering yokes, etc.), the treaty criminalises potential cyber-attacks en bloc, which assures better protection of airline passengers – regardless of method used by an offender, his act would be considered as a crime.

Another important remark concerns the time and place of committing the crimes. Under Hague Convention, as an offence regarded is only attempt of hijacking occurring on board an aircraft and when the latter one is "in flight". That only adds to argument that an attempt to remotely seize control of an aeroplane would not be treated as a crime under the Convention – an expression "on board" refers to physical presence of an offender in a plane being hijacked. As hacking systems may perfectly be performed at a great distance from a targeted machine, a potential hijacker would not be regarded as offender and in effect, left unpunished.

In turn, Beijing Protocol abandons the expression "on board", which is more relevant for a crime of cyber-hijacking. That automatically eliminate the problem of leaving an offender that attempts to hijack aircraft unpunished when he performs the act remotely, away from the machine itself. Consequentially, the Protocol further uses the expression "against or on board aircraft".

---

[20] Convention for the Suppression of Unlawful Seizure of Aircraft done in Hague 16 December 1970 (Dz.U. 1972 nr 25 poz. 181), art. 1(a).

[21] Not to be confused with *aerial piracy*. Although some authors treat the terms „aerial piracy" and „aircraft hijacking" as synonymous, their meanings are slightly different. An act defining „aerial piracy" is Convention on the High Seas, done at Geneva on 29 April 1958, that in its Article 15 gives the scope. First of all, an act of „piracy" may only be committed on high seas, or at least in the area outside of any state's jurisdiction. Also, such act may only be committed for „private ends", so a pirate usually has intent of steal or rub. Therefore, the term "aerial piracy" is much narrower than "aircraft hijacking".

[22] See more: S. Bazin, 'Le droit penal d'aviation civile' (Paris: Université Panthéon-Assas 2000) pp. 119-120.

[23] Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft done in Beijing on 10 September 2010, ICAO document nr 9959, Art. II.

As for the time of committing a crime, it was said above that Hague Convention criminalises hijacking of aircraft only when it is committed while the latter one is "in flight", so from the moment when all its external doors are closed following embarkation until the moment when any such door is open for disembarkation.[24]

Also in that matter, Beijing Protocol assures better protection of passengers by introducing the criterion of time "in service" (explained in its Article V replacing article 3 paragraph 1 of Hague Convention), so from the beginning of the pre-flight preparation of the aircraft by ground personnel or by the crew for a specific flight until twenty-four hours after any landing.[25] Such solution should be positively rated, as the process of hacking of aircraft systems may be started already when basic cockpit systems thereof are already launched, long before the doors ale closed. A potential offender would then try to connect to navigation devices remotely just after pilots commence preparing aircraft for flight, and already such a behaviour is, under Beijing Protocol, criminalised.

Both Hague Convention and Beijing Protocol do provide legal mechanisms of pursuing an offender and brining him before justice. But due to the fact that Beijing Protocol is much relevant to criminalisation of cyber-hijacking, this part shall be based only on provisions of the latter one.

Just like most other treaties related to crimes against civil aviation, also the Protocol consists of provisions dedicated to jurisdiction of crimes and extradition of offenders. The necessity of regulation of such question is crucial, as civil aviation is marked with factor of internationalism – an aircraft might be registered in state A, an offender might have a citizenship of state B, and the state C might be the one of aircraft's departure *etc*. In such circumstances, difficult it can be to asses which country is appropriate to establish jurisdiction in the case. International treaties usually refer to following jurisdiction theories:

- territorial theory: relevant is a state in whose aerospace the crime is committed,
- aircraft nationality theory: applied is the law of state of aircraft's registry,
- mixed theory: both upper theories may apply dependently of which state's security or public order is disturbed as a result of offence,
- person's nationality theory: appropriate is a state of nationality of either an offender, or persons on board,
- theory of law of state of departure,
- theory of law of state of landing.[26]

Beijing Protocol refers to all of those theories; which one shall be applicable depends strongly on circumstances stipulated in Article VII replacing Article 4 of Hague Convention. According thereto, a state on whose territory an offence is committed can establish jurisdiction (territorial theory) – in case of cyber-hijacking probably relevant would be the one where an offender takes action to seize control of an aeroplane remotely. Also, relevant might be states of (aircraft nationality theory):

- registry of hacked aircraft,
- seat (place of business or residence) of aircraft's lessee (if a plane is leased).

Moreover, either states of offender's nationality or those against whom the crime was committed are eligible. And finally, jurisdiction may equally established by a state of landing, provided that an offender seized a control of aircraft being on board (theory of law of state of landing).

Such extensive regulation of jurisdiction is on one hand problematic in practice, as if multiple states decide to establish jurisdiction, potential conflict between them on which one is more relevant may unnecessarily prolong the proceedings, but on the other hand assures that all states having a particular "interest" in pursuing an offender are eligible to do so under the Protocol.

The last mechanism in theory assuring that an offender would be brought before justice is extradition. Beijing Protocol dedicated its Articles XI to XIII thereto. It generally imposes obligation on state-parties that they include offence of aircraft hijacking (included cyber-hijacking) to all extradition

[24] Convention for the Suppression of Unlawful Seizure of Aircraft done in Hague 16 December 1970 (Dz.U. 1972 nr 25 poz. 181), art. 3.1.
[25] Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft done in Beijing on 10 September 2010, ICAO document nr 9959, Art. V.
[26] See also: I. H. Diederiks-Vershoor, 'An Introduction to Air Law' (The Hague: Kluwer Law International 2012) p. 488.

treaties between them (already existing or concluded in the future) or, if there is no extradition treaty binding them, accept the Protocol as a legal basis for extradition (Article XI). Articles XII and XIII, adding to Hague Convention Articles 8 bis and 8 ter respectively, to some extent restrict and widen protection against hijacking. Article XII prohibits state-parties to recognise act of aircraft hijacking as a political offence, and in consequence grant an offender asylum. However, Article XIII does entitle state-parties to refuse extradition if they have substantial grounds for believing that a request for extradition was made for the purpose of prosecuting a person on an account of their religion, race, nationality etc. So, states in fact have some leeway in deciding on refusal of extradition and in consequence may serve as safe heavens for cyber-hijackers.

Final remarks

Aircraft hijacking is definitely the "oldest" form of attack against civil aviation. Through decades, methods and motives of offenders have been changing. Originally, hijackers were attempting to flee from their homelands, or demand state authorities to pay ransom. Also, aircraft seizure were committed in seek for media attention. But in recent years the serious threat for airline passengers became the world terrorism.[27] International terrorists groups have been growing in strength and acquiring financial resources allowing them to buy advance technologies. Due to the fact that, as the experiment performed by American authorities proved, cyber-hijacking aircraft is now possible, there is even a stronger need for an international treaty that would make criminalisation of such act universal and in consequence not let offenders to be unpunished. Hence the initiative to draft Beijing Protocol that would supplement Hague Convention, that although forms a strong basis for juridical fight against skyjackers, is now obsolete. But does Beijing Protocol fulfil such role? On one hand, it totally does. It is the first treaty of its kind to criminalise cyber-hijacking (and some other forms of aerial terrorism) and covers many gaps left by Hague Convention. On the other hand, in practical way protection assured by the Protocol is somewhat weak. The document entered into force just on 1st January, 2018, so on the first day of of the second month following the date of the deposit of the twenty-second instrument of ratification, acceptance, approval or accession. And as of today, out of barely 35 signatories, only those 22 are now parties to the Protocol, including mostly smaller states, less involved in aerial terrorism problems (Benin, Ghana, Congo, Sierra Leone, Uganda).[28]

Is it then possible that cyber-hijacking shall become an act universally treated as a crime? Probably, but not too soon. After 8 years of conclusion, Beijing Protocol is still enforceable in few states, so treating fight against cyber-hijacking as custom is too early. States of the world should ratify the treaty or at least, accordingly to its provisions, criminalise in their domestic legal systems cyber-hijacking in order to make it be part of customary law. As for us, regular airline passengers, single option is just to wait until international community finally decides to set universal criminalisation of cyber-hijacking as a top priority.

Bibliography

Legal Articel

1. R. Abeyratne, 'The Beijing Convention of 2010 on the suppression of unlawful acts relating to international civil aviation—an interpretative study' [2011] Journal of Transportation Security 4 (4).
2. R. Abeyratne, 'Cyber terrorism and aviation—national and international responses' [2011] Journal of Transportation Security 4 (4), http://www.crime-research.org/Cyber_Terrorism_new_kind_Terrorism, accessed 5 April 2018.
3. T. Aleksandrowicz, 'Zamach terrorystyczny w świetle prawa międzynarodowego: przestępstwo czy akt walki zbrojnej? Ius ad bellum a współczesne zagrożenia terrorystyczne – uwagi de lege lata i

[27] See more: E. McWhinney, 'Aerial Piracy and International Terrorism' (Dordrecht: Martinus Nijhoff Publishers 1987) pp. 8-13.

[28] Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft done in Beijing on 10 September 2010, ICAO document nr 9959), list of parties, https://www.icao.int/secretariat/legal/List%20of%20Parties/Beijing_Prot_EN.pdf, accessed 9 April 2018.

de lege ferenda', in E. Mikos-Skuza, K. Myszona-Kostrzewa, J. Poczobut, et al., 'Prawo międzynarodowe – teraźniejszość, perspektywy, dylematy. Księga jubileuszowa Profesora Zdzisława Galickiego' (Warsaw: Wolters Kluwer Polska 2013).
4. T. Aleksandrowicz and K. Liedel, 'Zwalczanie terroryzmu lotniczego. Wybrane zagadnienia i źródła prawa międzynarodowego' (Szczytno: Wydawnictwo Wyższej Szkoły Policji 2010).
5. K. Anderson, 'Cyber terrorism and politically motivated computer crime are a big concern for the real world' [10 October 2010] Prague Post, https://www.praguepost.com/opinion/5996-virtual-hostage.html, accessed 6 April 2018.
6. Aviation Safety Network, https://aviation-safety.net/database/record.php?id=19310221-0, accessed 2 April 2018.
7. S. Bazin, 'Le droit penal d'aviation civile' (Paris: Université Panthéon-Assas 2000).
8. H. Dawson, 'Civil Aviation, Hijacking and International Terrorism - An Historical and Legal Review' [1987] International Business Law 15, https://www.telegraph.co.uk/travel/comment/2017-was-the-safest-year-in-aviation-history/.
9. P. Dempsey, 'Aviation Security: the Role of Law in the War against Terrorism' [2003] Columbia Journal of Transnational Law 3 (41).
10. I. H. Diederiks-Vershoor, 'An Introduction to Air Law' (The Hague: Kluwer Law International 2012).
11. M. Dupont-Elleray, 'Géopolitique du terrorisme aérien: de l'évolution de la menace à la diversité de la riposte ' [2005] Stratégique 1 (85).
12. K. Indecki, 'Prawo karne wobec terroryzmu i aktu terrorystycznego' (Lodz: Wydawnictwo Uniwersytetu Łódzkiego 1998).
13. M. Lech, 'Ochrona prawna społeczności międzynarodowej wobec zagrożenia terroryzmem' (Gdansk: Wydawnictwo Uniwersytetu Gdańskiego 2014).
14. E. McWhinney, 'Aerial Piracy and International Terrorism' (Dordrecht: Martinus Nijhoff Publishers 1987.
15. M. Osiecki, 'Terrorism vs. International Law – Case of Attacks in Brussels' in 5th International Conference of PhD Students and Young Researchers, 'How deep is your law? Brexit. Technologies. Modern conflicts conference papers 27-28 April 2017' (Vilnius, Lithuania Vilnius 2017).
16. P. Rembauville-Nicolle, 'L'effectivite du droit de la securité aérienne' in X. Latour, 'La securité et la sûreté des transports aériens' (Paris: L'Harmattan 2005).
17. O. Smith, '2017 was the safest year in aviation history – but which was the deadliest?' [2 January 2018] The Telegraph, https://www.telegraph.co.uk/travel/comment/2017-was-the-safest-year-in-aviation-history, accessed 2 April 2018.
18. P. Wilkinson, 'Weaknesses in Airport Security Must be Fixed' [8 February 2000] The Scotsman.

Legal sources

1. Convention for the Suppression of Unlawful Seizure of Aircraft done in Hague 16 December 1970 (Dz.U. 1972 nr 25 poz. 181).
2. Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft done in Beijing on 10 September 2010, ICAO document nr 9959), list of parties, https://www.icao.int/secretariat/legal/List%20of%20Parties/Beijing_Prot_EN.pdf, accessed 9 April 2018.
3. Convention for the Suppression of Unlawful Seizure of Aircraft done in Hague 16 December 1970 (Dz.U. 1972 nr 25 poz. 181).

ICOS IN BELGIUM: INITIAL CONSIDERATIONS ON FINANCIAL, ACCOUNTING AND TAX LAW IMPLICATIONS

Pauwels Karl and Snyers Alexander[1]

Abstract

Initial Coin Offerings or, in short, 'ICOs' can be considered a synergy between crowdfunding and distributed ledger technology. To date, however, there are no specific rules with respect to ICOs in Belgium. This lack of legislation and legal certainty may discourage companies or organisations to set up their ICO in Belgium. If the legislator refuses to act, Belgium risks to be left out while companies go elsewhere. This paper wants to highlight some potential legal implications of setting up an ICO in Belgium.

The structure of the paper is as follows: first, a classification of different kind of tokens is created. Second, after this classification, a high-level analysis from a financial, accounting and tax law perspective is made, and potential legal implications are indicated. The paper concludes with some general remarks.

This research shows that there is no such thing as "the ICO" since most tokens derived from ICOs have different characteristics. There are almost as many types of tokens as there are ICOs. This may explain why regulators seem to be reluctant to provide clear guidance on the topic. Furthermore, the paper shows that no regulation was specifically created with ICOs in mind. Therefore, applying current rules on ICOs leaves us with several legal uncertainties. As most ICOs are very similar to IPOs and most tokens that are issued through an ICO usually embody an investment aspect, it is very likely that token issuers will have to comply with financial law obligations such as prospectus, anti-money laundering and market abuse legislation. The same approach is used in the US. Moreover, the paper shows that the interpretations of these regulations are not always clear and some special regimes, such as the crowdfunding regime may apply as well. Lastly, the accounting and tax regime of ICOs is rather ambiguous as well. With this paper, we try to provide an introduction to prospecting token issuers on the potential legal implications of setting up an ICO in Belgium.

Keywords: ICO, tokens, securities, accounting, taxation

Introduction

In 2017, more than US$ 5.6 billion was raised through initial coin offerings[2] ("ICOs"). This number is expected to be even higher in 2018.[3] The growing rates of ICOs show that the time has come for regulators to provide guidance for this new way of raising funds.

The ICO process goes as follows: a legal or natural person, or even a factual organisation, issues "coins" or "tokens" (see below for a distinction between both terms) that are created with blockchain technology. These tokens are mostly sold for cryptocurrencies such as Bitcoin or Ether, or, in other cases for fiat currency, such as USD and EUR. As the aim of this paper is to dive deeper into this new way of obtaining corporate funding, we will only focus on ICOs that are set up by corporations.

A comparison is often made between ICOs and IPOs (Initial Public Offerings). Although they are both ways to raise funds, ICOs are a more flexible way to raise money since (i) the company does not trade its digital tokens on regulated stock markets, (ii) there is no requirement of involvement of investment banks and (iii) no strong track record is needed to have a successful ICO. Furthermore, companies are

---

[1] *Both authors are Researchers and Teaching Assistants at the Faculty of Law of the University of Antwerp, in the respective fields of Company and Financial Law, and Tax Law. They have both contributed equally to this paper.*

[2] According to F. Ventures, "The State of the Token Market report', a VC fund with a focus on Fintech, and TokenData (https://www.tokendata.io/), a platform that tracks data on token sales and ICOs, https://static1.squarespace.com/static/5a19eca6c027d8615635f801/t/5a73697bc8302551711523ca/1517513088503/The+State+of+the+Token+Market+Final2.pdf. Other tracking platforms, like CoinSchedule, report a lower number of US$ 3.8 billion, https://www.coinschedule.com/stats.html?year=2017, accessed on 10 April 2018.

[3] 'Cryptocurrency ICO Stats 2018', https://www.coinschedule.com/stats.html?year=2018, accessed on 10 April 2018.

free to choose the rights and obligations that their tokens will embody. When token characteristics of recent ICOs are studied, almost as many different types of tokens as there are ICOs can be distinguished. Some of them grant token holders access to a digital platform or give them a discount on the platform access fees. Other tokens grant their holders the right to purchase certain services or products that the token issuer will provide with the proceeds of the ICO. Furthermore, there are tokens with rights and obligations, which are akin to regular shares or bonds. These rights, obligations and other characteristics of a token are usually described in a "whitepaper", a document that is made publicly available prior to the ICO.

It is often argued in the media that ICOs are not subject to any regulation. [4] This may give companies the wrongful impression that everything is allowed. Even though there are no specific regulatory provisions regarding ICOs in Belgium at the moment, many existing regulations are formulated in a very general way or contain some kind of catch-all clause, so that ICOs may in fact fall in their scope.

Given that the current legislative framework is rather uncertain as far as ICOs are concerned, clarification is needed. The purpose of this paper is therefore to guide potential token issuers and investors in their efforts to set up or invest in an ICO in Belgium. The topic will be dealt with from a Belgian legal perspective. Due to many uncertainties, it is important for regulators to take action in order to create a stable and healthy environment for ICOs in Belgium.

The structure of the paper is as follows. Before diving into the legislative framework, a classification of tokens is made. Second, we analyse possible pitfalls of ICOs in the current legislative framework. Various issues are highlighted from a financial, accounting and tax law perspective. To conclude, some general remarks will be set out.

1. Cryptocurrencies? Coins? Tokens? Quid?

Since ICOs are a new phenomenon, we will firstly define the different concepts and terms. So far, there is no generally accepted terminology available.[5] Therefore, it is rather difficult for legislators to make nuanced decisions on ICOs. A clear conceptual framework, however, is important in order to create some degree of uniformity. Moreover, some degree of standardisation should, in fact, be implemented on a EU level.

The first concept that needs to be defined is "Cryptocurrency". This term is often (mis)used as an umbrella term for all "crypto-assets" (i.e. "cryptocurrencies" or "coins" and "tokens"). Crypto-assets rely on Distributed Ledger Technology (hereinafter referred to as "DLT"). The most famous example of a cryptocurrency is Bitcoin. Bitcoin uses DLT to make payment transactions that are secured by cryptography, hence the name "crypto-"currency.[6]

There is, however, a distinction to be made between different types of crypto-assets. On the one hand, there are 'Cryptocurrencies' or 'Coins'. These are crypto-assets that are used as a general-purpose medium of exchange, a store of value and a unit of account.[7] All constituent elements of a regular currency are present. The goal of cryptocurrencies is to provide for a peer-to-peer mechanism to conduct payments, without having to rely on trusted third parties.

On the other hand, there are so-called 'Tokens'. Tokens have an extra functionality. Other than a currency, they are no general-purpose medium to transfer value.[8] They constitute the embodiment of some kind of claim against the issuer of the token.[9] This claim can have various forms. Some tokens represent a claim against future cashflows of the issuing entity, others give right to future products or

[4] E.g., see R. Mooijman, 'Opgepast voor oplichting met crypto-munten' [2017] De Standaard, http://www.standaard.be/cnt/dmf20171113_03183447.

[5] T. Euler, 'The Token Classification Framework' [2018], http://www.untitled-inc.com/the-token-classification-framework-a-multi-dimensional-tool-for-understanding-and-classifying-crypto-tokens/.

[6] 'IFRS – Accounting for crypto-assets' [2018] EY, p. 4, http://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2018/03/EY-IFRS-Accounting-for-crypto-assets.pdf.

[7] 'Virtual Currencies' [2012] ECB, p. 10, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

[8] 'IFRS – Accounting for crypto-assets', *Ibid.*, p. 7.

[9] 'Statement in Connection with the 2017 AICPA Conference on Current SEC and PCAOB Developments' [2017] SEC, https://www.sec.gov/news/speech/bricker-2017-12-04.

services of the issuer. The rights and obligations attached to such a token are, as we pointed out earlier, listed in a detailed whitepaper from the issuer.

The above-mentioned distinction is important from a legal perspective, as both crypto-assets have different legal implications. In order to facilitate the decision-making processes of legislators, it is important that a framework is used where no ambiguities exist.

Since we are interested in this new means of raising funds for companies, this paper focusses solely on Tokens. The term 'ITO' or 'Initial Token Offering' is therefore more appropriate.

As stated above, tokens can embody different rights and obligations. Hence, a one-size-fits all solution is impossible to provide. One must look on a case-by-case basis to assess the legal implications of each ITO and the tokens that come forth from them.

It is, however, possible to distinguish two main Token archetypes: (i) Investment Tokens and (ii) Utility Tokens.[10]

1.1. Investment Tokens

The first type of tokens is the 'Investment Token'. These tokens are very similar to regular securities such as shares, bonds or hybrid products. They represent in other words an economic interest in the issuing entity. When purchasing Investment Tokens, the investor expects a future cashflow, comparable with interests or dividends, and hopes to generate a capital gain when selling them.

One could argue that the only innovative feature of these tokens is the technology behind them. By using DLT, transactions can be executed and registered instantaneously. The legal implications will be analogous to the implications regular products carrying similar rights and obligations entail (see below).

1.2. Utility Tokens

The second token class consists of so-called 'Utility Tokens'. These tokens give their holders a right to purchase (future) services or products of the issuer, or they give access to a specific platform.[11] The revolutionary aspect of these tokens is that they allow interaction between the users and the company through a platform. In this way, certain user behaviour can be rewarded with tokens, while token holders can also benefit from the value creation within the network.[12]

Utility tokens are a lot more challenging to approach from a legal perspective, as there are so many possibilities. The main difference with Investment Tokens is that Utility Tokens are – initially – not meant to generate cashflows for their investors.[13] The value of Utility Tokens stems from the functional aspect they embody.

To assess Tokens from a legal point of view, it is – in our opinion – important to consider the economic reality behind these tokens. It seems that a lot of Utility Tokens are bought merely for trading purposes. This reality might have severe implications from a financial law perspective.

In the next chapter, we will look into potential financial law implications of setting up an ITO in Belgium.

---

[10] Different distinctions are possible, depending on the point of view. For the different options to classify tokens, we refer to T. Euler, 'The Token Classification Framework' [2018] http://www.untitled-inc.com/the-token-classification-framework-a-multi-dimensional-tool-for-understanding-and-classifying-crypto-tokens/.

[11] T. Sameeh, 'ICO basics – security tokens vs. utility tokens' [2018], https://www.cointelligence.com/content/ico-basics-security-tokens-vs-utility-tokens/.

[12] J. Stauffer, 'The Coming Crypto Utility Token Economy: Definitions, Examples, and Why It Matters' [2018], https://medium.com/@jaredstauffer/the-coming-crypto-utility-token-economy-definitions-examples-and-why-it-matters-521f9390be69.

[13] T. Sameeh, 'ICO basics – security tokens vs. utility tokens' [2018], https://www.cointelligence.com/content/ico-basics-security-tokens-vs-utility-tokens/.

2. Potential financial law implications

To date, apart from some warnings of the Belgian Financial Services and Markets Authority ("FSMA")[14], no specific regulatory guidance has been provided regarding ITOs in Belgium. Depending on the rights and obligations embodied in tokens, ITOs may trigger financial law obligations.

2.1. Do tokens fall within existing financial law categories?

Depending on the facts and circumstances, tokens may qualify as regulated 'instruments' within a Belgian financial law context. Two main categories of instruments can be distinguished. The first category consists of 'financial instruments' as defined in the "Financial Supervision Law".[15] The same term is used in both the "Investment Services Law"[16], as well as in the "MiFID II Law" [17] (which transposes the MiFID II Directive[18]). When a token can be regarded as a financial instrument, the issuer will have to comply with different licensing obligations.

The second important category comprises 'investment instruments' as defined in the "Belgian Prospectus Law".[19] When tokens fall within this category, token issuers are obliged to fulfil prospectus requirements. In practice, many token issuers attach some kind of functionality to their tokens to qualify them as Utility Tokens, hoping to fall outside of the scope of the prospectus law. We are, however, very sceptical about this approach and stress the need to look at the economic reality. In most cases, we doubt that token issuers will escape these legal consequences.

Other qualifications may exist. However, since the main goal of an ITO is acquiring funds, the two above-mentioned categories are the most important ones to consider.[20]

2.1.1. When can tokens be considered to be financial instruments?

A definition of 'financial instruments' can be found in the Financial Supervision Law.[21] Article 2, 1° of this law contains a limitative list of different categories of instruments that can be regarded as a "financial instrument" within its context. Tokens as such, are nowhere to be found in this list. However, one could argue that some tokens (mostly Investment Tokens) can fall within the scope of the category 'transferable securities' of the Financial Supervision Law, which is a subcategory of financial instruments.[22]

Article 2,1° a) of the Financial Supervision Law defines transferable securities as "those classes of securities which are negotiable on the capital market, with the exception of instruments of payment, such as:

---

[14] 'Initial coin offerings (ICOs)' [2017] FSMA, https://www.fsma.be/sites/default/files/public/content/EN/Circ/fsma_2017_20_en.pdf. The FSMA endorsed prior statements of the ESMA (European Securities and Markets Authority); See: 'Statement firms' [2017] ESMA, https://www.esma.europa.eu/sites/default/files/library/esma50-157-828_ico_statement_firms.pdf and 'Statement Investors' [2017] ESMA, https://www.esma.europa.eu/sites/default/files/library/esma50-157-829_ico_statement_investors.pdf.

[15] "Financiële instrumenten"/"instruments financiers" as defined in the Belgian Law of 2 August 2002 on the supervision of the financial sector and on financial services [4 September 2002] Belgian Official Gazette 39121.

[16] Law of 25 October 2016 on the access to the investment services company and on the legal status and supervision of portfolio management and investment advice companies [18 November 2016] Belgian Official Gazette 76915.

[17] Law of 21 November 2017 on the infrastructures for markets in financial instruments and transposing Directive 2014/65/EU [7 December 2017] Belgian Official Gazette 107933.

[18] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61.

[19] "Beleggingsinstrumenten"/"instruments de placement" as defined in the Belgian Law of 16 June 2006 on the public offering of investment instruments and on the admission of investment instruments to trading on a regulated market [21 June 2006] Belgian Official Gazette 31352.

[20] For a more in-depth analysis, see: A. Snyers and K. Pauwels, 'ICOs in Belgium: down the rabbit hole into legal no man's land?' (Part 1)' [2018] ICCLR, in press.

[21] *Cf.* Art. (4)(1)(17) / Section C Annex I European Parliament and Council Directive (EU) 2004/39/EC on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC [2004] OJ L145/1 (MiFID I Directive), replaced by art. (4)(1)(15) / Section C Annex I European Parliament and Council Directive (EU) 2014/65 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU [2014] OJ L173/349 (MiFID II Directive).

[22] "Effecten"/"valeurs mobilières", see art. 2 1° a) of the Financial Supervision Law.

- shares in companies and other securities equivalent to shares in companies, partnerships or other entities, and depositary receipts in respect of shares;
- bonds or other forms of securitised debt, including depositary receipts in respect of such securities;
- any other securities giving the right to acquire or sell any such transferable securities or giving rise to a cash settlement determined by reference to transferable securities, currencies, interest rates or yields, commodities or other indices or measures" (own emphasis added).[23]

Since Investment Tokens are usually – apart from the technology used – very similar to regular bonds or shares, they ought to fall within the scope of transferable securities and should give rise to the same regulatory consequences of analogous instruments such as bonds and shares. Furthermore, most Investment Tokens are indeed 'transferable' as most of them are sold on 'crypto-exchanges' (i.e. a secondary market where crypto-assets are traded) and thus 'negotiable on the capital market'. Moreover, tokens issued by one issuer usually share the same features. Hence, one might say that they are 'standardised'.[24]

Utility tokens, on the other hand, are normally not meant to generate cashflows for their holders, as their functional aspect prevails. Generally, they are not considered to be transferable securities. However, this view needs to be nuanced. Utility Tokens are usually created with the only intention to grant the holder a discount on a specific service or product or access to a crypto-platform. Nevertheless, if one considers the economic reality, one must conclude that most of these Utility Tokens are purchased with the sole intention of reselling them at a higher price and thus realising a capital gain. Similar to Investment Tokens, Utility Tokens are actively traded on crypto-exchanges. This suggests that most Utility Tokens are just Investment Tokens dressed up as a Utility Token.

Therefore, we are convinced an alternative approach is needed. In our opinion, there is no reason to argue that Utility Tokens that are actively traded on secondary markets should be treated in a different way from other transferable securities. We believe they ought to fall within the scope of the concept 'financial instruments'. However, we are aware of the fact that there are Utility Tokens that are not listed on secondary markets and do have a fixed price. They are more akin to vouchers. This way, they are to be distinguished from 'regular' financial instruments. We have opted to call them 'Pure Utility Tokens'.

It might be a good idea to implement a 'financial instrument test'[25] to determine if a token constitutes de facto a financial instrument. A similar test is applied by the SEC (the "Securities and Exchange Commission") in the United States: the so-called 'Howey-test'[26]. In summary, there are four elements to determine whether an investment contract constitutes a security. The investment contract should be a contract where (i) a money investment is made into (ii) a normal enterprise, (iii) from which profits are expected (iv) that are derived from the managerial or entrepreneurial efforts of others.[27] Investment Tokens meet these requirements. If we look at the economic reality, most Utility Tokens grant their investor the expectation of profits, which are usually (partly) derived from the managerial efforts of the token issuer. Therefore, the SEC considers most Utility Tokens to be securities as well.[28]

[23] Art. 2, 31° Financial Supervision Law (*cf.* art. 4(1)(18) MiFID I Directive, replaced by art. 4 (1)(44) MiFID II Directive).
[24] P. Hacker and C. Thomale, 'Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law' [2017] SSRN, https://ssrn.com/abstract=3075820, pp. 20 *et seq.*
[25] A similar test was suggested by the Malta Financial Services Authority, see: 'Discussion Paper on Initial Coin Offerings, Virtual Currencies and Related Service Providers' [2017] MFSA, p. 8, https://www.mfsa.com.mt/pages/readfile.aspx?f=/files/Announcements/Consultation/2017/20171130_DiscussionPaperVCs.pdf.
[26] This test refers to case in the US where criteria were adopted to determine if an investment contract can be qualified as a security See: SEC v. W.J. Howey Co., 328 U.S. 293 [1946].
[27] SEC v. W.J. Howey Co., 328 U.S. 293 [1946] 301. See also: United Housing Found., Inc. v. Forman, 421 U.S. 837 [1975] 852-853; *SEC v. Edwards*, 540 U.S. 389 [2004] 393.
[28] *E.g. s*ee in this respect: SEC, In the Matter of Munchee Inc., Order (11 December 2017) p. 8.

2.1.2. When can tokens be considered to be investment instruments?

A definition of 'investment instruments' can be found in the Prospectus Law. Article 4 of this law lists the different categories of rights and values that can be qualified as 'investment instruments'. Since ITOs are a relatively new phenomenon, tokens are nowhere to be found in this list. This list, however is not intended to be limitative and contains two catch-all clauses. Therefore, all agreements that represent rights on investment instruments other than securities[29], and all instruments that – regardless of their underlying assets – make a financial investment possible[30], are considered to be investment instruments.

When considering both clauses, all tokens that are traded on an exchange ought to be regarded as investment instruments. All of them (with an exception for Pure Utility Tokens) embody an investment aspect since they are tradable on a crypto-exchange and can be subject to speculation. Hence, we argue that they fall within the scope of these catch-all clauses.

Therefore, token issuers in spe, should – for the sake of certainty – provide a prospectus and comply with prospectus rules before setting up an ITO. The question remains of course, whether this is desirable. Further regulatory guidance on the matter would be most welcome. To date, most token issuers provide a whitepaper – a less bulky alternative for a prospectus – to inform potential investors.[31] Although some whitepaper standards are being developed in the crypto-space, they are not yet regulated. It might be useful to consider the option to regulate these whitepapers so they can serve as a prospectus "light", and create a special regime, specifically tailored to ITOs.

2.2. What other financial law regimes are to be considered?

To conclude this financial regulatory perspective, we will briefly touch upon other financial law regimes like crowdfunding, the market abuse and the anti-money laundering regime. Furthermore, the UCITS[32] and the AIF[33] regime ought to be considered as well when setting up an ITO. These two regimes, however, fall outside the scope of this paper.

2.2.1. Crowdfunding regime

Depending on the facts and circumstances, an ITO could be set up to fall within the scope of the more advantageous Belgian crowdfunding regime.[34] ITOs constitute de facto a new way of crowdfunding.[35] In our opinion, the option of adapting crowdfunding rules to tokens should be explored, in order to give the issuers of tokens more leeway. One could, for instance, raise the current cap of EUR 300,000[36], which is the maximum amount that can be raised under this regime, to EUR 1,000,000. Belgium has, after all, the authority to raise the cap on the amount of funds that can be raised under an exemption.[37] Further guidance on this topic would be desirable.[38]

[29] Art. 4, §1, 9° of the Prospectus Law.
[30] Art. 4, §1, 10° of the Prospectus Law.
[31] E.g. see various whitepapers in the Whitepaper Database, http://whitepaperdatabase.com.
[32] Law of 2 August 2012 on undertakings for collective investment that comply with the conditions set out in Directive 2009/65/EG and undertakings for investment in debt claims [19 October 2012] Belgian Official Gazette 63652.
[33] Law of 19 April 2014 on alternative investment funds and their managers [17 June 2014] Belgian Official Gazette 45353.
[34] Belgian Law of 18 December 2016 on the recognition, delineation and definition of crowdfunding and containing various financial provisions, [20 December 2016] Belgian Official Gazette 87668.
[35] One could call it 'crowdfunding 2.0'. See: J. Baukema, 'Initial Coin Offerings (ICO's): crowdfunding 2.0?' [2018] TFR (NL) p. 113-121.
[36] Art. 18 of the law of 18 December 2016 on the recognition, delineation and definition of crowdfunding and containing various financial provisions, [20 December 2016] Belgian Official Gazette 87668.
[37] Art. 1(3) of the European Parliament and Council Directive (EU) 2017/1129 on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market, and repealing Directive 2003/71/EC [2017] OJ L168/12.
[38] The FSMA has already issued a FAQ (see: https://www.fsma.be/nl/crowdfunding-1, accessed on 2 April 2018) and a statement (see: 'Statement on Crowdfunding' [2017] FSMA, https://www.fsma.be/nl/file/49564/download?token=lm9iQG2r) on the regulatory requirements for crowdfunding in Belgium, which could be supplemented with a section on ITOs.

2.2.2. Market abuse regime

As most tokens will probably qualify as financial instruments, one has to look into the possibility of being subject to the Market Abuse Regulation[39].[40] The purpose of this regulation is to minimize insider trading and to counter market manipulation on exchanges. Again, further guidance on the application of these rules on ITOs would be most welcome.

2.2.3. Anti-money laundering regime

The European Commission recently proposed the fifth Anti-Money Laundering ("AML") Directive. This directive aims to, inter alia, minimize the risks that arise when dealing with virtual currencies.[41] Of particular relevance for ITOs, is that this directive defines 'virtual currencies'. Moreover, it brings both custodian wallet providers, as well as providers of exchange services between fiat currencies and virtual currencies, within the scope of the AML legislation

However, the European legislator did not go far enough with its new directive, since platforms where virtual currency can be exchanged for other virtual currency fall outside the scope of the new AML Directive and most token issuers sell their tokens in exchange for cryptocurrencies.[42] Generally speaking, most investors have acquired their cryptocurrencies at some place in time and should thus be identifiable. This may, however, not be the case when their cryptocurrencies were mined.[43]

3. Potential accounting and tax law implications

Tokens resulting from an ITO constitute in fact a new asset class. As is the case for most regulations, the Belgian GAAP (i.e. the Generally Accepted Accounting Standards), nor the Belgian tax law were designed with crypto-tokens or ITOs in mind. This leads to uncertainty which is exacerbated by the fact that, to date, no official guidelines have been issued on the accounting and tax treatment of tokens.

Pending further guidance, one should consider the existing general principles first. Given the fact that there are countless characteristics a token can embody, it is impossible to provide a one-size-fits-all analysis. Therefore, all ITOs should be assessed on a case-by-case basis.

3.1. Some general remarks regarding the accounting treatment of tokens

A problem that might occur when an entity is planning an ITO is how the sale of tokens must be recorded in its accounts. The accounting treatment will – of course – depend on the token that is issued.

When considering an Investment Token, it is very likely that the accounting treatment is analogous to the accounting treatment of more conventional instruments, such as shares, profit participating certificates or bonds. [44]

The difficulties arise when considering the accounting implications of Utility Tokens. Different approaches are conceivable. Some Utility Tokens resemble vouchers and should be treated the same

[39] European Parliament and Council Directive (EU) 596/2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC [2014] OJ L173/1.
[40] The Belgian FSMA recently pointed out that token issuers may indeed have to comply with MAR. See: 'Initial coin offerings (ICOs)' [2017] FSMA, p. 2, https://www.fsma.be/sites/default/files/public/content/EN/Circ/fsma_2017_20_en.pdf.
[41] COM/2016/0450, 'Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC' [2016] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016PC0450&qid=1523358551244&from=EN.
[42] A. Bal, 'Blockchain, Initial Coin Offerings and Other Developments in the Virtual Currency Market' [2018] Derivatives & Financial Instruments, Journals IBFD Volume 20, No. 2, p. 8. See also: N. Vandezande, 'Virtual currencies under EU anti-money laundering law' [2017] Computer Law & Security Review, No. 33, p. 351.
[43] Not all virtual currencies can be mined (*i.e.* they are already pre-mined).
[44] 'IFRS – Accounting for crypto-assets [2018] EY, p. 8, http://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2018/03/EY-IFRS-Accounting-for-crypto-assets.pdf.

way.[45] Therefore, when considering for example a Pure Utility Token, where the holder will merely acquire a right to purchase a product or access a service, the accounting treatment will likely be similar as a revenue earned in the context of a voucher. Others may share more characteristics with prepaid income for services or products and should thus be treated equally.[46] There are also Utility Tokens that have similar characteristics to so-called 'contracts-in-progress' ('sell first, create afterwards') and should be treated as such.[47]

3.2. Some general remarks regarding the tax treatment of tokens

3.2.1. Income Tax

When income derived from an ITO is considered to be revenue from an accounting perspective, it will be subject to corporate income tax in the taxable period in which the revenue is recognised. The issuance of Investment Tokens will probably not constitute a taxable event, whereas the issuance of Utility tokens will most likely trigger income taxes when the proceeds thereof are recognised in the accounts.

Another question that should be tackled is the treatment of the proceeds that stem from Investment Tokens. They may resemble regular dividends, or interest payments, etc., and may be treated as such. Also, capital gains on tokens (regardless whether they are considered to be Investment Tokens or Utility Tokens) will most likely be treated analogously to capital gains that are realised on other assets such as shares and bonds. An in-depth analysis of the tax treatment of both the proceeds derived from tokens and the capital gains of the sale of tokens falls outside the scope of this paper.[48]

Furthermore, it is important to consider different tax incentives, such as the notional interest deduction[49], which can reduce the company's tax base. The potential tax implications ought to be analysed on a case-by-case basis. Token issuers should consider the different tax incentives when drawing up the whitepaper of the ITO to optimize the tax treatment.[50]

3.2.2. VAT

To analyse the VAT implication(s) of an ITO, each case should be considered individually as well.

When an entity issues Investment Tokens, it is unlikely that this event an sich will trigger VAT, as most of these tokens can be regarded as (transferable) securities from a financial regulatory perspective (see above). This same qualification should be applicable for VAT purposes as well. Transactions with respect to such securities are exempt from VAT.[51] As Investment Tokens may be considered as securities and ITOs are the high-tech pendants of Initial Public Offerings, we are convinced that both types of fundraising will be treated equally in a VAT context.

When an entity issues Utility Tokens, the proceeds thereof might be considered as a consideration for (electronic[52]) services from the token holder to the issuer. Hence, the ITO might be subject to VAT in Belgium.[53] However, if one looks at the economic reality, it is clear that, at the time of the ITO, the event is merely used to acquire funding to develop a product, a service or a platform in the future. Therefore,

[45] *Cf.* 'Advice 148-1 on agreements providing staggered or successive supplies' [1984] CBN, http://www.cnc-cbn.be/files/advice/link/NL_148-01.htm.
[46] *Cf.* 'Advice 132/6 on prepayments' [1993] CBN, http://www.cnc-cbn.be/files/advice/link/NL_132_06_Herzien_advies.pdf.
[47] "Bestellingen in uitvoering"/"commandes en cours d'exécution".
[48] For a more in-depth analysis on this topic, see: K. Pauwels and A. Snyers, 'ICOs in Belgium: down the rabbit hole into legal no man's land? (Part 2)' [2018] ICCLR, in press.
[49] Art. 205bis *et seq.* Belgian Income Tax Code.
[50] M. Langer and S. Valenta, 'Taxation of Cryptocurrency and Blockchain-Based Companies in Liechtenstein' [2018], Tax notes international p. 172.
[51] Art. 44, §3, 10° of the Belgian VAT Code.
[52] A. Bal, 'Blockchain, Initial Coin Offerings and Other Developments in the Virtual Currency Market' [2018] Derivatives & Financial Instruments, Journals IBFD Volume 20, No. 2, p. 6.
[53] Art. 2 Belgian VAT Code.

we argue that, in many cases, the ITO-event itself, should not be considered as a taxable event.[54] Of course, when the Utility Tokens are used for their real purpose (traded for a product or service), these transactions will be subject to VAT. Arguing that ITO itself is to be considered as a taxable event would result in a double taxation. Firstly, VAT would be triggered at the time of the token issuance and secondly at the time the token is used for its actual purpose.

Furthermore, it is possible that some Utility Tokens could fall within the scope of the VAT regime regarding 'multi-purpose vouchers'.[55] The multi-purpose vouchers will only trigger VAT at the time of "the actual handing over of the goods or the actual provision of the services in return for a multi-purpose voucher accepted as consideration or part consideration by the supplier shall be subject to VAT".[56]

3.2.3. Miscellaneous taxes

ITOs and tokens may also be subject to other Belgian taxes. When considering setting up an ITO or investing in tokens, one must take these taxes into account. Two specific examples are the Belgian stock exchange tax[57], which is levied when securities are transferred, and the annual tax on Belgian and foreign securities accounts[58], which is levied when one is holding securities worth at least EUR 500,000 in a security account. The question remains whether the different kind of tokens will fall within the scope of these taxes.

Conclusion

As we pointed out in this paper, a lot of uncertainty remains with respect to ITOs. In some cases, the tokens fall perfectly within the scope of the existing regulatory framework, whereas other tokens are more difficult to classify and consequently, their legal implications remain rather uncertain.

The main conclusion is that one should always take into account the economic reality behind all ITOs. This reality shows that most investors buy tokens purely with the intention to realise capital gains, no matter whether the token can be qualified as a Utility Token or an Investment Token.

Regulators who are willing to tackle the regulatory issues arising from ITOs will have a difficult task. We hope they will manage to regulate ITOs in a neutral way, so that the blockchain technology can evolve, without being hampered by an over-regulating regulator. Belgium could follow the example of countries such as Estonia[59], Switzerland[60], Liechtenstein[61] and Belarus[62] and implement a lenient approach with respect to ITOs. These countries attract a lot of token issuers and, in doing so, they attract a lot of capital. In the Belgian system, several challenges remain with regards to ITO regulation.[63] We are, however, convinced that it is worth to provide regulatory guidance, so the digital economy can thrive.

---

[54] To strengthen this reasoning, one may say that there is also no 'direct link' between the consideration received and the services provided by the service provider, which is a constitutive element to trigger VAT. E.g., see: Coöperatieve Aardappelenbewaarplaats, Case 154/80 [1981], §12; *Tolsma*, Case C-16/93 [1994] ECJ, § 13; GFKL Financial Services, Case C-93/10 [2009] ECJ, §19.

[55] Council Directive (EU) 2016/1065 amending Directive 2006/112/EC as regards the treatment of vouchers [2016] OJ L177/9.

[56] Article 30b of VAT Directive.

[57] "Taks op de beursverrichtingen en de reporten"/"taxe sur les opérations de bourse et les reports", see art. 120 et seq. of the Belgian Code of Miscellaneous Rights and Taxes.

[58] "Taks op de effectenrekeningen"/"taxe sur les comptes-titres", see art. 152 et seq. of the Belgian Code of Miscellaneous Rights and Taxes.

[59] R. J. Witismann, 'Estonia to become a global ICO hub' [2018] https://medium.com/@Incorporate_ee/estonia-to-become-a-global-ico-hub-6a4a53863719.

[60] S. Ozelli, 'Why Switzerland is Becoming a "Crypto Nation" with a Flourishing ICO Market: Expert Take' [2018] https://cointelegraph.com/news/why-switzerland-is-becoming-a-crypto-nation-with-a-flourishing-ico-market-expert-take.

[61] M. Langer and S. Valenta, 'Taxation of Cryptocurrency and Blockchain-Based Companies In Liechtenstein' [2018] Tax notes international p. 172.

[62] S. Solodkiy, 'USSR's crypto paradise: $1B ICO of Abkhazia, Belarus legalizes ICOs and cryptocurrencies' [2017], https://medium.com/@slavasolodkiy_67243/ussrs-crypto-paradise-1b-ico-of-abkhazia-belarus-legalizes-icos-and-cryptocurrencies-105aec08fa1d.

[63] E.g.,see: K. Pauwels and A. Snyers, 'ICOs in Belgium: down the rabbit hole into legal no man's land? (Part 2)' [2018] ICCLR, in press.

Bibliography

Legal doctrine

1. A. Bal, 'Blockchain, Initial Coin Offerings and Other Developments in the Virtual Currency Market' [2018] Derivatives & Financial Instruments, Journals IBFD Volume 20, No. 2.
2. A. Bal, 'Taxing Virtual Currency: Challenges and Solutions' [2015] Intertax, 390.
3. 'Cryptocurrency ICO Stats 2018', https://www.coinschedule.com/stats.html?year=2018, accessed on 10 April 2018.
4. J. Baukema, 'Initial Coin Offerings (ICO's): crowdfunding 2.0?' [2018] TFR (NL) 113-121.
5. T. Euler, 'The Token Classification Framework' [2018], http://www.untitled-inc.com/the-token-classification-framework-a-multi-dimensional-tool-for-understanding-and-classifying-crypto-tokens/..
6. P. Hacker and C. Thomale, 'Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law' [2017] SSRN, https://ssrn.com/abstract=3075820.
7. 'IFRS – Accounting for crypto-assets' [2018] EY, http://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2018/03/EY-IFRS-Accounting-for-crypto-assets.pdf.
8. M. Langer and S. Valenta, 'Taxation of Cryptocurrency and Blockchain-Based Companies in Liechtenstein' [2018], Tax notes international.
9. R. Mooijman, 'Opgepast voor oplichting met crypto-munten' [2017] De Standaard, http://www.standaard.be/cnt/dmf20171113_03183447.
10. S. Ozelli, 'Why Switzerland is Becoming a "Crypto Nation" with a Flourishing ICO Market: Expert Take' [2018] https://cointelegraph.com/news/why-switzerland-is-becoming-a-crypto-nation-with-a-flourishing-ico-market-expert-take.
11. K. Pauwels and A. Snyers, 'ICOs in Belgium: down the rabbit hole into legal no man's land? (Part 2)' [2018] ICCLR, in press.
12. T. Sameeh, 'ICO basics – security tokens vs. utility tokens' [2018], https://www.cointelligence.com/content/ico-basics-security-tokens-vs-utility-tokens/.
13. S. Solodkiy, 'USSR's crypto paradise: $1B ICO of Abkhazia, Belarus legalizes ICOs and cryptocurrencies' [2017], https://medium.com/@slavasolodkiy_67243/ussrs-crypto-paradise-1b-ico-of-abkhazia-belarus-legalizes-icos-and-cryptocurrencies-105aec08fa1d.
14. J. Stauffer, 'The Coming Crypto Utility Token Economy: Definitions, Examples, and Why It Matters' [2018], https://medium.com/@jaredstauffer/the-coming-crypto-utility-token-economy-definitions-examples-and-why-it-matters-521f9390be69.
15. A. Snyers and K. Pauwels, 'ICOs in Belgium: down the rabbit hole into legal no man's land?' (Part 1)' [2018] ICCLR, in press.
16. N. Vandezande, 'Virtual currencies under EU anti-money laundering law' [2017] Computer Law & Security Review, No. 33.
17. F. Ventures, "The State of the Token Market report', a VC fund with a focus on Fintech, and TokenData (https://www.tokendata.io/), a platform that tracks data on token sales and ICOs, https://static1.squarespace.com/static/5a19eca6c027d8615635f801/t/5a73697bc8302551711523ca/1517513088503/The+State+of+the+Token+Market+Final2.pdf.
18. R. J. Witismann, 'Estonia to become a global ICO hub' [2018] https://medium.com/@Incorporate_ee/estonia-to-become-a-global-ico-hub-6a4a53863719.

Jurisprudence

1. Coöperatieve Aardappelenbewaarplaats, Case 154/80 [1981].
2. GFKL Financial Services, Case C-93/10 [2009] ECJ.
3. SEC v. Edwards, 540 U.S. 389 [2004].
4. SEC v. W.J. Howey Co., 328 U.S. 293 [1946].
5. Tolsma, Case C-16/93 [1994] ECJ.
6. United Housing Found., Inc. v. Forman, 421 U.S. 837 [1975].

Legislation and regulatory documents

1. 'Advice 148-1 on agreements providing staggered or successive supplies' [1984] CBN, http://www.cnc-cbn.be/files/advice/link/NL_148-01.htm.
2. 'Advice 132/6 on prepayments' [1993] CBN, http://www.cnc-cbn.be/files/advice/link/NL_132_06_Herzien_advies.pdf.
3. Belgian Code of Miscellaneous Rights and Taxes.
4. Belgian Income Tax Code.
5. Belgian VAT Code.
6. COM/2016/0450, 'Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC' [2016] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016PC0450&qid=1523358551244&from=EN.
7. Council Directive (EU) 2016/1065 amending Directive 2006/112/EC as regards the treatment of vouchers [2016] OJ L177/9.
8. 'Discussion Paper on Initial Coin Offerings, Virtual Currencies and Related Service Providers' [2017] MFSA, p. 8, https://www.mfsa.com.mt/pages/readfile.aspx?f=/files/Announcements/Consultation/2017/20171130_DiscussionPaperVCs.pdf.
9. European Parliament and Council Directive (EU) 2004/39/EC on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC [2004] OJ L145/1 (MiFID I Directive).
10. European Parliament and Council Directive (EU) 2014/65 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU [2014] OJ L173/349 (MiFID II Directive).
11. European Parliament and Council Directive (EU) 596/2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC [2014] OJ L173/1.
12. European Parliament and Council Directive (EU) 2017/1129 on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market, and repealing Directive 2003/71/EC [2017] OJ L168/12 (Prospectus Regulation).
13. 'Initial coin offerings (ICOs)' [2017] FSMA, https://www.fsma.be/sites/default/files/public/content/EN/Circ/fsma_2017_20_en.pdf.
14. Law of 2 August 2002 on the supervision of the financial sector and on financial services [4 September 2002] Belgian Official Gazette 39121 (as amended from time to time).
15. Law of 16 June 2006 on the public offering of investment instruments and on the admission of investment instruments to trading on a regulated market [21 June 2006] Belgian Official Gazette 31352 (as amended from time to time).
16. Law of 2 August 2012 on undertakings for collective investment that comply with the conditions set out in Directive 2009/65/EG and undertakings for investment in debt claims [19 October 2012] Belgian Official Gazette 63652 (as amended from time to time).
17. Law of 19 April 2014 on alternative investment funds and their managers [17 June 2014] Belgian Official Gazette 45353 (as amended from time to time).
18. Law of 25 October 2016 on the access to the investment services company and on the legal status and supervision of portfolio management and investment advice companies [18 November 2016] Belgian Official Gazette 76915 (as amended from time to time).
19. Law of 18 December 2016 on the recognition, delineation and definition of crowdfunding and containing various financial provisions, [20 December 2016] Belgian Official Gazette 87668 (as amended from time to time).
20. Law of 21 November 2017 on the infrastructures for markets in financial instruments and transposing Directive 2014/65/EU [7 December 2017] Belgian Official Gazette 107933 (as amended from time to time).
21. 'Statement in Connection with the 2017 AICPA Conference on Current SEC and PCAOB Developments' [2017] SEC, https://www.sec.gov/news/speech/bricker-2017-12-04.

22. ‘Virtual Currencies’ [2012] ECB, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.
23. ‘Statement on Crowdfunding’ [2017] FSMA, https://www.fsma.be/nl/file/49564/download?token=lm9iQG2r.
24. ‘Statement firms’ [2017] ESMA, https://www.esma.europa.eu/sites/default/files/library/esma50-157-828_ico_statement_firms.pdf.
25. ‘Statement Investors’ [2017] ESMA, https://www.esma.europa.eu/sites/default/files/library/esma50-157-829_ico_statement_investors.pdf.

THE SHARING ECONOMY – THAT NEW OLD THING

Ricardo Pazos[1]

Abstract

The 'sharing economy' is a new way of human interaction with a clear disruptive effect, both for the now existing business models and for the law. But how to address the challenges it brings from a regulatory perspective depends on how we solve a paradox. For some, the sharing economy greatly diverts from the free-market economic model, whereas for others it is precisely a concrete manifestation of it. This paper presents a general overview of the paradox and argues that the latter view is the right one. If this claim is correct, the discussion about the general regulatory framework for the sharing economy will probably amount to the classical discussion on the free-market system itself. Within this debate, scholars will have to focus more on ideas, principles and convictions than on practical grounds, statistics and numeric data, because many of the consequences of the sharing economy are hardly measurable.

Keywords: sharing economy, technology, free market, consumer protection, disrupted law

Introduction

The 'sharing economy' reflects the technological development experienced in recent years. But, with any new reality, new risks and challenges arrive. And some of the economic ideas, transactions and features encompassed within the sharing economy are not welcomed by all. There seem to be two main reasons leading to look at it with a certain degree of scepticism. On the one hand, those new challenges and risks can be highlighted to foster a high degree of regulation, remarking how the legislator needs to step in to counter some negative consequences. On the other, the sharing economy has a disruptive effect—the well-known idea of the 'creative destruction' process[2]—and this new reality may destroy much, and very fast. In this context, identifying the origins of the different sensibilities towards the sharing economy is crucial in order to set the ground for a productive debate on how to regulate it best.

This paper is organised as follows. Part I offers an overview of several perspectives regarding the sharing economy, observing a paradox. For some, the sharing economy is a change of paradigm from the 'traditional' free-market economy, whereas for others the former is just a manifestation of the latter. Part II turns to the solution of the paradox. My claim is that the sharing economy is a new way of personal interaction to satisfy economic needs and desires, which means it is a new way of doing commerce, thus a new old thing. Part III focuses on the fact that the correspondence between the sharing economy and the free-market economy explains why the suspicions towards the former are very close to the typical suspicions towards the free market as a whole—the creative destruction it entails, consumer protection issues, unfair competition risks, and so on and so forth. In addition to that, many of the effects of the sharing economy are non-measurable, thus hampering a comprehensive cost-benefit analysis of the whole. All this means that the debate on the sharing economy will get into a philosophical sphere—subjective opinions and sensibilities about the free market. Finally, Part IV briefly deals with the Uber service and its categorisation as a service in the field of transport, and not as an electronic intermediary service or an information society service.

---

[1] *Non-practicing lawyer of the Bar Association of Santiago de Compostela, Spain. Currently Postdoctoral researcher at the University of Santiago de Compostela, on a stay at Universität Bayreuth until June 2018. The topic of his dissertation was the control of the content of standard contract terms. His research interests lie in the fields of contract law, tort law, technology and law, data protection and law and economics. He is a member of SECOLA (Society of European Contract Law), GRERCA (Groupe de Recherche Européen sur la Responsabilité Civile et l'Assurance) and ELI (European Law Institute), among others.*

[2] J. A. Schumpeter, 'Capitalism, Socialism and Democracy' (London, New York: Routledge 1994) pp. 81-86.

1. The paradox regarding the approaches towards the sharing economy

The sharing economy is a concept with fuzzy lines. Under this notion, many different business models are encompassed, transportation and accommodation being just the two paradigmatic examples. Scholars have drawn several categories to classify different types of interaction between consumers. I will not go deep into this, but the reader who has been following the evolution of the sharing economy will probably be familiar to notions such as product-service systems, redistribution markets, collaborative lifestyle, collaborative production, peer-to-peer financing, and so on.[3]

Therefore, to define the topic of this paper, it is important to underline that we are not talking about one economic phenomenon, but about a series of phenomena which share some common features. It is always difficult to precise these, and I do not want to start a comprehensive analysis on the matter. That is why I will stay in a very general view, highlighting three conceptual features of the sharing economy that seem to raise not so many remarks against. The first is the importance of the Internet and new technologies for its functioning and development, thanks to the reduction of transaction costs. The second is the fact that, by way of technology, people can use other people's assets whose potential utility—or some of it—would otherwise be wasted. The third, that transactions comprised within the sharing economy are between consumers—thus making them rather 'prosumers'[4]—who, nevertheless, often benefit from the intervention of a business which aims at making a profit by providing some kind of intermediation.[5] In sum, sharing economy means consumer-to-consumer transactions aiming at granting temporary access to goods with 'excess capacity', transactions made possible thanks to new technologies.[6] However, it should be noted that some voices do not restrict the sharing economy to physical goods, stating that what is shared or exchanged can also be intangibles such as time and hobbies.[7]

The advantages of the sharing economy may be best summarised as increasing the dynamism of the market—making it simpler and more flexible, thus allowing consumers to get access to more goods and services.[8] Another aspect that is often referred to while supporting the sharing economy is its sustainability, because people do not need to become owners to benefit from goods, and the already existing assets provide welfare to more people. This would reduce the necessity of producing more and more to satisfy human needs and desires.[9] Therefore, the sharing economy could also be summarised as a sustainable technological economy.[10] Another benefit of the sharing economy is that it tends to lower prices. And this is one of the reasons why it has grown a lot in recent years—many platforms have arisen during an economic crisis which made low-cost alternatives very attractive to consumers.[11]

The sharing economy is a very alluring idea because it stimulates our altruist, unselfish side. But things are not perfect, and we can easily identify its risks, weaknesses and disadvantages. However, to some people, those aspects are not only the typical downsides any reality has, but severe problems that affect the core of the sharing economy itself. In this context, I see a paradox within the debate, and future regulation may depend on how we solve it.

---

[3] See Á. Carrasco, 'Consumer sharing economy: a critique of the fallacy' [17 April 2015] Blog CESCO 1; A. M. de la Encarnación, 'El alojamiento colaborativo: Viviendas de uso turístico y plataformas virtuales' [2016] 5 Revista de Estudios de la Administración Local y Autonómica: Nueva Época 34.

[4] See A. de Franceschi, 'European Contract Law and the Digital Single Market. Current Issues and New Perspectives', in A. de Franceschi (ed.), 'European Contract Law and the Digital Single Market. The Implications of the Digital Revolution' (Cambridge, Antwerp, Portland: Intersentia 2016) pp. 4-5.

[5] See Á. Carrasco, *Ibid*., pp. 1-3.

[6] K. Frenken and J. Schor, 'Putting the sharing economy into perspective' [2017] Environmental Innovation and Societal Transitions 4 p. 23-5. See also C. Twigg-Flesner, 'Disruptive Technology – Disrupted Law? How the Digital Revolution Affects (Contract) Law' in A. de Franceschi (ed.), 'European Contract Law and the Digital Single Market. The Implications of the Digital Revolution' (Cambridge, Antwerp, Portland: Intersentia 2016) p. 29.

[7] M. N. Pacheco Jiménez, 'La Web 2.0 como instrumento esencial en la economía colaborativa: auge de negocios de dudosa legalidad' [2016] Revista CESCO de Derecho de Consumo 17 p. 77.

[8] M. L. de Castro, '¿Por qué es buena la economía colaborativa desde el punto de vista del consumidor? ¿Qué le trae de positivo?' [17 April 2015] Blog CESCO 1.

[9] K. Frenken and J. Schor, *Ibid*., p. 6.

[10] A. M. de la Encarnación, *Ibid*., p. 50.

[11] P. Jarne Muñoz, 'El consumo colaborativo en España: experiencias relevantes y retos de futuro' [2016] Revista CESCO de Derecho de Consumo 17 p. 63.

On the one hand, there are many people who maintain a rather positive view on the sharing economy. Of course, they highlight the risks it brings, but they place themselves—explicitly or tacitly—in favour of the sharing economy as such. One of the issues this first group emphasize on while pointing at the advantages of the sharing economy, is the difference between this and the traditional free-market economy. In short, they present those two models as substantively different. The sharing economy is perceived as an example of a pro-consumer era where people take the prominent spot. In contrast, the industrial-era economy would place the focus on entrepreneurs, whose products and services are even said to be offered *against* consumers. With this background, the sharing economy is welcomed because it allows satisfying human needs and desires through 'non-commercial acts'.[12] Also reflecting this perspective, it is maintained that the sharing economy takes the idea of replacing the competition-based, free-market economy with a cooperation-based, collaborative one.[13] The new model would take into account ideas alien to the old one—such as citizen welfare, social justice, cultural exchanges or communal life—fostering a new philosophy where benefits are not purely economic, but also emotional.[14] It would be a trend against the consumption society we are living in.[15]

On the other hand, there are critics of the sharing economy precisely because they see big correspondences between it and the free-market economy. For example, a Spanish journalist argues that the so-called 'gig economy'[16] is included within the 'alternative systems' which also encompass the 'sharing economy', the 'gift economy' and the 'barter economy' just to give it a better outfit, stating that 'gigging' is just a nice word for 'exploitation'.[17] When scholars outline the risks of the sharing economy, some of these are typical problems associated with the market as a whole. Among other points raised by a Spanish scholar who places himself explicitly 'against the market-consumer-oriented shared economy', we found that the sharing economy goes against the current trend of consumer protection, which is not about fostering cheap prices, but high quality and safety. The sharing economy would be a step backwards, causing a race to the bottom.[18] Even those who are in favour of the sharing economy admit that it entails risks regarding consumer and employee protection, taxes, data protection, and the system of permits and licences.[19]

There is also a third group of people who welcome the sharing economy because they see it as an example of free-market capitalism. A commentator who is not fond of small government and deregulation has qualified the sharing economy as 'a libertarian's dream in terms of creating economic models without rules'.[20] Criticism to this assertion aside—because libertarianism obviously does not mean 'no rules'—it is undeniable that people who are more free-market oriented tend to embrace the sharing economy. For them, it benefits consumers and reveals shortcomings of regulation which is outdated or counterproductive, or that protects some business models from competition.[21] For example, if accommodation services within the sharing economy pose problems because a given rule does not allow spare rooms in touristic houses to be offered—the house must be offered in full—one can use it as a first step to start a debate on whether or not such a rule makes sense.[22] According to this third view, the sharing economy should be welcomed because, at least so far, 'it has overcome market imperfections without recourse to regulatory bodies prone to capture by entrenched firms'.[23]

---

[12] See M. L. de Castro, *Ibid*., pp. 1, 3.
[13] A. Beltran i Cangròs, 'Plataformas de economía colaborativa: una mirada global' [2018] The Ostelea School of Tourism & Hospitality p. 9.
[14] A. M. de la Encarnación, *Ibid*., pp. 31, 34, 50.
[15] P. Jarne Muñoz, *Ibid*., p. 63.
[16] According to the online Cambridge dictionary, 'a way of working that is based on people having temporary jobs or doing separate pieces of work, each paid separately, rather than working for an employer'.
[17] X. M. Pereiro, 'Exploit Yourself' [2017] Luzes 46 p. 23.
[18] Á. Carrasco, *Ibid*., pp. 4-7.
[19] M. L. de Castro, *Ibid*., p. 3.
[20] M. Lux, 'A Libertarian Dream: The "Sharing Economy"' [19 May 2015] The Huffington Post.
[21] See B. Hunter, 'In The Sharing Economy, The Consumers Are The Real Winners' [11 October 2016] Generation Opportunity.
[22] For just one instance, see article 66(2) of the Catalan Decree 159/2012, dated 20 November 2012. See also A. M. de la Encarnación, *Ibid*., pp. 43-45.
[23] C. Koopman, M. Mitchell and A. Thierer, 'The Sharing Economy and Consumer Protection Regulation: The Case for Policy Change' [2015] Journal of Business, Entrepreneurship & the Law 8 pp. 530, 539-543.

2. Solving the paradox. The sharing economy, that new old thing

I do not want here to openly take sides on the look towards the free market. I would like to limit myself to the question on whether or not the sharing economy and the classical free-market models are substantively different. If the answer were affirmative, the perspective previously outlined first would seem the right one. If it is negative, then the debate on the sharing economy would basically consist on a debate about the free market and economic policy.

As ADAM SMITH famously coined, 'it is not from the benevolence of the butcher, the brewer, or the baker, that we expect our dinner, but from their regard to their own interest'.[24] He was not promoting isolated and selfish human beings, and a quick look at another book, The Theory of Moral Sentiments, shows us he strongly believed human beings are compassionate, emotional and empathetic.[25] But free-market capitalism relies on the fact that progress can be better achieved when people with no special feelings towards each other collaborate—often without being aware of it—while exercising their personal freedom. People have skills and goods they can trade with, but if they are free, they will do so only when they gain. And it would not be possible to enjoy the simplest goods and services of everyday life without the collaboration of many different people. People participating in the process are not particularly interested in satisfying the demand of the ultimate consumer as such, and they do not enter the chain for the sake of it. They do it because satisfying the needs and desires of others is a necessary and previous step to satisfy their own. Thus, the free market compels you to help others first as the only way to reach your own goals.[26]

Therefore, it is a big mistake to attach notions such as 'cooperation' or 'collaboration' to the sharing economy and deny that those concepts are inherent to the free market.

First, because all exchanges need them both. Denying the collaborative nature of the free market may be an instance of what has been coined 'emporiophobia' or 'fear of markets'. That is, an anti-market tendency arises by associating the marketplace with rogue competitors who would do anything to make more profits. The main idea behind 'emporiophobia' would be that unless the market is heavily regulated, we would witness a rumble in the jungle where only the strong survive and all the rest are left behind. However, this perspective forgets that businesses compete to get clients, that is, they compete to be them, and not the rest, the ones who cooperate the most with consumers. With the first view, competition and the market itself is a zero-sum game. With the second view, competition is just a process where people try to satisfy other people's needs and desires in the best possible way.[27] In short, one may criticise the market for many things, but definitely not for lack of cooperation.

And second, because the sharing economy also has self-interest behind. Nobody enters a contract if he does not think he will be better-off after concluding the deal. The same applies in the sharing economy.[28] The novelty of the sharing economy is that, thanks to new technologies—and businesses acting as intermediaries—transaction costs and information uncertainty get lower. This makes it possible for everybody to obtain benefits which in other times were unthinkable, and creates a scenario of trust, essential to bring people together.[29] Think about accommodation and transportation, the two paradigmatic services of the sharing economy. Consumers realise they have free rooms, apartments or car seats. And, instead of using them for lower goals or not using them at all, the sharing economy allows them to make a profit. Companies see a way of making a profit, too, and they invest to invent the technology that will bring consumers closer, erase barriers, and allow them to benefit more from each other.

---

[24] A. Smith (ed. E. Cannan), 'An Inquiry into the Nature and Causes of the Wealth of Nations' (London: Methuen 1904) Vol 1, p. 43.
[25] A. Smith (ed. D. Stewart), 'The Theory of Moral Sentiments' (London: Henry G. Bohn 1853).
[26] As brilliantly explained by L. A. Read, 'I, Pencil' [1958] The Freeman 8 pp. 32-37.
[27] On this issue, see P. H. Rubin, 'Emporiophobia (Fear of Markets): Cooperation or Competition?' [2014] Southern Economic Journal 80 p. 875-889.
[28] K. Frenken and J. Schor, *Ibid*., p. 6.
[29] A. Hira and K. Reilly, 'The Emergence of the Sharing Economy: Implications for Development' [2017] Journal of Developing Societies 33 p. 176.

Of course, one may argue that, insofar as profits and intermediaries get into the picture, the sharing economy is not about sharing anymore.[30] But then it is necessary to understand that this new model will remain with a limited role. Unlike some commentators maintain,[31] it is not that the development of the sharing models has been 'accompanied' by an increase in its commercial nature—it is that without this commercial nature, the sharing models would not have developed that much.

The sharing economy is disruptive because the technology needed is a new one and creates new markets.[32] But it creates new markets in the sense of making it possible to establish new interpersonal relationships, not in the sense of providing completely new services. Sharing is not new, nor are cooperative behaviour, non-for-profit actions, philanthropy, donations of second-hand goods, and so on. But profits bring the incentive to make the necessary efforts to enter the market, they bring an advantage to make up for assuming the risk of dealing with strangers, and they foster innovation by businesses to provide the essential network large-scale cooperation requires. This idea must not be undervalued. The sharing economy is a revolution precisely because it makes *direct* cooperation with complete strangers feasible, while, historically, direct cooperation had been rather limited to people within the same geographical area, and mainly with relatives and friends.[33] In sum, erase profits for whatever reason and you may have a 'real' sharing economy, but one with much lower potential—less interpersonal cooperation—than the sharing economy now developing. Whether this outcome would be good or bad, that belongs to each person's subjective opinion.

Under no circumstances must all this be understood as claiming that non-for-profit actions would disappear, nor that there would not exist any 'truly altruist' sharing economy model. But altruism is better captured as a way of self-interest. The actor does not sacrifice himself for others in the sense that he surrenders a higher value for a lesser one. Looking at altruism this way would require people to harm themselves in order to help others, and it would lead us to see altruism as a zero-sum game. What really happens is that the altruist integrates another person's well-being into his own.[34] An altruist action should be regarded as follows: 'the uneasiness the actor wants to remove is his own present dissatisfaction with the expected state of other people's affairs in various periods of the future. In taking care of other people he aims at alleviating his own dissatisfaction'.[35] This alternative understanding of altruism as 'empathetic self-interest' fosters benevolence because it shows that both persons experience gains, and it is more realistic because it takes into account that humans care for others. But, obviously, we all care more about relatives and friends than about strangers. This explains why it will be impossible for a sharing economy without economic benefits to maintain the degree of personal cooperation there is nowadays—monetary profit makes it easier to find situations where satisfying other people's well-being is a previous step to satisfy your own.

Another aspect to comment is that some people draw a distinction between business models within the sharing economy. They deny that transportation services through an application like Uber amounts to a 'sharing method', claiming that, on the contrary, the agreement to split costs in a trip using BlaBlaCar is 'sharing'.[36] In my view, this statement is wrong. As I have said, economy is all about collaboration and cooperation. Self-interest is just the fuel—what brings people together, but exchanges and deals require those people actually being together, having opposed but complementary goals, and satisfying somebody else's needs and desires to satisfy their own. The sharing economy follows the same pattern. One person can provide something to others and those others are willing to pay money for that, which is what the first person wants. All are pursuing a benefit, including the driver who offers spare car seats to split costs. Insofar as he would do the trip anyway, the whole cost of the trip is a sunk cost, a 'loss' the driver will

[30] A. M. de la Encarnación, *Ibid*., pp. 51-52; P. Jarne Muñoz, *Ibid*., p. 72.
[31] See P. Jarne Muñoz, *Ibid*., p. 67.
[32] See C. Twigg-Flesner, *Ibid*., pp. 22-23.
[33] K. Frenken and J. Schor, *Ibid*., pp. 4, 6.
[34] See A. Rand, 'The Virtue of Selfishness. A New Concept of Egoism (With Additional Articles by Nathaniel Branden)' (New York: Signet 1964) pp. 49-53.
[35] L. von Mises, 'Human Action. A Treatise on Economics (The Scholar's Edition)' (Auburn: Ludwig von Mises Institute 1998) p. 496.
[36] X. M. Pereiro, *Ibid*., p. 22.

assume entirely if no companions are found. This implies the money paid by the other travellers represents a price for a service—transportation—and a true benefit for the driver.[37]

When you take this into consideration, there is another argument that seems to lose strength. Some point out that trips made through transportation services like Uber will not be made at all if nobody demands them, whereas in car-sharing schemes, such as the one of BlaBlaCar, the trip will be done anyway, but without companions. That implies Uber is an on-demand service, whereas BlaBlaCar is sharing economy.[38] In other words, Uber is professionalised and drivers can make of it a substantial source of income, while drivers in BlaBlaCar are also satisfying a personal need for transportation and therefore cannot supply the service to others on such a regular basis.[39] But, when somebody puts his private property, his labour force or his skills at the disposal of others in exchange of a price—as the driver does in both the transportation and the car-sharing contexts—we call it a market transaction. In this sense, there is no substantive difference between the two examples referred to, nor between the sharing and the traditional economies.[40] If you want the car-sharing to be completely non-for-profit, what you will have is just 'digital hitchhiking'. Would this success? The answer depends on two questions. First, would many drivers want to give someone a ride, trading some minutes to pick people up and drop them off, just to not to travel alone—which in fact is also an example of self-interest? Second, would someone want to invest on the technology to run the system?

The sharing economy is a new old thing—using what is yours to improve your well-being by improving other's well-being first. A marketplace for underutilised goods and services of any kind, where people may want to get in for monetary or non-monetary benefit.[41] And this new way of doing commerce is possible because some companies are pursuing their own self-interest to provide consumers the technology that allows them to come closer and make deals. The sharing economy is just the market, at its best or at its worst, depending on your view about the market itself.

3. Some regulatory challenges of the sharing economy, and the framework for an intellectual debate

Since the sharing economy is a concrete expression of the free-market model, the discussion about the regulatory system to be implemented to best tackle its shortcomings will be similar to the general discussion about the free market itself. After all, as I have already pointed out, many of the risks of the sharing economy coincide with the perceived risks of free-market capitalism. Therefore, the discussion will probably reflect the different sensibilities towards the market, and it will be done in the field of ideas, principles and convictions. This becomes more probable because it looks like only a few of the vast array of consequences of the sharing economy can be measured and quantified. If this forecast turns out to be correct, scholars must be ready to debate not only on practical grounds, but—mainly—on ideas. Let me give some examples of challenges brought by the sharing economy that will probably require a principle-based discussion rather than a practical one.

Nobody questions how disruptive the sharing economy is. It endangers existing business models, because traders operating in traditional schemes must comply with many rules and standards that sharing economy operators might avoid, the latter gaining market share at the expense of the former.[42] In this context, the fact of not playing with the same rules may result in accusing the newcomers of unfair competition.[43]

All new business models that survive in the market are creating something new and destroying something old at the same time. And the more creative and the more destructive, the larger the

[37] Against this conclusion, see P. Jarne Muñoz, *Ibid*., p. 71. On the issue of car-sharing, without a total coincidence with the reasoning followed, see Á. Carrasco, *Ibid*., pp. 5-6.
[38] K. Frenken and J. Schor, *Ibid*., p. 5.
[39] P. Jarne Muñoz, *Ibid*., pp. 66, 71.
[40] Although the difference regarding the frequency of transactions raise questions on whether the consumer-service provider is still a consumer or has become a trader. See C. Twigg-Flesner, *Ibid*., pp. 34-36.
[41] As described by C. Koopman, M. Mitchell and A. Thierer, *Ibid*., p. 531.
[42] K. Frenken and J. Schor, *Ibid*., p. 6.
[43] A. M. de la Encarnación, *Ibid*., p. 50; A. Hira and K. Reilly, *Ibid*., p. 178.

improvement is in comparison to what there was before. Whether or not in each case the creation makes up for the destruction is certainly difficult to measure, becoming prone to an intellectual debate founded on subjective considerations.

Regarding the unfair competition claim, there is an obvious counter-argument. The rules currently in force are justified on grounds such as consumer protection. If that is so, newcomers who do not comply with those rules cannot offer their clients that 'government-sanctioned quality label'. Therefore, accusing the new of unfair competition could amount to a tacit admission that the relevant rules are not needed anymore, that they create a heavy burden without providing correspondent benefits that consumers value highly. The claim of unfair competition could also be questioned in the following way. Are we sure that many rules currently in force, under nice justifications, are not indeed protecting the position of the established firms by creating barriers to entry? Are we sure that when some companies promote high standards, it is not because they want to increase costs to all their competitors and make them play on the field the former are good at?[44]

Ask these questions to someone more prone to a rather deregulated free market, he will tell you that this is exactly what is happening. He will suggest that the right thing to do is not to constrain the new models with old rules, but to free the old models from those rules.[45] Ask that to someone more prone to economic regulation, he will provide a complete different answer. The latter will argue that all those rules are necessary, and that the creative destruction process should only take place if it respects them. The former would accuse those more favourable to regulation of something like applying the 'logic of dead men' instead of the 'logic of living people', the two kinds of logic referred to by Netti, one of the characters in ALEXANDER BOGDANOV's 1912 novel *Engineer Menni*. According to that character, two opposed conclusions can be reached with the same premises without falling in hypocrisy. It just depends on the kind of logic applied. The logic of living people aims at moving ahead and improving, while the one of dead men aims at peace, immobility, standstill.[46]

The same happens with market failures, which is another aspect where the sharing economy raises some concerns, just exactly as the free-market does.[47] Although the notion of market failure is widely admitted, for some it is itself a failure based on two grounds. First, because when the market is deemed to be failing, the standard of comparison is a completely unrealistic scenario where humans are perfect—and therefore not humans anymore. Second, because the notion tacitly leads to the assumption that regulators can correct the failure and improve the outcome, something which is not always so.[48] Market imperfections are opportunities for businesses because the market is a dynamic process, whereas good intentions regulators may have do not always translate into good regulation.[49]

The sharing economy has developed thanks to the fact that, so far, intermediaries have been able to put in practice a framework that creates mutual trust between strangers, for example with review and rating systems. Despite admitting this, scholars warn of the shortcomings of such systems, arguing that harmonisation to set common rules and standards is the best way to correct these weaknesses.[50] The conclusion is appealing, but it will be subjected to criticism by those more favourable to the free market. If that framework of trust loses its reliability, platforms will cease making a profit. In this scenario, businesses have a powerful incentive to correct the shortcomings themselves. Besides, it could be said that harmonised rules stifle competition—also at the regulatory level, might respond to special interests, and discourage innovation. Therefore, the room for debate on non-measurable issues remains.

---

[44] C. Koopman, M. Mitchell and A. Thierer, *Ibid*., pp. 534-539.

[45] C. Koopman, M. Mitchell and A. Thierer, *Ibid*., p. 544.

[46] See L. R. Graham and R. Stites (Indiana University Press 1984), p. 212, https://ia800309.us.archive.org/1/items/BogdanovRedStar/Bogdanov%20-%20Red%20Star%20-%201984.pdf.

[47] A. Hira and K. Reilly, *Ibid*., p. 179.

[48] See S. Horwitz, 'The Failure of Market Failure' [8 December 2011] Foundation for Economic Education.

[49] C. Koopman, M. Mitchell and A. Thierer, *Ibid*., pp. 532-534.

[50] See C. Busch, 'Crowdsourcing Consumer Confidence. How to Regulate Online Rating and Review Systems in the Collaborative Economy' in A. de Franceschi (ed.), 'European Contract Law and the Digital Single Market. The Implications of the Digital Revolution' (Cambridge, Antwerp, Portland: Intersentia 2016) p. 223-243.

Another risk relates to consumer protection, because the sharing economy may lead to 'low-cost, low-quality' business models which deprive consumers of legal rights and safety standards.[51] Again, the debate would be set in terms of principles and subjective views. Consumer protection can become a tool to set standards according to what some companies and lawmakers desire, and to steer all people towards a single set of economic patterns. The sharing economy would have the potential to disrupt this insofar as it can offer more tailor-made services and choice.[52] Depending on your personal stand, these remarks will be sheer nonsense or an accurate description of the situation. Regulatory issues around new technologies merely reflect the eternal general debate on consumer protection within the free market - how to strike a balance to place users in a good position vis-à-vis traders without stifling competition and innovation, designing sufficiently flexible rules to make them adaptable to new circumstances.[53]

In any case, there are two aspects that should not be forgotten. First, increasing consumer protection entails an increase in operating costs and prices that might offset the benefits of the former. Second, the sharing economy platforms have already tried to develop systems to ensure consumers have a minimum degree of safety, essential to earn their trust.[54] Does this lead to make a general case for deregulation? For some, absolutely yes.[55] Others remain sceptical and warn about the dangers of such an approach.[56]

Another possible downside attributed to the sharing economy is that the gains it entails may not be evenly distributed. If that is so, the sharing economy would be a cause of income inequality.[57] Here we have another philosophical discussion. Is a somehow patterned distribution of income and wealth fair and desirable? If this question is asked to someone who shares ROBERT NOZICK's view outlined in *Anarchy, State and Utopia*, the answer will be a clear no—it does not matter which pattern you choose, it will always be contrary to personal freedom and will require permanent intervention and control over people, thus being illegitimate.[58] According to the latter view, it should not be hoped that the sharing economy decreases inequality, but poverty. The right hopes would then be better described as granting 'access and mobility' to the poorest ones.[59]

In other contexts, you can certainly measure some effects of the sharing economy, but the numbers cannot provide an image of the whole situation. For example, you can observe if housing prices for long-term rentals increase when many owners decide not to enter that market, but the one for short-term accommodation through the sharing economy. But higher prices would mean there is a business opportunity to enter the housing market. Companies would have an incentive to build housing units, and ordinary people would have an incentive to put on sale secondary residences, or to move to another area selling or renting their old home at a sufficiently good price. If housing prices increase in touristic cities, people also might tend to accept more often job offers in other places. The overall costs and benefits of these outcomes are impossible to measure. It is difficult to put into question that, regarding the adaptation of the law to new technologies from a regulatory perspective, 'an appropriate cost-benefit analysis is crucial'.[60] The problem comes before that—is such an appropriate analysis possible at all within the sharing economy?

One could go on and on stressing non-measurable, potential consequences of the sharing economy, but this part will end mentioning just another two. First, concerning accommodation services, nuisances to neighbours and a feeling of insecurity due to the higher contact with strangers.[61] Second,

[51] A. M. de la Encarnación, *Ibid*., p. 45-47.
[52] See C. Koopman, M. Mitchell,´and A. Thierer, *Ibid*., pp. 531-532.
[53] See A. de Franceschi, *Ibid*., p. 17; C. Twigg-Flesner, *Ibid*., pp. 23-25.
[54] P. Jarne Muñoz, *Ibid*., pp. 73-74.
[55] See C. Koopman, M. Mitchell and A. Thierer, *Ibid*., pp. 529-545.
[56] C. Twigg-Flesner, *Ibid*., p. 25.
[57] K. Frenken and J. Schor, *Ibid*., p. 7.
[58] R. Nozick, 'Anarchy, State, and Utopia' (Oxford: Basil Blackwell 1974) pp. 155-164.
[59] See A. Hira and K. Reilly, *Ibid*., pp. 177, 181.
[60] A. de Franceschi, *Ibid*., p. 16.
[61] A. M. de la Encarnación, *Ibid*., pp. 47-49; K. Frenken and J. Schor, *Ibid*., p. 6.

an increase in for-profit sharing methods may reduce the availability of assets for the more classical free-basis sharing mainly within the family and friendship contexts, possibly harming social cohesion.[62]

4. Uber, a service in the field of transport or a mere intermediary?

One issue that I would like to cover in this paper, even if it must be briefly, is the categorisation of Uber as a transport service provider, or as an electronic intermediary service or an information society service. The Court of Justice of the European Union answered to this question in its judgement *Asociación Profesional Élite Taxi*, ruling that the intermediation activity is 'inherently linked to a transport service', thus compelling to classify it as 'a service in the field of transport'.[63] The decision is not surprising, because it is founded on a well-known ground. Scholars have differentiated platforms which are merely 'passive' intermediaries from those that set out the rules according to which goods and services can be offered through the platform, including the price.[64] With this in mind, it looks logical that a service like Uber's, which sets out most of the conditions of the transaction between the driver and the user, is categorised as a transport service.

However, another approach is equally possible, concluding that the service provider is each driver, and that the application remains just the link between the provider and the user. To make its business model successful, the company must overcome important information asymmetries, something it does by regulating contract terms. Consumers do not need to inquire about the price, the quality of the driver or the vehicle's condition, because they know beforehand that all drivers found in Uber meet some given standards and operate under certain conditions. Thanks to that, the transport service becomes more alluring, and the business can make a profit offering the technology needed to bring people together. In other words, Uber sets out important contract features because it is the only way to make the transport service that others provide simple and attractive enough.[65] In short, Uber does not fix the terms of *their* drivers, it only links users to transport service providers who operate under a given set of rules.

With this short remark I would like to make just one point. A typical discussion about the legal challenges brought by new technologies is to which extent old rules are suited to the new challenges, if we need to adapt those rules, or if we have to pass new regulation because it is impossible or inconvenient to reshape them—all three options having both advantages and disadvantages.[66] But to make a decision on this, before we must correctly understand and categorise the reality we are analysing. And within the sharing economy business models, that is not always easy.

Conclusion

A famous parable found in the Bible refers to pouring *new wine into old wineskins*, recommending not to do it so the wineskins do not break and the wine does not spill.[67] This can be taken as guidance to implement a whole new set of rules for the sharing economy, instead of using classic legal categories and well-known principles. However, the sharing economy is better understood as *old wine*—commerce as the substance—*into new wineskins*—the sharing economy as the shape the substance takes. This leads us to a smoother approach towards the law currently applied, and to hold that the disruption of the law caused by a disruptive technology does not necessarily have to result in a complete legal revolution.

The fact that the sharing economy is just a new way of doing commerce has one major implication. Much of the debate on it from a regulatory perspective is going to fall on the same grounds as the general debate on how much room we should leave to the free market. However, the sharing economy is revealing how heterogeneous the effects of interaction within the market process are. It is extremely difficult to grasp all the consequences the several phenomena entail, and it is even more difficult to quantify all costs and

[62] K. Frenken and J. Schor, *Ibid*., p. 8.
[63] CJEU judgement Asociación Profesional Élite Taxi, Case C-434/15 [2017] ECLI:EU:C:2017:981.
[64] C. Twigg-Flesner, *Ibid*., pp. 28-29, 36-37, 46-47.
[65] See J. R. Rallo, 'Con o sin sentencia, acabemos con las licencias de taxi' [2º December 2017] El Confidencial.
[66] See C. Twigg-Flesner, *Ibid*., pp. 25-27.
[67] Matthew 9:17, Mark 2:22; Luke 5:37.

benefits, because many of the outcomes are non-measurable. This can result in a certain change of approach towards social sciences, one in which practical and mathematical models leave more room to a philosophical debate on ideas. Such a change would make it harder to reach consensus, and it would compel us to focus on convictions. Whether or not this would be bad, it is up for discussion.

Finally, the sharing economy as consumer-to-consumer transactions raises another issue. Economic regulation is perceived to affect mostly businesses, and ordinary people do not always identify its effects. From now on, consumers will be more aware, possibly changing their views on the creative destruction process and on the role of legislators and policymakers. Therefore, the applicable rules to the sharing economy will need to better reflect social perceptions, and that is why scholars would do bad in limiting themselves to a pure 'intellectual' discourse. It is time to get closer to people, just like the sharing economy inspires to do.

Bibliography

1. A. Beltran i Cangròs, 'Plataformas de economía colaborativa: una mirada global' [2018] The Ostelea School of Tourism & Hospitality, https://static.hosteltur.com/web/uploads/2018/03/Informe_Economya_Colaborativa_Ostelea.pdf.
2. C. Busch, 'Crowdsourcing Consumer Confidence. How to Regulate Online Rating and Review Systems in the Collaborative Economy' in A. de Franceschi (ed.), 'European Contract Law and the Digital Single Market. The Implications of the Digital Revolution' (Cambridge, Antwerp, Portland: Intersentia 2016).
3. Á. Carrasco, 'Consumer sharing economy: a critique of the fallacy' [17 April 2015] Blog CESCO 1, http://blog.uclm.es/cesco/files/2015/04/SHARING-ECONOMYali.pdf.
4. M. L. de Castro, '¿Por qué es buena la economía colaborativa desde el punto de vista del consumidor? ¿Qué le trae de positivo?' [17 April 2015] Blog CESCO, http://blog.uclm.es/cesco/files/2015/04/Por-qu%C3%A9-es-buena-la-econom%C3%ADa-colaborativa-desde-el-punto-de-vista-del-consumidor.pdf
5. CJEU judgement Asociación Profesional Élite Taxi, Case C 434/15 [2017] ECLI:EU:C:2017:981.
6. A. M. de la Encarnación, 'El alojamiento colaborativo: Viviendas de uso turístico y plataformas virtuales' [2016] 5 Revista de Estudios de la Administración Local y Autonómica: Nueva Época 34. DOI: http://dx.doi.org/10.24965/reala.v0i5.10350
7. A. de Franceschi, 'European Contract Law and the Digital Single Market. Current Issues and New Perspectives', in A. de Franceschi (ed.), 'European Contract Law and the Digital Single Market. The Implications of the Digital Revolution' (Cambridge, Antwerp, Portland: Intersentia 2016).
8. K. Frenken and J. Schor, 'Putting the sharing economy into perspective' [2017] Environmental Innovation and Societal Transitions 4, DOI: https://doi.org/10.1016/j.eist.2017.01.003.
9. L. R. Graham and R. Stites (Indiana University Press 1984), https://ia800309.us.archive.org/1/items/BogdanovRedStar/Bogdanov%20-%20Red%20Star%20-%201984.pdf.
10. A. Hira and K. Reilly, 'The Emergence of the Sharing Economy: Implications for Development' [2017] Journal of Developing Societies 33, DOI: 10.1177/0169796X17710071.
11. S. Horwitz, 'The Failure of Market Failure' [8 December 2011] Foundation for Economic Education, https://fee.org/articles/the-failure-of-market-failure/.
12. B. Hunter, 'In The Sharing Economy, The Consumers Are The Real Winners' [11 October 2016] Generation Opportunity, https://blog.generationopportunity.org/articles/2016/10/11/in-the-sharing-economy-the-consumers-are-the-real-winners/.
13. P. Jarne Muñoz, 'El consumo colaborativo en España: experiencias relevantes y retos de futuro' [2016] Revista CESCO de Derecho de Consumo 17, https://www.revista.uclm.es/index.php/cesco/article/view/998.
14. C. Koopman, M. Mitchell and A. Thierer, 'The Sharing Economy and Consumer Protection Regulation: The Case for Policy Change' [2015] Journal of Business, Entrepreneurship & the Law 8, https://digitalcommons.pepperdine.edu/cgi/viewcontent.cgi?referer=https://www.google.de/&httpsredir=1&article=1130&context=jbel.

15. M. Lux, 'A Libertarian Dream: The "Sharing Economy"' [19 May 2015] The Huffington Post, https://www.huffingtonpost.com/mike-lux/a-libertarian-dream-the-sharing-economy_b_7313014.html.
16. L. von Mises, 'Human Action. A Treatise on Economics (The Scholar's Edition)' (Auburn: Ludwig von Mises Institute 1998), https://mises.org/sites/default/files/Human%20Action_3.pdf.
17. R. Nozick, 'Anarchy, State, and Utopia' (Oxford: Basil Blackwell 1974).
18. M. N. Pacheco Jiménez, 'La Web 2.0 como instrumento esencial en la economía colaborativa: auge de negocios de dudosa legalidad' [2016] Revista CESCO de Derecho de Consumo 17, https://www.revista.uclm.es/index.php/cesco/article/view/1055.
19. X. M. Pereiro, 'Exploit Yourself' [2017] Luzes 46.
20. J. R. Rallo, 'Con o sin sentencia, acabemos con las licencias de taxi' [2º December 2017] El Confidencial, https://blogs.elconfidencial.com/economia/laissez-faire/2017-12-20/sentencia-tjue-taxi-uber-licencias_1496098/.
21. A. Rand, 'The Virtue of Selfishness. A New Concept of Egoism (With Additional Articles by Nathaniel Branden)' (New York: Signet 1964).
22. L. A. Read, 'I, Pencil' [1958] The Freeman 8, https://fee.org/media/1947/1958-12.pdf.
23. P. H. Rubin, 'Emporiophobia (Fear of Markets): Cooperation or Competition?' [2014] Southern Economic Journal 80, DOI: 10.4284/0038-4038-2013.287.
24. J. A. Schumpeter, 'Capitalism, Socialism and Democracy' (London, New York: Routledge 1994), http://cnqzu.com/library/Economics/marxian%20economics/Schumpeter,%20Joeseph-Capitalism,%20Socialism%20and%20Democracy.pdf.
25. A. Smith (ed. E. Cannan), 'An Inquiry into the Nature and Causes of the Wealth of Nations' (London: Methuen 1904) Vol 1, http://lf-oll.s3.amazonaws.com/titles/237/Smith_0206-01_EBk_v6.0.pdf.
26. A. Smith (ed. D. Stewart), 'The Theory of Moral Sentiments' (London: Henry G. Bohn 1853), http://lf-oll.s3.amazonaws.com/titles/2620/Smith_TMS-Languages1648_Bk.pdf.
27. C. Twigg-Flesner, 'Disruptive Technology – Disrupted Law? How the Digital Revolution Affects (Contract) Law' in A. de Franceschi (ed.), 'European Contract Law and the Digital Single Market. The Implications of the Digital Revolution' (Cambridge, Antwerp, Portland: Intersentia 2016).

THE RIGHT TO BE OFFLINE. ANALYSIS OF THE PROBLEM IN THE LIGHT OF WORK LIFE BALANCE CONCEPTION

Pietras Aleksandra[1]

Abstract

In the age of development of modern technologies, the boundaries between professional and private life gradually become blurred. Wider access to the Internet and the use of mobile devices in the process of providing work induce reflection on the extent to which labour law norms should affect the sphere of professional and private lives of employees. It is equally important to consider what measures in the field of work-life balance should be reflected in the content of the labour code.

In France, since the 1st of January 2017, regulations to limit the possibility of contact with employees after working hours, so called "the right to be offline", have come into force. Pursuant to these provisions, employers are therefore obligated to agree with employees on situations in which it would be acceptable to receive business calls or e-mails during their free time.

In Poland, the issue of contact with employees after working hours has not been regulated so far, which raises many doubts in practice. One of them relates to the possibility of recalling an employee from leave in a situation when an employee has the phone off and did not leave the employer any information as for their whereabouts. In addition, the question arises, whether the current provisions of the Labour Code constitute a sufficient basis to protect employees from the risks associated with the expectation of their availability also after business hours. There is no doubt that "special needs of the employer" justifying overtime work or an employee's duty to care for the good of the employing establishment, due to lack of provisions regulating the contact with employees in time off work, can in fact create room for abuse for employers.

Keywords: work-life balance, employment relationship, modern technologies, right to be offline

Introduction

The development of modern technologies has changed the way people perceive work, leading to gradual blurring of the boundaries between private and professional life. Currently, we can talk about the progressive "digitization of work", which, on one hand, has made human work more flexible, on the other hand also involving the employee not only physically, but also mentally - regardless of the time and place of performing tasks. Therefore, it is being increasingly referred to the need to set the boundaries between work and private life. On the other hand, it is pointed out that in the near future, intelligent machines will annihilate many jobs[2]. From the perspective of the work-life balance, it seems that the fulfilment of such a scenario would have many advantages. A man with more free time could perform his obligations also outside of professional life, moreover, a longer and undisturbed rest would allow for a more efficient use of shorter working time. Undoubtedly, the issue of the impact of technological changes on the labour market is an important and complex issue, that is why it is difficult to determine with what problems law-makers will tackle, even though several important ones emerge against this background already today.

In the first place, one should consider to what extent people will be able to benefit from the technological revolution. It is rightly pointed out that the progressive digitization of work can render many people jobless, which will lead to deep divisions of society and economic inequalities[3]. Taking into account the positive approach to freedom of work, reflected in the constitutional provisions and the Labour Code,

---

[1] *PhD student at the University of Lodz (Poland), Faculty of Law and Administration, Department of Labour Law. Research interests are related to the topic of doctoral dissertation: The impact of work-life balance conception on the protection of personal interests in the employment relationship".*

[2] Y. N. Harari "The mystery of immortality" [2018] Newsweek Poland 14 pp. 26-27.

[3] *Ibid*.

it is important to determine the optimal actions that, on the one hand - thanks to the use of modern technology in the work process - would minimize costs and effort, on the other - would reduce negative consequences, including the disappearance of certain professions, or replacing humans with machines while performing some of them. In accordance with Article 65 item 5 of the Constitution[4] and Article 10 of the Labour Code[5], the state has a policy aimed at full and productive employment, which means that the freedom to seek and take up employment has been complemented with the "necessity of some intervention of state in the labour market"[6].

In addition, taking any action at the legislative level, it is worth having in mind that the technological progress is not only about benefits and the threat of unemployment resulting from limited demand for labour, but above all it is about the serious consequences of work performed in conditions continually blurring boundaries between professional and private life. Work plays an important role in human life, as it is one of the conditions for self-realisation of the human being, as well as the basic source of income for most households. Therefore, it should not be considered solely in the category of duty – it is also the subject of the right to work, one of the most important rights in the human rights system. Therefore, there should be no doubt that human work cannot be replaced.

The issue of the impact of technological progress on human work is so significant and timeless that it has found its reflection not only on the pages of history (it is worth mentioning the Luddites' fights against industrialization, which peaked in the 19th century, when craftspeople destroyed thousands of machines, burned factories associated mainly with a long working day, lack of safe and hygienic working conditions and exploitation), but also in the social teaching of the Catholic Church. Particular attention was given to the problems of human work in the encyclical Laborem exercens, where it is indicated that technology understood as a set of tools that a person uses at work can be his ally. Undoubtedly, this is the case when technology facilitates work, accelerates it and multiplies the number of work products at an accelerated pace, while at the same time improving many of them in terms of quality[7].

The author rightly indicates, however, that the technology can transform from a human ally into his opponent, especially when it deprives him of the sense of job satisfaction and inspiration for creative action and responsibility, and also when it leads to job loss or "due to exaggerated fascination with the machine, it makes a man its slave"[8].

For this reason, it is worth considering the impact of access to mobile devices commonly used in the work process on human relationships. What is important is the answer to the question whether contemporary technology has not become an opponent of human being. Lack of balance negatively affects the well-being of a person, which manifests itself with, among others, reduced mood, decreased physical activity and the extent to which the employee is happy with his life. It also leads to health problems, such as, for example, back pain, headaches, as well as sleep disorders, exhaustion, and increases the likelihood of anxiety and depression[9].

From the perspective of the work-life balance conception, the answer to the question whether it is really possible to separate individual spheres of human life is therefore extremely important, despite the fact that technological progress is increasingly enabling us remote working. Hence, in the first place, a definition of the work-life balance will be presented, with a particular focus on a possible interpretation of the components of this notion in order to determine what should be understood as personal, family and professional life. Then, some specific problems concerning this issue will be discussed.

[4] Constitution of Poland of 2 April 1997 (the Journal of Laws of the Republic of Poland 1997, No. 78, item 483).
[5] Act of 26 June 1974 Labour Code (the Journal of Laws of the Republic of Poland 2018, item 108).
[6] Z. Góral, "On the topicality of treating the right to work as a principle of labour law in 'Unity in diversity. Studies from a range labour law, social security and social policy. A memorial book to honour Professor Wojciech Muszalski" (Warsaw: C.H. Beck 2009) p. 53.
[7] John Paul II, "Laborem Exercens" in "Encyclicals of the Holy Father John Paul II" (Cracow: Publisher Sign 2009) p. 154.
[8] *Ibid*.
[9] F. Burner, "Work-Life Balance: Challenges for workers in the context of work without limits and recommendations for action to improve the work-life balance" (Hamburg: Diplomica 2014), p. 8, http://han3.lib.uni.lodz.pl/han/ebsco/search-1ebscohost-1com-1002d1dwi325a.han3.lib.uni.lodz.pl/login.aspx?direct=true&db=nlebk&AN=794819&lang=pl&site=eds-live, accessed: 11 April 2018.

The notion of work-life balance

The notion of work-life balance is the subject of research in many scientific disciplines. For example, psychologists and sociologists try to determine how the work-life balance affects a person and his environment as well as the roles that he fulfils in his life[10]. On the basis of labour law, however, the key is to assess the possibility of regulating certain issues related to undertaking activities in the field of work-life balance at the level of legislation, especially that the specificity of particular employing establishments points out the need to determine how detailed the provisions on this issue should be.

Undoubtedly, the need to influence the sphere of professional and private lives of employees through labour law standards is an important task that the legislator must face in the near future, reaching at the same time solutions developed not only in the area of legal sciences. It is necessary to agree with Prof. W. Szubert, who pointed out the desirability of using funds belonging to different fields of science depending on the nature of threats occurring in a given work environment[11]. The fact that in a workplace the parties of the employment relationship may come into contact with various hazards stemming from improper organization of the work process, which lead among others to overloading with professional duties, as well as research on such phenomena as workaholism or burnout, conducted by psychologists, sociologists, physicians, can set the direction that the legislator should follow. In Poland, the obligation to organize work in a way that ensures full use of working time, as well as the achievements of employees, using their talents and qualifications, high efficiency and due quality of work, was expressed expressis verbis in Art. 94 item 2 of Labour Code. The doctrine indicates that the importance of actions taken in the implementation of this duty justifies considering it in terms of a primary obligation[12].

For this reason, it is worth taking a closer look at the notion of work-life balance, indicating at the same time possible forms of role conflict between individual spheres of human life. The right to be disconnected is in fact intended to provide employees with effective rest, thus limiting the risk of burnout, mental and physical exhaustion, or even death from overwork[13].

Pursuant to the content of Art. 207 section 2 of the Labour Code. science and technology are to protect human life and health. It is unacceptable, however, that technological or scientific progress leads to objectification of a human being, subordinating him to work and depriving him of the possibility of fulfilment in other areas of life.

Moving on to the next part of the considerations, it is worth pointing out that the concept of work-life balance is variously defined in the source literature. In general, it is indicated that it means a balance between professional and personal life of a person or a lack of conflict between the requirements that a person encounters in these spheres of his life[14]. Above all, doubts arise in the context of the interpretation of the components of this concept. In addition, there are different terms for it in the literature, for example work-family balance or life domain balance, which is not conducive to ordering this complex problem. That is why it needs to be mentioned that the work-life balance is a wider concept than the concept of work-family balance, because in non-working time a person fulfils not only obligations resulting from parenthood, but also undertakes various activities for self-improvement and regeneration of psychophysical condition. In this place, it is worth quoting the definition of the term work-life balance developed by the Federal Ministry for Family, Elderly, Women and Youth, according to which the concept should include effective coordination of professional and private life, which is achieved by including

[10] M. Binniger, "Work-life balance as an opportunity against demographic development: an investigation into the current skills deficit" (Hamburg: Diplomica 2014) p. 36, http://han3.lib.uni.lodz.pl/han/ebsco/search-1ebscohost-1com-1002d1dwi325a.han3.lib.uni.lodz.pl/login.aspx?direct=true&db=nlebk&AN=794952&lang=pl&site=eds-live, accessed 11 April 2018.

[11] W. Szubert, "Labour protection. Social and legal study" (Warsaw: National Publisher Scientific 1966) pp. 26-27.

[12] J. Wratny, "Comment to article 94" in: "Labour Code. Comment", ed. 6, Legalis/el 2016.

[13] A. Kanai, "'Karoshi (Work to Death)'' in Japan" [2009], http://eds-1b-1ebscohost-1com-1002d1dlp0523.han3.lib.uni.lodz.pl/eds/pdfviewer/pdfviewer?vid=3&sid=221bd269-e174-46bb-995b-2b7ce9a42124%40sessionmgr102, accessed 11 April 2018; J. McCurry, "Japanese woman 'dies from overwork' after logging 159 hours of overtime in a month", https://www.theguardian.com/world/2017/oct/05/japanese-woman-dies-overwork-159-hours-overtime, accessed 11 April 2018.

[14] F. Burner, *Ibid*., p. 4.

private, social, cultural and health aspects[15]. Thus, the time off from work, referred to as "life", belonging to the private sphere of a person, includes the individual's personal life, social contacts, and family life, under which a person also performs various activities related to running a household and rests. Family life should not be understood solely as an area in which an employee acts as a parent. A problem for many employees may also be the reconciliation of work and care for elderly or disabled family members.

The concept of "work" covers, on the other hand, activities carried out professionally, for profit-making purposes, in contrast to work performed in connection with the fulfilment of various roles in private life[16]. For this reason, when it comes to classifying the work of volunteers, the indicated interpretation allows to state that it also falls within the broadly understood concept of "life", because according to the definition of a volunteer accepted in the Polish law - it is a natural person who volunteers and shall perform benefits without remuneration under the terms specified in the Act. In addition, volunteering is a form of social activity undertaken in a time off from work, which connects people with common goals and a sense of mission - for many of them it is a form of self-fulfilment.

Of course, it is impossible to ignore the fact that for many people also professional career is an important aspect of self-fulfilment[17]. However, taking into account the need to protect an employee from possible threats resulting from scientific and technological progress, a criterion should be adopted that will allow delimitation of the sphere of professional and private life in order to undertake work-life balance activities. This is not about the complete separation of these areas of human life, because their penetration is inevitable and can also have a positive impact on the assessment of the quality of life, which is shaped by the material situation of the employee and intangible assets, among which health, family, social contacts and professional work play a crucial role[18].

Therefore, the concept of balance should not be equated with static equilibrium, because individual spheres of human life interpenetrate each other and there are various interactions between them, which makes it impossible to separate them completely[19]. The essence of activities that guide the work-life balance comes down to creating the conditions necessary for full human development, conducive to the transfer of positive emotions and values that people learn by undertaking an effort accompanying work for the common and own good, while eliminating those that lead to conflicts in private and professional life of a person.

For this reason, it is worth looking briefly at the forms of conflict between work and private life identified in literature, which may concern time, tension and behaviour and have a particularly severe impact on the sphere of family life of an employee[20].

For example, we deal with the conflict of time when the time that an individual devotes to the implementation of requirements in one of the areas leads to physical absence in the other, or absorbs him psychologically to such an extent that, despite physical presence, he is unable to meet the requirements of with functioning in the other area. This is the case when a parent is worried about their family's material existence after working hours, or after returning home, he receives business mail, telephones, which makes him stay mentally in the professional sphere.

The tension-related conflict, however, means that the employee transfers the feeling of anxiety, fatigue, and apathy from one of the spheres of life to another, which makes it difficult to perform different roles.

---

[15] S. Schnieder, "Work Life Balance in Companies: An Opportunity in Competition for Specialists" (Hamburg: Diplomica 2013) p. 37, http://han3.lib.uni.lodz.pl/han/ebsco/search-1ebscohost-1com-1002d1dwi329b.han3.lib.uni.lodz.pl/login.aspx?direct=true&db=nlebk&AN=794265&lang=pl&site=eds-live, accessed 11 April 2018.

[16] F. Burner, *Ibid.*, pp. 5-6.

[17] M. Binniger, *Ibid.*, p. 4.

[18] G. Wudarzewski, "Job satisfaction - conceptualization of the notion in the light of literature research", p. 326, http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.desklight-d4cad932-dde1-41f5-be2b-3665269d5811, accessed 23 April 2018.

[19] R. Gargi, "Impact of mobile communication technology on the work-life balance of working woman – a review of discourses", p. 82-85, http://han3.lib.uni.lodz.pl/han/ebsco/search-1ebscohost-1com-1002d1dwi32a4.han3.lib.uni.lodz.pl/login.aspx?direct=true&db=bth&AN=113644339&lang=pl&site=eds-live, accessed 12 April 2018.

[20] B. Lachowska, "Work and family: conflict or synergy? Facilitation and conflict between family and work roles - conditions and the importance of the quality of life for women and men" (Lublin: Publisher KUL 2012) pp. 42-43.

Yet, when the behaviours acquired in one of the areas are not consistent with the requirements of the role in another area, and the person moving between particular spheres of his life is not able to adapt them to the currently performed role, we deal with a behavioural conflict. This may be the case when a father or a mother who performs a managerial role in professional life treats their partners and children as subordinates.

It can therefore be concluded that the notion of work-life balance should be understood as the state of relative balance between work time, time devoted to the family and the time when an individual pursues his passions and interests or rests. It is about the ability of an employee to fulfil all his obligations and interests, both in the sphere of personal, family and professional life[21].

Contact with employees after working hours from the perspective work-life balance

Measures taken within the framework of work-life balance can have various character. They include, among others activities that affect employees and their work directly and are performed in the following areas: working time, workplace, scope of responsibilities and organization of work (the so-called primary measures). These include job sharing, flexible time and place of work, and teleworking[22].

In France, effective from 1st of January, 2017 provisions under which employees are granted the so-called right to be disconnected can be included in this type of measures. Having in mind the need to ensure conditions for effective rest, the legislator obliged employers hiring at least 50 employees to start negotiations with them in order to determine when they do not have to collect business e-mails or phone calls[23]. Importantly, before the right to remain offline came into effect, some companies have already addressed this issue. For example, according to the company agreement in force at Axa, e-mails received by employees in the evenings or weekends do not require a quick response. The Michelin tire manufacturer uses a computer system to record how long after working hours employees are connected to the company's server[24]. From the point of view of labour law, the reflection on the possibility of affecting the sphere of professional and personal life through primary means, including, for example, regulation of time work, can be particularly interesting. It is worth considering whether the Polish law is not a sufficient guarantee of protection for employees whose nature of work means that they are expected to be available also outside of working hours.

The situation of employees in Poland who receive business e-mails or telephones after working hours should be treated as overtime work or duty, if the employer obliges the employee to remain outside normal working hours in readiness to perform work resulting from a contract of employment at the workplace or in another place designated by the employer (Article 151^5 of the Labor Code).

In Poland, overtime work is allowed in the event of:

I. the necessity to conduct rescue operations in order to protect human life or health, protect property or the environment or remove failures;
II. special needs of the employer (Article 151 of the Labour Code).

In particular, the second justification for overtime work, defined as the "special needs of the employer" has been formulated so broadly that in practice this enables it to be treated very flexibly. There is no doubt, however, that overtime work cannot relate to a specific employee in a relatively constant manner, as well as constitute a permanent element of work organization by the employer[25].

The problem appears also in the absence of institutionalized forms of control of the legitimacy of ordering overtime work. In addition, the regulations do not indicate the mode that is in force for the employer issuing the order of such work. Such a command can take the form of any supervisor's behaviour

[21] F. Burner, *Ibid*., pp. 5-6.
[22] S. Rolle, "Work-Life Balance as a Future Task: Staffing and Work-Satisfaction in the Context of Family Friendliness" (Hamburg: Diplomica 2013) p. 35, http://han3.lib.uni.lodz.pl/han/ebsco/search-1ebscohost-1com-1002d1dwi32a4.han3.lib.uni.lodz.pl/login.aspx?direct=true&db=nlebk&AN=794533&lang=pl&site=eds-live, accessed 12 April 2018.
[23] K. Beck, "France's battle against an 'always on' work culture", http://www.bbc.com/capital/story/20170507-frances-battle-against-always-on-work-culture, accessed 11 April 2018.
[24] Offline: French employees now have the right to be unreachable, https://www.wallstreet-online.de/nachricht/9207395-arbeitsrecht-offline-franzoesische-angestellte-recht-unerreichbarkeit, accessed: 11 April 2018.
[25] K. Rączka, "Overtime work in the amended Labour Code" [2004] 1 PiZS p. 16.

that reveals his will in a sufficient manner[26]. According to the position presented in the case-law, the absence of the employer's objection to performing duties in his presence by the employee may be classified as an order to perform work overtime[27]. In order to recognize that we are dealing with overtime work, it is also irrelevant whether such work was performed with the consent or knowledge of the superior when the need to perform overtime work results from objective working conditions that prevent the employee from performing the tasks assigned to him or her within the statutory working time standards[28].

Determining the number of hours intended to be spent on business phone calls, or checking and servicing the service mail, may be problematic, although it is much easier in telephone calls due to the possibility of using billing. In order to determine how much time the employee devoted to getting acquainted with the business electronic correspondence, and then its analysis and preparation of the answer, the situation becomes more complicated[29]. It seems, however, that in the age of technological progress, there are solutions that allow such arrangements to be made. The employer has at his disposal programs for monitoring the time and course of work carried out with the use of a computer, including the use of keylogger programs, written specifically for the needs of a given person or institution. Programs of this type register all keystrokes and write them as a character string to a file, which is then sent over the network[30]. Thus, there are services available on the market that allow you to monitor the employee's activity on the Internet, by providing access to pages visited by the employee, records of time spent on a specific website, preview of website headlines, and even time devoted to the activities. Detailed analysis of the work is possible thanks to information about breaks at work, the scope in which the employee uses specific applications and viewing the history of sessions and logins[31]. It is also possible to control and archive all e-mails sent and received from a given server.

However, such forms of employee control may raise legitimate concerns due to the protection of personal data and the need to respect the employee's personal rights, including the right to privacy and the confidentiality of correspondence. Suffice it to mention the case of R. Bărbulescu against Romania[32], in which the European Court of Human Rights held that the concept of private life is a broad concept that cannot be exhaustively defined, and which may also include professional activities as well as activities taking place in a public context. Conclusions arising from the considerations regarding the relationship between the sphere of professional and private life are therefore confirmed in the case law.

Referring this issue to the issue of the right to be offline, it should be stated that also in this case it is difficult to reach a consensus, because it is not only about protecting the personal rights of the employee to privacy, but also about protecting the employee's health and life by creating conditions for effective rest during leisure time. Moreover, on the employer's side, the right to undertake monitoring is based on the expectation of the employee's duty of loyalty. Therefore, it is necessary to agree with the statement presented in the ruling of the European Court of Human Rights and the doctrine[33], according to which, while maintaining the principle of proportionality and procedural guarantees, monitoring the correspondence and an employee's activity on the Internet is admissible, and although it is an important aspect of this issue, the possibility of using technology should be analysed not only in terms of the benefits that its use brings in the sphere of protection of employer's interests. Considering the fact that there are no solutions similar to French ones in Poland, i.e. guaranteeing the employee the right to be offline, as

[26] K. Walczak, (ed.) 'Comment to art. 151' in 'The Labour Code. The Comment' (Legalis/el 2018), ed. 25.
[27] Judgment of Supreme Court of 14 May 1998, I PKN 122/98, Legalis No. 43286.
[28] Judgment of Supreme Court of 3 November 1978, I PRN 91/78, Legalis No 21101.
[29] State Labour Inspectorate about work and on-call duty during high days and holidays, https://www.pulshr.pl/prawo-pracy/panstwowa-inspekcja-pracy-o-pracy-i-dyzurach-w-swieta,40283.html, acessed 08 April 2018.
[30] Z. Góral (ed), "Employee control. Technical possibilities and legal dilemmas" (Warsaw: Wolters Kluwer 2010) pp. 350-352'; cf. M. Kuba, "Legal forms of employee control in the workplace" (Warsaw: Wolters Kluwer 2014) pp. 311-316.
[31] https://www.statlook.com/pl/monitorowanie-komputera-pracownika?gclid=CjwKCAjw-6bWBRBiEiwA_K1ZDWkt5FyyYBAITssEvmStKYaL5eGOnZNGiCubZCS7BWA2F6I39pYAzhoCW2gQAvD_BwE, accessed 08 April 2018.
[32] Bărbulescu v. Romania, Eur. Ct. H.R Application No. 61496/08, (2017) https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22Barbulescu%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22]} (accessed: 23 April 2018), cf. Copland v. United Kingdom, Eur. Ct. H.R. Application No. 62617/00, (2007), https://www.juridice.ro/wp-content/uploads/2016/07/1531450.pdf, accessed 23 April 2018.
[33] Z. Góral (*ed*), "Employee control. Technical possibilities and legal dilemmas" (Warsaw: Wolters Kluwer 2010) p. 211; cf. M. Kuba, "Legal forms of employee control in the workplace" (Warsaw: Wolters Kluwer 2014) pp. 323-326.

well as the difficulties which in practice relate to the time spent by an employee on business phones or analysis and preparation of responses to e-mail, it is worth considering the possibility of using the employer's right to e-inspect an employee from documenting thanks to the currently available technical achievements, also the time devoted to particular activities ordered as a part of overtime or on-call work. Any electronic equipment owned by an employer, used by an employee to work outside business hours, should be equipped with software which, in the event of a dispute over the number of hours worked overtime, will be used as evidence in the case.

In Poland, the regulation included in Art. 167 of the Labour Code, according to which an employer may dismiss an employee from leave when circumstances unforeseen at the time of starting the leave requires his presence in the workplace. The provision does not explain in what form an employer is to perform it. Therefore, it is assumed that an employer can submit a statement on the dismissal of an employee from leave in any form, which will allow the employee to become acquainted with its content (Article 61 section 1 of the Code of Association in conjunction with Article 300 of the Labour Code). However, the question arises whether an employer has the right to ask an employee to indicate his whereabouts or to provide a mobile number to be able to use this right. The answer to this question, as in the cases referred to earlier, requires the settlement as for which value is superior: the right of an employee to undisturbed rest, or protection of an employer's interest[34].

It seems that a compromise solution to this problem is the assumption that only in very exceptional situations an employee will be required to provide data that will enable an employer to contact him during the leave. In addition, this possibility should exist only in relation to specialists, not regular employees. It is a situation when the skills of a given employee make it impossible to be replaced[35].

Although so far in Poland there is no regulation guaranteeing the employees the right to be offline, or provisions regarding the forms and scope of control of the employment relationship for the parties, in the current legal status there are grounds for undertaking actions aimed at reducing contact with employees after working hours. It is worth mentioning here, for example, Article 207 section 2 of the Labour Code referred to earlier, which imposes on an employer an obligation to protect the health and lives of employees by providing safe and hygienic working conditions with appropriate use of the achievements of science and technology. The doctrine indicates that the reference in this provision has the nature of a technical directive, which obliges an employer to take measures to protect the health and lives of employees not only by implementing occupational health and safety regulations, but also taking into account various kinds of technical and organizational achievements that have not yet been expressed in legal norms[36]. In particular, an employer, under the obligation to protect the health and lives of employees, is obliged, among others to respond to the needs in the area of occupational health and safety, and adapt measures taken to improve the existing level of protection of health and lives of employees, taking into account the changing conditions for performing work (Article 207 section 2 item 3 of the Labour Code).

Therefore, considering the constantly evolving work environment, and thus risks, among which there is undoubtedly the loss of control over time, which man also devotes to working at home or during holidays, an employer using the opportunities provided by technological progress should strive for improvements that will make human work less onerous and dangerous, but more effective.

Conclusions

The solution introduced in France, the so-called right to be offline is an interesting form of preventing phenomena that accompany work overload, such as occupational burnout or workaholism. It could be that they would also work in Poland, although now there are grounds for organizing work in a way that allows employees to harmoniously combine roles and rest in their free time from work. The problem is rather in the wrong culture of work and in underestimating the impact of professional stress on

[34] K.W. Baran (*ed*), "Labour Code. The Comment" (Warsaw: Wolters Kluwer 2016) p. 1044.
[35] K.W. Baran (*ed*.), *Ibid*., p. 1045.
[36] K.W. Baran (*ed*), *Ibid*., p. 1200.

people, conditioned by factors both physical and psychosocial. In addition, employers often promote a destructive style of work among their employees, which leads not only to stress, but also workaholism, burnout, more frequent absences at work caused by the deteriorating health of a physically and emotionally exhausted employee.

Therefore, the legislator should first and foremost place the emphasis on educating employees and employers, which means that in obligatory training programs on occupational safety and health there should be issues related to stress, workaholism and burnout. Employees should be aware of the symptoms of these phenomena, know how to fight them and what factors of the work environment contribute the most to their development. Perhaps that is why it would be worth considering a cyclical organization of meetings with a psychologist who would help employees to properly manage their development in all areas of their lives. Bearing in mind the growing awareness of the conflict of roles in professional and private life, and thus, probably more people who will specialize in the future in the work-life balance, it may be worth for employers to offer their employees the opportunity to take advantage of services of this type of advisers. Of course, depending on the type of work performed by an employee and the nature of a given workplace, the needs in this area may be shaped in various ways. Therefore, the labour code regulations on this issue should on one hand reflect the wider scale of psychosocial risks in the workplace, which are a consequence of technological progress to a large extent, but on the other hand they should be general enough for employers to adapt them to the needs of their employees.

In addition, extremely important is the aforementioned issue of furnishing employers with electronic equipment, made available to an employee in order to perform work, and with technological solutions that enable the control of the time spent by an employee on work at home or during holidays. An employer, until the deadline for limitation of employee's claims due to overtime work, should store the collected documentation in this way for evidentiary purposes in the event of a potential litigation.

Interesting and worth noting is the practice introduced in some German companies, which means that between certain hours company servers do not provide e-mails[37]. An interesting solution was also introduced in the Daimler company, the so-called mail on holidays, which employees can optionally use. It consists in the fact that emails arriving at employees during their absence at work are automatically deleted, and an absence notification indicates to the sender the deputy who can deal with the matter. In turn, working time on a computer or telephone conferences taking place after working hours can be entered into the time recording system.

As a summary, it is worth noting that it should be the principle to organize the work process in such a manner that employees can rest after leaving the workplace. In the case when they work at home, it is important that the flexibility of time and place of work does not cause too much commitment to the duties performed, which might be a consequence of a greater freedom in planning the working day. Flexible working time can be a measure in the field of work-life balance, due to the possibility of adjusting start and end times to the individual needs of an employee[38]. However, in the case of an employee who is a victim of workaholism or is prone to this condition to a greater extent, due to his personality or quality of parental attitudes that shaped his childhood experience[39], can lead to more stress, overloading, difficulties in maintaining relationships with the family, instead of reconciling different social roles[40]. That is why it is so important to shape appropriate attitudes towards work. Employees as well as employers should be aware of not only the risks, but also the opportunities entailed by the development of technology and the digitization of work.

[37] M. Kaufmann, "German companies fight against the mobile phone delusion", http://www.spiegel.de/karriere/erreichbar-nach-dienstschluss-massnahmen-der-konzerne-a-954029.html, accesse: 23 April 2018; D. Hoffmann, "No emails during your free time", https://www.derwesten.de/leben/digital/keine-e-mails-waehrend-der-freizeit-id9166023.html, accessed 23 April 2018.

[38] M. Binniger, *Ibid*., p. 39.

[39] J. Wachowiak, "Dysfunctional attitudes of employees" (Warsaw: Difin 2011) p. 37-40; L. Golińska, „Workaholism – addiction or passion?" (Warsaw: Advisory and Information Center Difin 2008) p. 18-20; K. Wojdyło, "Workaholism. A cognitive perspective" (Warsaw: Difin 2010) p. 78-83, K. Wojdyło, „Addiction to work. Theory - diagnosis – psychotherapy" (Lublin: The Natanaelum Association. Institute of Psychoprophylaxis and Psychotherapy 2006) pp. 25-55.

[40] M. Binniger, *Ibid*., p. 39.

Bibliography

1. Act of 26 June 1974 Labour Code (the Journal of Laws of the Republic of Poland 2018, item 108).
2. Bărbulescu v. Romania, Eur. Ct. H.R Application No. 61496/08, (2017).
3. K. W. Baran (ed.), 'Labour Code. The Comment' (Warsaw: Wolters Kluwer 2016).
4. K. Beck, "France's battle against an 'always on' work culture", http://www.bbc.com/capital/story/20170507-frances-battle-against-always-on-work-culture, accessed 11 April 2018.
5. M. Binniger, "Work-life balance as an opportunity against demographic development: an investigation into the current skills deficit" (Hamburg: Diplomica 2014), http://han3.lib.uni.lodz.pl/han/ebsco/search-1ebscohost-1com-1002d1dwi325a.han3.lib.uni.lodz.pl/login.aspx?direct=true&db=nlebk&AN=794952&lang=pl&site=eds-live, accessed 11 April 2018.
6. F. Burner, "Work-Life Balance: Challenges for workers in the context of work without limits and recommendations for action to improve the work-life balance" (Hamburg: Diplomica 2014), http://han3.lib.uni.lodz.pl/han/ebsco/search-1ebscohost-1com-1002d1dwi325a.han3.lib.uni.lodz.pl/login.aspx?direct=true&db=nlebk&AN=794819&lang=pl&site=eds-live, accessed: 11 April .2018.
7. Constitution of Poland of 2 April 1997 (the Journal of Laws of the Republic of Poland 1997, No. 78, item 483).
8. R. Gargi, "Impact of mobile communication technology on the work-life balance of working woman Copland v. United Kingdom, Eur. Ct. H.R. Application No. 62617/00, (2007)
9. – a review of discourses", http://han3.lib.uni.lodz.pl/han/ebsco/search-1ebscohost-1com-1002d1dwi32a4.han3.lib.uni.lodz.pl/login.aspx?direct=true&db=bth&AN=113644339&lang=pl&site=eds-live, accessed 12 April 2018.
10. L. Golińska, 'Workaholism – addiction or passion?' (Warsaw: Advisory and Information Center Difin 2008).
11. Z. Góral (ed), "Employee control. Technical possibilities and legal dilemmas" (Warsaw: Wolters Kluwer 2010).
12. Z. Góral, "On the topicality of treating the right to work as a principle of labour law in 'Unity in diversity. Studies from a range labour law, social security and social policy. A memorial book to honour Professor Wojciech Muszalski' (Warsaw: C.H. Beck 2009).
13. Y. N. Harari, "The mystery of immortality" [2018] Newsweek Poland 14.
14. D. Hoffmann, 'No emails during your free time', https://www.derwesten.de/leben/digital/keine-e-mails-waehrend-der-freizeit-id9166023.html, accessed 23 April 2018.
15. Judgment of Supreme Court of 14 May 1998, I PKN 122/98, Legalis No. 43286.
16. Judgment of Supreme Court of 3 November 1978, I PRN 91/78, Legalis No 21101.
17. A. Kanai, 'Karoshi (Work to Death)'' in Japan' [2009], http://eds-1b-1ebscohost-1com-1002d1dlp0523.han3.lib.uni.lodz.pl/eds/pdfviewer/pdfviewer?vid=3&sid=221bd269-e174-46bb-995b-2b7ce9a42124%40sessionmgr102, accessed 11 April 2018.
18. M. Kaufmann, "German companies fight against the mobile phone delusion", http://www.spiegel.de/karriere/erreichbar-nach-dienstschluss-massnahmen-der-konzerne-a-954029.html, accessed 23 April 2018.
19. M. Kuba, "Legal forms of employee controli n the workplace" (Warsaw: Wolters Kluwer 2014) .
20. B. Lachowska., 'Work and family: conflict or synergy? Facilitation and conflict between family and work roles - conditions and the importance of the quality of life for women and men' (Lublin: Publisher KUL 2012).
21. J. McCurry, "Japanese woman 'dies from overwork' after logging 159 hours of overtime in a month", https://www.theguardian.com/world/2017/oct/05/japanese-woman-dies-overwork-159-hours-overtime, accessed 11 April 2018.
22. 'Offline: French employees now have the right to be unreachable', https://www.wallstreet-online.de/nachricht/9207395-arbeitsrecht-offline-franzoesische-angestellte-recht-unerreichbarkeit, accessed 11 April 2018.
23. J. Paul II, "Laborem Exercens" in "Encyclicals of the Holy Father John Paul II" (Cracow: Publisher Sign 2009).
24. K. Rączka, "Overtime work in the amended Labour Code" [2004] 1 PiZS 16.

25. S. Rolle, "Work-Life Balance as a Future Task: Staffing and Work-Satisfaction in the Context of Family Friendliness" (Hamburg: Diplomica 2013, http://han3.lib.uni.lodz.pl/han/ebsco/search-1ebscohost-1com-1002d1dwi32a4.han3.lib.uni.lodz.pl/login.aspx?direct=true&db=nlebk&AN=794533&lang=pl&site=eds-live, accessed 12 April 2018.
26. S. Schnieder, "Work Life Balance in Companies: An Opportunity in Competition for Specialists" (Hamburg: Diplomica 2013), http://han3.lib.uni.lodz.pl/han/ebsco/search-1ebscohost-1com-1002d1dwi329b.han3.lib.uni.lodz.pl/login.aspx?direct=true&db=nlebk&AN=794265&lang=pl&site=eds-live, accessed 11 April 2018.
27. State Labour Inspectorate about work and on-call duty during high days and holidays, https://www.pulshr.pl/prawo-pracy/panstwowa-inspekcja-pracy-o-pracy-i-dyzurach-w-swieta,40283.html, accessed 08 April 2018.
28. W. Szubert, "Labour protection. Social and legal study" (Warsaw: National Publisher Scientific 1966).
29. J. Wachowiak, 'Dysfunctional attitudes of employees' (Warsaw: Difin 2011).
30. K. Walczak (ed.), 'The Labour Code. The Comment', ed. 25, Legalis/el., 2018.
31. K. Wojdyło, 'Addiction to work. Theory - diagnosis – psychotherapy' (Lublin: The Natanaelum Association. Institute of Psychoprophylaxis and Psychotherapy 2006).
32. K. Wojdyło, 'Workaholism. A cognitive perspective' (Warsaw: Difin 2010).
33. J. Wratny, 'The Labour Code. The Comment', ed. 6., Legalis/el, 2016.
34. G. Wudarzewski, 'Job satisfaction - conceptualization of the notion in the light of literature research', http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.desklight-d4cad932-dde1-41f5-be2b-3665269d5811, accessed 23 April 2018.
35. https://www.statlook.com/pl/monitorowanie-komputera-pracownika?gclid=CjwKCAjw-6bWBRBiEiwA_K1ZDWkt5FyyYBAITssEvmStKYaL5eGOnZNGiCubZCS7BWA2F6I39pYAzhoCW2gQAvD_BwE, accessed 8 April 2018.

THE UTOPIA OF A PAN-EUROPEAN INSOLVENCY REGISTER

Podhalicz Mateusz[1]

Abstract

In less than 2 years, pursuant to the art. 25 (1) of the Regulation 2015/848 an online insolvency register for the entire EU will become reality. The focus of the presentation shall be the circumstances, under which it was decided that a pan-european insolvency register should be established. Further the feasibility of such register and potential difficulties in its creation, which can emerge on both European and national level shall be addressed. Answering the abovementioned and many other questions concerning the new interconnected system will allow to preliminary answer, whether the new pan-european has a chance of becoming a major accomplishment or rather an unrealizable utopia – feasible, as utopias frequently are - only on paper.

Keywords: Regulation 2015/848; pan-european insolvency register; insolvency law

Introduction

It borders on truism, to say that due to globalization of economy, more and more insolvency proceedings tend to have effect on more than one country, i.e. have cross-border character. The obviousness of the statement notwithstanding, the Regulation 346/2000[2] on insolvency proceedings i.e. the predecessor of the current Regulation 2015/848[3], did little to ensure that creditors from different States have equal chances of both: learning about and participating in insolvency proceedings. Rather, the Council adopted a more laissez-faire approach.

A criticism regarding this situation was expressed by stakeholders, practitioners and scholars in 2012 reports conducted by or at the request of European Commission on the effectiveness of the regulation. More than 75% of participants of public consultation advocated an introduction of mandatory publication system of all of proceedings which could fall under the scope of the cross-border insolvency regulation[4]. The solution was indeed introduced in the art. 25 (1) of the Regulation 2015/848, in a form of interconnection of national online registers, which by the date of interconnection (June 2019) will have to have been established by Member States. The interconnection shall enable all the interested parties to search in their own language for information about their debtors' insolvency procedures. The presents paper seeks to present the current state of law, the changes brought about by art. 25 (1) of the Regulation 2015/848 as well as to address the practicability and the effectiveness of the new solution. The first doubt concerning its applicability is regarding the scope of the interconnected system – that is whether every single case of insolvency proceedings will have to be published via the interconnection along with all of the accompanying costs. The second doubt is whether the register, while offering uniformity, will remain sensitive to different national solutions in the field of insolvency proceedings. Thirdly, there can be a doubt whether the language barrier and necessity of translation of the information and documents provided via the platform will not hinder equality of rights of the foreign and domestic debtors. Next it needs to be considered, whether the system should not include an option of lodging the claims or even become not a system of interconnection of national online registers, but rather a uniform pan-European system, replacing the national systems, or at least functioning independently. Finally, the paper will seek to suggest an efficient and viable solution, which could replace the one envisaged by the Regulation 2015/848.

---

[1] *The author is a law doctoral candidate at the University of Łódź, holds MA degree in law, as well as BA in economics. Professionally, the author is a trainee judge at the National School of Judiciary and Public Prosecution.*

[2] Council Regulation (EC) No 1346/2000 of 29 May 2000 on insolvency proceedings [2000] OJ L 160, p. 1, (Regulation 346/2000).

[3] Regulation (EU) 2015/848 of the European Parliament and of the Council of 20 May 2015 on insolvency proceedings [2015] OJ L 141, 5.6.2015, p. 19–72 (Regulation 2015/848).

[4] P. Sziranyi, 'EU-wide interconnection of insolvency registers', ERA 2015;

Registration duties under Regulation 346/2000

The original regulation regarding the registration duty of newly opened insolvency proceedings in other Member States, was stipulated in article 22 of the Regulation 346/2000**.** Pursuant to the abovementioned article, a judgment opening the proceedings might have been registered in another's State register, at the request of the liquidator. The regulation also granted States possibility of requiring that such a registration be mandatory, in which case the liquidator were to take any means necessary to ensure that such a registration would take place. Indeed, such a solution was adopted by many Member States, including Hungary, Latvia, Belgium, France, Germany and Lithuania. However, some States such as Italy, Poland, Romania, Greece and Finland did not opt for it, which clearly undermined the guarantee that all creditors in European Union would be promptly informed about the opening of the insolvency proceedings.

The scarcity of regulation was criticized by the scholars for that very reason, i.e. informational asymmetry among creditors in different States[5]. The shortcomings of the regulation became particularly manifest in the light of the ECJ judgement in the Eurofood Case[6], which highlighted the right of creditors (or their representatives) to participate in insolvency proceedings "in accordance with equality of arms principle"[7]. The ECJ stressed that all the creditors enjoy the rights enshrined in art. 47 of the Charter of Fundamental Rights of the European Union, as well as art. 6 of the European Convention of Human Rights. Thus, the creditors were to guarantee that they have an equal chance of participation in the proceedings.

After 12 years of the regulation remaining in force, European Commission conducted a public consultation and requested that a report be conducted regarding the efficiency of the regulation, *inter alia* regarding the question, whether the aforementioned equality was indeed guaranteed by the article 22 of of the Regulation 346/2000[8]. The report has since been published as the "Heidelberg Luxembourg-Vienna Report" in 2014. The national reports contained Heidelberg Luxembourg-Vienna Report in the national revealed that most of the respondents were convinced that there existed a need for a centralized register of insolvency proceedings[9]. According to the report's findings the lack of centralized information system put foreign creditors at risk of either not learning about the insolvency proceedings or learning about it too late. Another issue that was highlighted was the threat of multiple concurrent proceedings, conducted as main proceedings, because the judicial organs in one State could be oblivious as to fact, that insolvency proceedings were conducted in another State. Last but not least, in its report the Commission identified the potential impact of the lack of transparency and informational asymmetry on stakeholders of a debtor insolvent in a different State. These stakeholders were at risk of unwittingly entering into business dealings with an insolvent party, if that party failed to reveal its financial distress[10]. Also, report determined that the most efficient registers are, not surprisingly, the internet-based ones.

Based on the report and the public consultation, as well as European Parliament's recommendations in that respect[11], the European Commission presented a first draft of a "Proposal for a Regulation of European Parliament and of the Council amending Council Regulation (EC) 1346/2000 on insolvency proceedings" on December 12, 2012[12]. It was apparent from the outset, that the solution preferred by the European Commission was to establish interconnection of States' online insolvency

[5] G. Moss, I.F. Fletcher and S. Isaacs (eds.), 'The EC Regulation on Insolvency Proceedings: A Commentary and Annotated Guide' (Oxford: Oxford University Press 2009) p. 8.298.

[6] Eurofood IFSC Ltd., ECJ case C-341/04, 5/2/2006, ECR 2006 I-3813, para. 65 and seqq.

[7] H. Burkhard Hess; P. Oberhammer and T.Pfeiffer, 'European Insolvency Law' (Heidelberg: C.H. Beck 2013) p. 253.

[8] External Evaluation of Regulation no. 1346/2000/EC on Insolvency Proceedings - the reports of the studies are available in the Europa-website of DG Justice: http://ec.europa.eu/justice/civil/document/index_en.htm, retrieved [May 30th 2017], hereafter: (Impact Assessment).

[9] Annex II, Question 40 of the Impact Assessment.

[10] Impact Assessment, p. 25.

[11] European Parliament resolution of 15 November 2011 with recommendations to the Commission on insolvency proceedings in the context of EU company law (2011/2006(INI)), document no. P7_TA(2011)0484. The relevant recommendations can be found in Part 4 of the Annex to the resolution.

[12] Proposal of the Commission for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 1346/2000 on insolvency proceedings, Strasbourg 12 December 2012, COM(2012) 744 final.

registers, rather than an independent centralized register. According to the Commission that approach was adequate to satisfy the demand or the information and thus advisable even if it required certain financial output on the part of Member States[13]. On the 20th of May 2015, the final version of the Regulation was adopted, along with new provisions aiming at rectifying the above described shortcomings or in the words of the regulation itself: "*in order to improve the provision of information to relevant creditors and courts and to prevent the opening of parallel insolvency proceedings*"[14].

The current regulation

The new regulation, brought about substantial changes, as regards the dissemination of information regarding cross-border insolvency proceedings. The abovementioned article 22 of the Regulation 346/2000 was reiterated in the new regulation, although somewhat altered. As of now, whenever there are assets in a State, where the insolvency was not initiated, a debtor or insolvency practitioner is to request that the notice of opening of insolvency proceedings, along with information about the insolvency practitioner whenever required by the local law, be published[15]. Also, the new article 29 of the Regulation 346/2000 requires the insolvency practitioner to ensure that the proceedings are also disclosed in the relevant public insolvency register of the State, where the debtor has its seat or their immovable property, whenever such a requirement does exists in that State's legal system [16].

The above regulations, which are nothing more than a slight variation of the article 22 of the Regulation 346/2000 do not exhaust the measures adopted by the European Union in order to ensure the equality of arms among the creditors. Arguably the key aspect of the regulation is obligation imposed on the Member States to establish and maintain central insolvency register by the date of June 26th of 2018[17]. The information concerning insolvency proceedings is to be published as soon as possible after the opening of such proceeding, and shall include the following (so called mandatory information): the date of the opening of insolvency proceedings, the court opening insolvency proceedings and the case reference number, the type of insolvency, information regarding basis of jurisdiction, the legal characteristics of the debtor, the contact details of the insolvency practitioner, if any, appointed in the proceedings, the time limit for lodging claims, if any, or a reference to the criteria for calculating that time limit , the court before which and, where applicable, the time limit within which a challenge of the decision opening insolvency proceedings is to be lodged in accordance with Article 5, or a reference to the criteria for calculating that time limit the date of closing main insolvency proceedings[18].

The registers meeting the above described criteria will be subject to an interconnection via the e-justice portal, which will enable the creditor to search for a debtor in all of the national registers at once, using either basic or advanced search criteria[19]. What is important is that the information shall be available in every single official language of the EU (i.e. in 24 different languages). The information is to be available free of charge, with a possibility of charging the inquirers for access to additional information, i.e. not included within the scope of mandatory information[20].

The interconnection is to be established under the supervision of the European Commission within a year from the date of June 26th of 2018, and the Commission is to adopt by that date technical specification defining the methods of communication and information exchange by electronic means on the basis of the established interface specification for the system of interconnection of insolvency registers, the technical measures ensuring the minimum information technology security standards for communication and distribution of information within the system of interconnection of insolvency registers

[13] *Ibid*.
[14] Recital 76 of the Regulation 2015/848.
[15] Art. 28 (1) of the the Regulation 2015/848.
[16] Art. 28 (1) of the the Regulation 2015/848.
[17] Art. 24 (1) of the the Regulation 2015/848.
[18] *Ibid*.
[19] Art. 24 (1) of the the Regulation 2015/848; R. Dugué and M. Becker, 'The European Insolvency Regulation in theory and practice' in 'The new European insolvency register portal, Insolvency and Restructuring in Germany – Yearbook 2017' (Schultze & Braun Achern 2016).
[20] Art. 24 (1) of the the Regulation 2015/848.

and the means and the technical conditions of availability of services provided by the system of interconnection.

As of today, not much is known about the technical side of the project, nor whether the it will be completed as scheduled. Some indicator of how the system is going to operate can be the pilot project which was launched in 2014, and included interconnection of 7 national insolvency registers available online (i.e. Austria, Germany, the Netherlands, Czech Republic, Estonia, Romania and Slovenia – as of now it also includes the eighth participant – Italy). The system, operational until today, enables a real-time search in the national registers of the Member States involved. The search function allows conducting two types of searches: the 'simple' search running a parallel search according to the debtor's name (legal or natural person) in all participating registers; and 'advanced' search using different criteria – subject to various functionalities of the Member States' registers. The overall user's experience is ambivalent – the scope of information is uneven, depending on which State provided the information (where the most user-friendly and extensive one is provided by Latvia, and the least – by Italy). Also translations of the various judgements and orders seems to be an issue – e.g. in case of German entries, only basic information are available in EU languages, whereas the summaries of judgements are available only in German. Based solely on the pilot project, there can be raised a number of misgivings as regards the viability of the system, not to mention other considerations. The most important will be addressed in turn.

Critical assessment of the interconnection imitative

As above indicated, there are numerous concerns which can be raised regarding the new regulation. First of all, there can be a doubt which proceedings are subject to the interconnection. From the textual standpoint, one would have to assume that all of proceedings are covered by the Regulation, given that the wording of Articles 24 and 25 of the Regulation 2015/848 does not contain any limitations, which would that only cross-border proceedings are to be available via the interconnected systems. On the other hand, one could make a case[21], that the Recital 76 of the Regulation 2015/848 does indeed suggest that only cross-border cases should be published, as required by article 24. The recital reads: "Member States should be required to publish relevant information in cross-border insolvency cases in a publicly accessible electronic register." Thus, from that viewpoint it would seem that only insolvency proceedings with a foreign element necessitate that information about them be published in public registers – and, rather importantly – that only these require translation. Such an interpretation would have to be deemed as more cost-efficient, as the insolvency proceedings having impact only on local scale, would not have to be processed in 24 different languages, thus saving both time and work of court staff. On the other hand, given the globalization of trade and services, it would be increasingly difficult to exclude an option, that a debtor has some international trade relations, and thus their insolvency case may eventually be revealed as being a cross-border one. Also conceivable would be a purchase of a debt by a foreign creditor, which would automatically mean that an insolvency case has a foreign element. Taking all of the above into consideration, one would have to say that both alternatives are not optimal. One approach, which requires translation of all of the judgement is from economic point of view utterly inefficient and the other puts at risk the very goal of the new Regulation, which is ensuring the equality of rights of creditors. In summary, it seems that a different approach than that proposed be the Commission could be more suitable.

Another issue, which should be taken into consideration is striking a proper balance between, uniformity of the system on the one hand, on the other remaining sensitive to idiosyncrasies of each State's insolvency law. Given that on the European Union level, there has been little harmonization of the material insolvency law, the insolvency regulations adopted in each State differ substantially from one another. It seems that this aspect has not been sufficiently pondered upon by the Commission, since the so-called mandatory information contains only one aspect which is bound to be different – State-to-State, and that is the time limit for lodging claims. There are however different aspects to be taken into consideration, such as question of the managing the debtors affairs (whether it is done solely by the

[21] R. Dugué and M. Becker, *Ibid*., p. 31.

insolvency practitioner, or to some extent also by the debtor) or the influence of the insolvency proceedings on individual debt execution. These aspects are not included within mandatory information, which means that it will be again a free choice of State's legislature to include them. Lack of such information may put creditors from foreign States at clear disadvantage towards the domestic creditors, since the latter will be in the position of better assessing their legal situation. In the literature it has been noted that the sensitivity to idiosyncrasies of each State's insolvency law was already an issue in case of the pilot project (encompassing jurisdictions) which means that it will be even more of a challenge in case of 27 jurisdictions[22].

The third issue which should be underlined is the language barrier. It is difficult to conceive how exactly the translation of all of the relevant data is supposed to be ensured. As noted above, even in case of the pilot project, only in some jurisdictions the judgements and orders were translated from the original language – and not into all other EU languages but only into English. The e-justice portal acknowledges this fact, stating that certain that some case-specific information, such as excerpts from judgments, are not to be translated[23], which seems rather astonishing since in practice, very often, legal results are determined by tiniest details. Possible negative consequences might ensue, which will be demonstrated using an example based on Polish insolvency procedure. During Polish insolvency, the insolvency practitioner drafts - and the courts accept - a rather important document from the i.e. the list of creditors. The list contains all of the known creditors with their category, which determine their priority of satisfaction. Since such a list does not have to be translated and published via the interconnection, because it is not mandatory, and also non-mandatory are the information about the priority of satisfaction, a potential foreign creditor may be oblivious to the fact, that their claim has no practical chance of being satisfied given the limited resourced owned by the debtor and the participation of debtors with higher priority of satisfaction. That in turn will mean that such a creditor may take steps towards lodging claim and perhaps even contracting a lawyer, without realizing that their actions are bound to fail. Such an eventuality does speak neither for equality of arms nor for the strengthening of internal market. Depriving the foreign creditors of full access to the same amount of information that is accessible for the domestic creditors along with abovementioned insensitivity of the interconnected system to their meaning, will not guarantee the required equality of arms.

On the other hand, if all of judgements, orders and interim measures were to be translated by all of the European insolvency courts, it would necessitate a tremendous financial and organizational output on the part of each State (given the rule that the costs of interconnection is imposed on each State). To fully appreciate the scale of the issue, a case of European Court of Justice of European Union could be mentioned, as an example of how much resources is dedicated to translating all of its documents into 24 EU languages. The translators account for 50% of the staff of ECJ and are as numerous as 1000 translators, at the same time being one of Europe's leading experts in legal linguistics, very often having expertise of more than 4 languages and obligatory legal background. It would be difficult to expect that all of the insolvency courts - essentially low-tier courts (e.g. in Poland alone there are 30 such courts) will be up to the challenge both financially and from organizational standpoint, when one considers that even one of the most affluent, well-staffed judicial body, such as European Court of Justice needs 1000 expert translators to have all of the required documents translated. Even if it were viable, it would mean that from transactional costs[24] of the insolvency proceedings would rise, thus either reducing the cost-efficiency of the proceedings for the creditors (since the translation costs will be counted as proceedings costs and thus satisfied in the first place from the debtors assets) or the attractiveness of such proceedings will in turn will create the need for alternative methods of dealing with insolvency and may have negative impact on the internal market as a whole.

[22] P. Sziranyi, *Ibid*., p. 10.

[23] R. Dugué and M. Becker, *Ibid*., p. 31.

[24] Assessing the situation according to the Coase Theorem, N. S. Cheung, 'Transaction Costs, Risk Aversion, and the Choice of Contractual Arrangements" [1969] Journal of Law & Economics 12 (1) pp. 23–42. DOI:10.1086/466658. Retrieved, accessed 14 April 2018; R. H. Coase, 'The Nature of the Firm' Economica. 4 (16): 386. DOI:10.1111/j.1468-0335.1937.tb00002.x.

Finally, it is somewhat disenchanting that the system will not offer such a functionality as lodging claims in the insolvency proceedings and also a way of actively participating in the proceedings. While the European Commission boasts that the system will contain "a tool to find a lawyer or notary who speaks your [creditor's – author's addition" language throughout the Union, and tools to allow direct electronic communication between citizens and courts in other Member States."[25] , the achievement is not that impressive, when one considers that in many cases such a lawyer will not be found (it is doubtful whether there are plenty of Spanish lawyers with fluent expertise of the Latvian language) and that the electronic communication will not allow the foreign creditors to communicate most important acts – such as lodging of claims. Such limitation means that the inequality of arms in the proceedings will be preserved, because the distance of foreign creditors from the insolvency court will put them at a clear disadvantage, as long as the Internet will not be the primary means of communication between the parties involved. This aspect indicates inherent weakness of the new Regulation 2015/848, its superiority over the previous one notwithstanding.

Final remarks and conclusions *de lege ferenda*

As results from the critical assessment of the Regulation 2015/848 in respect to disseminating of information and guaranteeing equality of arms among the creditors, it has to be stated that there may be a reasonable doubt, whether the new provisions are the optimal ones. As a matter of course, not much is known about the final form which the interconnected system will have, but from the information available it seems that it will be only a preliminary, but surely not final step towards true interconnection of insolvency proceedings in Europe. The current regulation do not determine which cases are covered by its scope, does not seem to take into account the overall cost-efficiency of the system, does not account for differences in insolvency law, does little to tackle the issue of multilingualism of the proceedings and does not guarantee that foreign creditors have the same communication capabilities with the court as the domestic creditors.

A case may be made, that the source of the issue lies in the underlying assumption made by the European Commission in 2012, when the interconnection, was chosen in favour of a centralized insolvency register. It seems that such a register, albeit requiring far greater financial input at the outset, would in the end become more efficient and effective. One could envisage such a system as consisting of separate national subsystems, which the judicial organ would employ to perform all of the necessary activities such as registration of insolvency proceedings and issuing orders, judgements and interim measures. One way to enable that would be to create the system as an algorithm-based set of available options, from which the judge would have to choose step-by-step, based on the pre-set forms. For instance – in case of registration of insolvency proceedings the judge would have to first choose whether the proceedings are aimed at liquidation or at restructuring, then whether the management of debtor's affairs has been granted to the practitioner, and other necessary questions. Aside from the variables (such as names, quantities, addresses and so on which do not necessitate translation), which the judge would have to introduce in the preset form, permanent aspects of the proceedings would be automatically provided – such as the name, localization of the court and and state's law specifities relevant to particular proceedings. The same situation could apply to issuing orders and judgements – which could be arranged in a way of interactive forms created beforehand for different kinds of procedural eventualities, which the judge could generate only introducing certain case-specific variables (such as names, quantities, addresses and so on which do not necessitate translation). Such an arrangement would easily do away with the translation problem, since all of the preset option for each jurisdiction would have to be translated within the system only once. Once translated, in case of each insolvency proceedings, the preset form would simply be completed with the non-translatable variables introduced and chosen by the insolvency judge in the country of origin. Also preset translation of the legal events taking place in different countries would have to be accompanied by the preset legal clarifications which would ensure the equality of arms

[25] European Commission Press Relase: Modern Insolvency Rules: European Commission kicks off EU-wide interconnection of insolvency registers http://europa.eu/rapid/press-release_IP-14-774_en.htm, accessed 20 May 2018.

of the creditors. Such a system would present a substantial challenge to the Member States and the European Union but, it seems that such a solution could be viable and possible, should the collective effort be undertaken. Instead European Union chose a method which is cheap, but ultimately inefficient and severely lacking. The situation can be compared with constructing a building without preparing the terrain for it, using all of the cheapest material and working crew which consists of workers who do not know one another's language and cannot communicate. What will result is an unstable, inconsistent construction which will not fulfill its goals and is very likely to require a soon replacement. One can be afraid, that such is the fate of the interconnected insolvency register, as envisaged by the Regulation 2015/848.

Bibliography

1. H. Burkhard Hess, P. Oberhammer and T. Pfeiffer, 'European Insolvency Law' (Heidelberg: C.H. Beck 2013).
2. N. S. Cheung, 'Transaction Costs, Risk Aversion, and the Choice of Contractual Arrangements" [1969] Journal of Law & Economics 12 (1),. DOI:10.1086/466658, accessed 14 April 2018.
3. R. H. Coase, 'The Nature of the Firm' Economica. 4 (16), doi:10.1111/j.1468-0335.1937.tb00002.x.
4. Council Regulation (EC) No 1346/2000 of 29 May 2000 on insolvency proceedings [2000] OJ L 160, p. 1, (Regulation 346/2000).
5. R. Dugué and M. Becker, 'The European Insolvency Regulation in theory and practice' in 'The new European insolvency register portal, Insolvency and Restructuring in Germany – Yearbook 2017' (Schultze & Braun Achern 2016).
6. Eurofood IFSC Ltd., ECJ case C-341/04, 5/2/2006, ECR 2006 I-3813, para. 65 and seqq.
7. European Commission Press Relase: Modern Insolvency Rules: European Commission kicks off EU-wide interconnection of insolvency registers http://europa.eu/rapid/press-release_IP-14-774_en.htm retrieved [20th May 2018].
8. European Parliament resolution of 15 November 2011 with recommendations to the Commission on insolvency proceedings in the context of EU company law (2011/2006(INI)), document no. P7_TA(2011)0484. The relevant recommendations can be found in Part 4 of the Annex to the resolution.
9. External Evaluation of Regulation no. 1346/2000/EC on Insolvency Proceedings - the reports of the studies are available in the Europa-website of DG Justice http://ec.europa.eu/justice/civil/document/index_en.htm, retrieved [May 30th 2017].
10. G. Moss, I.F. Fletcher and S. Isaacs (eds.), 'The EC Regulation on Insolvency Proceedings: A Commentary and Annotated Guide' (Oxford: Oxford University Press 2009).
11. Proposal of the Commission for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 1346/2000 on insolvency proceedings, Strasbourg 12 December 2012,COM(2012) 744 final.
12. Regulation (EU) 2015/848 of the European Parliament and of the Council of 20 May 2015 on insolvency proceedings [2015] OJ L 141, 5.6.2015, p. 19–72 (Regulation 2015/848).
13. P. Sziranyi, 'EU-wide interconnection of insolvency registers' [2015] ERA.

BLOCKCHAIN VERSUS GDPR

Poulenard Hanna[1]

Abstract

The general regulation of the protection of personal data offers people rights of various kinds: right to information, access to data, right to limitation of treatment, right of rectification or right to be forgotten. It's the controller to ensure that these rights are effective for its own users. We will discuss here the confrontation of some of these rights which are particularly problematic with regard to the Blockchain technology.

Keywords: Blockchain, GDPR, GAFA, Data, Regulation

Introduction

The GDPR (General Data Protection Regulation) is a new fundamental text of the European Union aimed at strengthening national data protection systems and harmonizing rules on the European territory. It will enter into force on 25 May and will be directly applicable to the Member States. As of May 25, 2018, the GDPR will therefore frame the right to the protection of personal data. After a first reading it is clear that this regulation did not take into account the development of a new technology, Blockchain technology, but aims to regulate the processing of data that already exists, including data owned by giants of the web that are Google, Amazon, Facebook or Apple. Nevertheless, to the extent that will be found on a Blockchain information that the GDPR considers as personal data, this text is fully applicable to the various activities that will rely on this technology. The processing of data on a Blockchain is radically different from their "classical" processing, so it is necessary to reconcile the text and the development of Blockchain technology which is not easy. The first difficulties arise when the scope of the GDPR has to be identified and the rights granted by the Regulation to individuals are to be studied. Is compliancy with the GDPR standards technically feasible concerning Blockchain?

The Blockchain "Is an "open source" digital data management protocol, decentralized, tamper-proof and based on P2P exchanges in the networks"[2]. The Blockchain is a digital technology that stores and digitizes information and operates without a control organ or instance. It also forms a distributed database[3] that keeps lists of all transactions between users made since it was started. Each transaction list is contained in a block that is linked to the next block, forming a chain. The last block of a chain is added to the previous blocks which have been authenticated and validated by minors[4].

A public Blockchain is consulted by all and there is no restriction to participate in the network. Anyone can interact with the registry. The modification of the protocol[5] requires an agreement (consensus) and the coordination of minors. We talk about immutability in the public Blockchain because to change a block it would be necessary to agree, the consensus of more than half of the hash[6] power (51%). And even if it is modifiable by consensus, in practice it is impossible to go back to make a change without

[1] *PhD student in Financial Law, Paris Nanterre university, Centre de droit civil des affaires et du contentieux économique (CEDCACE, EA 3457) - Université Paris-Nanterre. Thesis's topic: "Le régime juridique des Fintech" [The legal regime of Fintechs] under the direction of the professor David Robine. Research Interests: Finance, new technology, high frequency trading, cryptocurrency, blockchain. E-mail: hanna.poulenard@parisnanterre.fr*

[2] J. de Rosnay, 'La Blockchain : un défi aux pouvoirs centralisés' [2016] La blockchain décrypté 8

[3] 'In computing, a distributed database is a database whose management is processed by a network of interconnected computers that store data in a distributed manner. This storage can be either partitioned between different nodes of the network, or replicated entirely on each of them, or be organized in a hybrid way.' A. Gomez, 'Les bases de données distribuées' [2013] Substance.

[4] 'Node of the network whose peculiarity is to use its computing power to add a block to the Blockchain, by calculating a precise hash function' F. Godebarge and R. Rossat 'Principes clés d'une application Blockchain' [2016] Mémoire EM Lyon Business school.

[5] A protocol is a set of rules that govern the exchange of data or the collective behavior of processes or computers in networks or connected objects. A protocol aims to perform one or more tasks contributing to the smooth functioning of a general entity.

[6] The hash in the Blockchain is created from the data in the previous block. The hash is a fingerprint of this data that locks blocks in order and time' T. Laurence 'La Blockchain pour les nuls' (Paris: 2018) p. 400.

modifying the following blocks. Because all the blocks exist according to the information of the previous block, if I want to modify a block I would have to modify thereafter all the following blocks. So, it would take on the IT side many years.

The private Blockchain runs on a private network, it is publicly available, but permission is needed to interact. The managers of this Blockchain can therefore modify the protocol if they wish. In a private Blockchain with only 10 actors, the consensus will be easy to reach. If important data is wrong in the chain, they may decide to "back off" to remove the problematic data.

Furthermore, depending on the protocol used by blockchains, which may be public or private, the nature of the data collected and processed will vary, these blockchains may or not contain personal data, and it is possible or not to change, delete data.

Blockchain and GDPR sometimes seem antithetical. As an example, the Regulation states that the controller is anyone who determines the purposes and means of treatment. Since the Blockchain is a decentralized register, the identification of the controller is impossible. GDPR raises problems being given the technical specificities of the Blockchain: the erasure of the data is not possible in public blockchain, once the block created it is impossible to erase it, the register is immutable. But GDPR created a right to datum rectification. How is it going to be done technically? Should a new regulation be established? Regulating new technologies is a hard task since they constantly evolve, therefore that process has two separate steps. Upstream, when drafting new text, these evolutions need to be taken into account, and downstream, interpretation of the texts need to be adapted because of these evolutions. It is possible to find solutions to adapt GDPR to Blockchain technology, and that is what the article will demonstrate. At first in we will study the inclusion of blockchain in the GDPR fields, and to finish modality of application the GDPR to the Blockchain.

1. The inclusion of Blockchain in the GDPR field

The GDPR is fully applicable to those responsible for the processing of personal data. This calls for two questions: what is a personal data and who is responsible for processing in a Blockchain.

1.1. Personal data

Article 4 paragraph 1 of the GDPR defines personal data as: "any information relating to an identified or identifiable natural person; is deemed to be an "identifiable natural person" a natural person who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or to one or more specific elements specific to its physical, physiological, genetic, psychic, economic, cultural or social identity "[7].

It appears from the text and from its mind that the notion of personal data must be understood in its broadest sense. A very extensive interpretation will therefore be made by the various actors who will have to hear these questions.

If the regulation excludes anonymous information from its scope, this is not the case for information that can be traced back to an identified or identifiable natural person. In order to determine whether information is personal data, the Regulation states that "all means reasonably likely to be used by the controller or by any other person to identify the individual directly or indirectly" should be considered. indirectly". An IP address could thus be considered as a personal data insofar as it can indirectly identify a natural person[8]. The question could arise for the data within the public Blockchain, including such bitcoin that uses cryptography, which is an encryption technique, whose purpose is to ensure the confidentiality

[7] Regulation (EU) 2016/679 of the European Parliament and of the council on the protection of natural persons with regard to the processing of personal data [2016] OJ L 119.

[8] For the CJEU, this is indeed the case. The court thus states in its judgment that "a dynamic Internet protocol address registered by a provider of the occasion of the consultation by a person of a website that this provider makes available to the public constitutes personal data. "The court nevertheless brings a significant nuance: the IP address alone is not personal data, but that it becomes so when the provider has "legal means to identify the person concerned. The IP address thus becomes a personal datum since it allows, in conjunction with other means, nominally identify the user. Patrick Beyer v Bundsrepublik Deuschland, Case C-582/14 [2016].

of a given data. This is not data anonymization but data encryption. Encryption is to make the comprehension of a document impossible for anyone who does not have the decryption key. A person holding the key can thus have access to the data.

At first reading, all information is a personal datum since it allows to go back to an individual by various means. In theory, in a Blockchain, the information that can be considered as personal data will depend on the decryption key. In practice, restricting only personal data depending on whether or not we can hold a decryption key amounts to restricting the protection that information contained in a Blockchain might have.

1.2. The controller in the Blockchain

The legal obligations imposed by the GDPR affect both the controller and the subcontractors. It follows from Article 4 (7) of the Regulation that the controller is "any natural or legal person who alone or together with others, determines the purposes of treatment and means of treatment." The same article specifies that the subcontractor is the one who processes the data on behalf of the controller.

Because Blockchain is a decentralized registry, it can be difficult to identify the controller. The Blockchain may contain information that may be considered personal data and it is unlikely that an authority that would have to review such data believes that there is no data controller. One of the likely solutions would be for the judge or authority to consider that the designer of the Blockchain technology application or smart-contracts[9] is designated as the controller.

Once information of a personal nature has been identified and data controllers have been designated, there are many obligations under the General Data Protection Regulation. Indeed, if with the Blockchain the thorny question of the consent arises less since the user will perform a positive act before his data integrate the chain. On the other hand, issues related to the right to be forgotten or the right to rectification are much more problematic here than in other sectors.

2. Modality of application the GDPR to the blockchain

The right to forget, rectify and portability of data are the most expected rights because they finally offer people using new technologies the control of their data. However, these rights will be difficult to apply within a Blockchain, including a public Blockchain.

2.1. The right of rectification (Article 16)

Article 16 of the GDPR provides: "The data subject has the right to obtain from the data controller, as soon as possible, the rectification of inaccurate personal data concerning him / her. In view of the purposes of the processing, the data subject has the right to have the incomplete personal data completed, including by providing a supplementary declaration."

The problem posed by the right of rectification is with regard to the immutability of the Blockchain. It is not possible to change information that has already integrated the block. One can nevertheless imagine a solution that would be to take advantage of the possibility offered by this article 16 which aims at a "complementary declaration". It might be considered to rewrite the information that needs to be rectified in a new block. On this point, the nature of the information in question will probably have to be examined to determine how the controller will proceed. The opinions and communications of the G29[10] or the commission in the coming months will prove to be very useful.

[9] Computer protocols that facilitate, verify and execute the negotiation or execution of a contract, so render a contractual clause unnecessary.
[10] Is an independent European advisory body on data protection and privacy. Its organization and tasks are defined by Articles 29 and 30 of Directive 95/46 / EC, from which it derives its name, and Article 14 of Directive 97/66 / EC. As of the entry into force of the General Data Protection Regulation in May 2018, it will be replaced by the European Data Protection Board.

2.2. The right to be forgotten (Article 17)

The right to be forgotten devotes two rights to it: The first is the right to dereference, this right allows to ask a search engine to delete some search results associated with your first and last names. This notion does not interest us to the extent that the content of a Blockchain is not intended to be referenced on a search engine. The second right is the withdrawal of information. The first of Article 17 of the GDPR states that: "the data subject has the right to obtain from the controller the erasure, as soon as possible, of personal data concerning him and the person responsible for processing the data. Obligation to erase this personal data as soon as possible. This article of the regulation poses a problem given the technical characteristics of the Blockchain: erasing data does not seem possible, especially in the public Blockchain because as it is mentioned in the introduction it is immutable. However, one solution that can be considered is to encrypt this data so that other users of the Blockchain cannot access it. When the contracting party requests that his information be erased, it is then sufficient to revoke the encryption key which allows their reading. Blockchain data erasure is not effective but cannot be read by anyone. Clearly, the data are still present but they are unreadable.

This calls for several remarks: The first being that this solution does not seem to correspond to the precise requirements posed by the text, which is the deletion. Nevertheless, it does not seem that the spirit of the text is to prevent the existence and development of Blockchain. We can therefore think that such a solution, which is encryption can be declared compliant by the supervisory authorities. Nevertheless, it will be necessary to make sure of several things. For example, the data manager should adopt a particular process and stick to it as soon as the encryption key is transmitted to a third party. It will also have to guarantee the proof of the revocation of the encryption key by all those who had access to it. To be certain of the validity of such a process it will be necessary to ensure the development of a code of conduct to show the willingness of the designers of the Blockchain to respect and enforce the rules. This code of conduct may be presented to the G29 for an opinion and we will closely follow all the recommendations that the latter will publish in the coming months and years to find out how a Blockchain could respect this right and avoid any sanction.

For this solution to work, it will also be necessary to do a very precise and precise job of identifying the information that can be considered as personal data. Because if information that was thought outside the scope of the regulation was to be integrated in a block without being encrypted, the consequence will be such that the effectiveness of the right to forget about this data will be impossible. However, the identification of personal data is not easy and this for two reasons. First of all because the definition given by the regulation is so extensive that one can have doubts about certain information. This was the case of the IP address which was finally recognized as personal data by two judgments of 2016 to the extent that it can indirectly identify the person concerned. We must also project ourselves, and take into account that tomorrow a new technology can be born and will be able to find a person even if his data have been encrypted.

2.3. Data portability (Article 20)

The right to portability offers people the opportunity to obtain and reuse their personal data to meet their own needs, through different services. This right allows a person to retrieve the data about them processed by an organization, for personal use, and store them on a device or a private cloud. This right allows you to manage your personal data more easily and by yourself. Transfer your personal data from one organization to another. The personal data can thus be transmitted to a new organization, by the person himself, by the organization that holds the data. The right to portability strengthens people's control over their personal data. It also creates new opportunities for development and innovation by facilitating the sharing of personal data, in a secure manner and under the control of the person concerned.

This new right applies if all three conditions are met. It is limited to the personal data provided by the person concerned. It applies only if the data are processed in an automated manner as in the present case for blockchain technology and on the basis of the prior consent of the data subject or the performance

of a contract concluded with the concerned person for example a smart contract. The exercise of the right to portability must not affect the rights and freedoms of third parties, whose data would be found in the data transmitted following a request for portability. Whence this interrogation, a request for portability of data located in a block are likely to undermine the rights of members of the community? That is, an inherent right to blockchain technology for viewing transaction history. In the case of an obvious infringement, the portability request will not succeed. Alternatively, the entity (designated as a controller) that manages a blockchain transmits the relevant data to the specified recipient and keeps a copy of the user's data in order to maintain the Blockchain's fundamental transaction history. Indeed, the portability is limited to a transfer of data, the recovery thereof and their transfer to a third-party recipient, but does not include the deletion of data concerned.

Conclusions

Article 40 of the GDPR encourages processors and subcontractors to develop codes of conduct to assist in the proper implementation of the regulation. These codes of conduct will thus facilitate the control (by the CNIL[11] for example) of compliance with the requirements of the Regulation and may undoubtedly prove the good faith of the company.

These codes of conduct may be presented to the supervisory authorities for advice and the commission may publish these codes and make them of general application. The development of a code of this type will undoubtedly be necessary in order to write in black and white all the identified processes to develop a Blockchain respectful of European texts and to serve as proof during a possible control.

Bibliography

Books

1. B. Chouli, F. Goujon and Y. M. Leporcher, 'Les Blockchains, De la théorie à la pratique, de l'idée à l'implémentation' (France: 2017).

Articles

1. D. Birch, 'Mutable and immutable blockchains' [2016] Tommorow's transaction.
2. S. Bourguigon, 'Part V: Blockchain privée ou publique, quelle différence?' [2018] les Echos.
3. F. Cavazza, 'Définition, usages et enjeux des blockchains' [2016].
4. P. De Filippi, 'What blockchain Means for the Sharing Economy' [2017] Harvard Business Review.
5. F. Godebarge and R. Rossat 'Principes clés d'une application Blockchain' [2016] Mémoire EM Lyon Business school.
6. A. Gomez, 'Les bases de données distribuées' [2013] Substance
7. G. Greenspan, 'The Blockchain Immutability Myth' [2017] MultiChain.
8. C. Jentzsch, 'Public vs Private chain' [2017] Motivation.
9. 'La Blockchain, une technologie avec un potentiel immense' [2015] Journal quotidien finance
10. T. Laurence 'La Blockchain pour les nuls' (Paris: 2018).
11. T. Moore and R. Anderson, 'Internet security, The Oxford Handbook of the Digital Economy' (Oxford: Oxford University Press 2012).
12. G. Pavet, 'Blockchain Publique Ou Blockchain Privée: Comment Envisager L'Avenir Des Cryptomonnaies?' [2018] Forbes.
13. P. Prados, 'Blockchain: modifier un contrat immuable' [2017] GNU/Linux Magazine.
14. J. de Rosnay, 'La Blockchain: un défi aux pouvoirs centralisés' 2016 La blockchain décrypté 8.
15. X. Simonin, 'Pour comprendre la technologie blockchain' [2016] Revue Banque.
16. D.Teruzzi, 'La programmation de smart contracts: une opération hautement délicate' [2016] BlockchainCafe.
17. D. Teruzzi, 'Les consensus: Proof of Work vs Proof of Stake' [2016] finyyear.com.

[11] The National Commission for Informatics and Liberties (CNIL) of France

18. D. Teruzzi, ‘Les protocoles de consensus distribués’ [2016] BlockchainCafe.
19. M. Walport, ‘Distributed Ledger Technology: Beyond Blockchain’ [2016] UK Government Ofice for Science.
20. O. Wyman, Anthemis group, ’The Finetech 2.0 Paper: Rebooting financial services’ [2015] Santander InnoVenture.
21. D. Yermack, ‘Corporate Governance and Blockchain’ [2015] NBER Working Paper.

Legislation

1. Regulation (EU) 2016/679 of the European Parliament and of the council on the protection of natural persons with regard to the processing of personal data [2016] OJ L 119.

Cases

1. Patrick Beyer v Bundsrepublik Deuschland, Case C-582/14 [2016].

DIGITALIZATION IN LABOUR LAW – THE OPPORTUNITIES AND CHALLENGES

Rietveld Rachel[1]

Abstract

The judiciary labour market is already changing and will shift more quickly. For example, in the Netherlands the judicature is implementing digital litigation, which causes job loss for 60% of support personnel. Other examples include large law firm offices that hire legal specialists or implement the usage of document generating tools. By doing so, employment costs diminish and the speed of the legal process increases.

A step further in digitalization possibilities are tools that provide a ruling. Watson, is a famous example of AI. This is a system that can 'only' generate answers to questions from information in articles, websites and books. It is a highly sophisticated application of artificial intelligence, but is not able to predict the outcome of legal cases in common law. In this paper, we will first distinguish artificial intelligence from systems built by humans and with human interference. Decision-making based on algorithms differs from artificial intelligence implementations such as machine learning or deep learning.

The next step is using a showcase model to describe the possibilities, but also the limitations of digitalization in law. We ourselves have been experimenting for several years with a digital tool (see www.magontslag.nl, in Dutch) that generates all of the legal documentation an employee needs for a dismissal procedure in court. This is an example of decision-making by algorithms programmed by humans. All the employee has to do is simply answer questions about the facts of his case. The outcome is an evidence-based prediction of the ruling of the judge. We tested the system with 400 cases derived from judicial decisions and, in 93% of the cases, the outcome of the digital tool coincided with the ruling of the judge. The system in the meantime has been expanded and it can fully determine the legal position of the employee as well of the employer in a dismissal.

By building these tools, many of problems and questions arise: not only technical problems, but also multidisciplinary and ethical ones. In this paper we will explain in more detail how the tools deal with the limitations of digitalization and which multidisciplinary questions arise using the tools. There are restrictions, so we will look into the question whether we need to set boundaries to the implementation of these tools and if so, what they can be in order to prevent prejudice by digitalization and only maximize the benefits.

Keywords: labour law, legal position, decision-making tools, accessibility of law

Introduction

Due to rapidly growing new technologies and globalization, digitalization is a hot topic. Digitalization brings changes; worldwide and in all levels of playing fields. It makes us legal experts investigate the consequences of digitalization for the division of labour and application of labour law itself. We wonder what consequences the introduction of new techniques, such as robots, will end up having on legal experts and also on civilians. eBay now decides 60 million disputes a year, completely digitally.[2] In Europe, too, there has been the possibility of digitally dealing with cross-border consumer disputes since 2016. In the first year 24,000 disputes were dealt with in this manner.[3] The digital developments in the law had Richard Susskind sighing back in 2010: "*the central theme ... is that lawyers should change the way they work. Better and more efficient techniques for delivering legal services are emerging and I urge the legal profession to embrace them*.". He is not all too optimistic himself that his plea will be heeded: "*More*

[1] *Rachel Rietveld is investigator and developer with ArbeidsmarktResearch Uva B.V., a Company which builds and sells digital employment law systems (www.magontslag.nl, only in Dutch). She is also a PhD-candidate writing a dissertation on „The use of data in (labour) law".*

[2] http://www.fbdebt.co.uk/2016/10/ebay-style-online-resolutions-court-future-debt-recovery-cases/.

[3] http://europa.eu/rapid/press-release_IP-17-727_en.htm.

worrying still, I fear that few law schools are preparing our future law students for the very different workplace that I and others are predicting."[4]

In this paper I will look deeper into possibilities and changes of digitalization in labour law, especially decision-making tools based on algorithms programmed by humans (instead of artificial intelligence). Therefore, I will describe how I categorize digitalization. First, I will then go into an example of this kind of tools and end with an explanation of limitations, opportunities and desired boundaries, without pretending to be anything near complete.

1. Digitalization in categories

Digitalization is a broad term. Putting text in a Word-document is a form digitalization, as is an app for any kind of business and as are robots. Before digging into possibilities, we have to categorize forms of legal digitalization. Because all forms have differences as well as similarities, it is hard to set sharp boundaries for the different forms. We can look at it from different points of view, such as time savings for the user, legal knowledge for either developer or user and complexity of techniques. For this paper I chose to distinguish applications based on the set goal, hence the purpose of the tool. Therefore, I distinguish four categories.

The first category is simply about process automation within (legal) companies. They are for example platforms collecting and organizing documents, automated calendars or decision trees making certain processes transparent. They can be used internally or as a tool to communicate with clients. In the Netherlands a good example is KEI, a judicial reform that was meant to make digital litigation possible. In the beginning of April, the news came through that the project failed and that the goal was going to be limited to making civilians and lawyers communicate with the court in a save, digital environment.[5]

A next category is also about process automation, but then for legal steps or documents. Tools in this category generate standard legal documents by making the user fill out the blanks. There's no legal check built in, so the users are free to fill out whatever they want, without the tool checking whether it is compliant with the legal framework. Of course, the developer has to have a sufficient knowledge of that specific subject, but most of the subjects suitable for text generators are not that difficult. Also, most chatbots are a form of legal process automation. Digital systems, which help the jurist to generate digital legal documents, are increasingly used.[6] In the words of Susskind, this issue is not a 'legal disruptive technology', because this form of digitalization fits the way in which traditional legal labour is now organized.[7]

The third group contains tools and applications that digitalize legal decision making. This technique demands a high knowledge of law as well of the way to compose proper algorithms and translate them into software. It is almost a mathematic way of approaching legal questions, making sure all scenarios are covered. By doing so, the user's legal position can be estimated based on questions and given answers. The right wording of these questions is important, both to allow target users to understand the question and to precisely address the issue. These tools also generate documents, but in this category these documents differ from the ones in the second category because they are made especially for the specific situation of the user. I will dig in to the details of these tools in the next paragraph.

Finally, there is artificial intelligence. It is not really a separate category, since artificial intelligence is a way to come up with tools, hence a form of development. The first reason to take this technique aside within the legal field is an important one. To get a proper artificial intelligence tool, it is necessary to fulfil the demands of the 'four V's': velocity, variety, volume and veracity. In Dutch labour law, but also in many other legal jurisdictions, it is impossible to use artificial intelligence due to a lack of one or more of the V's. For example, law is changing rapidly, not all case law is published and barely no case is similar to another, which makes it impossible to make a system learn something from previous cases. The second reason

[4] R. Susskind, 'The End of Lawyers?: Rethinking the nature of legal services' (2010) pp. 7, 276.
[5] https://www.nrc.nl/nieuws/2018/04/10/digitalisering-rechtspraak-moet-opnieuw-a1598839 (newspaper in Dutch).
[6] See among more, e.g.: www.rossintelligence.com, www.clio.com, www.law.standfort.edu, www.rocketlawyer.com, www.legalzoom.com.
[7] R. Susskind, *Ibid*., p. 275.

to distinguish artificial intelligence from the tools described in the third category, is the large difference in figuring algorithms. With machine learning or deep learning, complexity is limited, since the system is not cleaver; it does not learn itself and cannot cope with unstructured data. On the other hand, human beings can establish clear linkages. They can designate aspects that are decisive and can interpret open norms. That is why we need human interaction for setting algorithms. Even more so, to keep a transparent decision-making system instead of the black-box artificial intelligence is.

2. Digital decision making; an example

In the Netherlands we are experimenting with a digital tool in the third category as described above that generates all of the legal documentation an employee needs for a dismissal procedure in court, just by simply answering questions. The system is not just a database or questionnaire, but contains multiple interactive decisions trees, all connected, which leads to a tool with hundreds of questions and formulas. A question is either posed or not, depending on answers to the previous ones, so the user never has to fill out all the questions in the system. Many answers contain some form of weighing, for example points in the range of minus twenty up to plus twenty. By calculating the scored answers and setting an algorithm for the outcome bases on the total score, the legal position of the user is estimated. Also, other forms of weighing are possible. It depends on the legal question the tool is built for and on how case law handled that question. For example, the question whether employees can be dismissed in their probationary period, depends on straight forward questions such as the duration of the contract and whether a collective labour agreement is applicable to the contract.[8] On the other hand we have reasons for dismissal which has to be judged based on all the circumstances of the particular case. That means that eating leftovers can be qualified as theft in one situation, but with slightly different circumstances it will not be. To make the tool generate the right estimation, algorithms are necessary to weigh all the different factors.

The outcome is an evidence-based prediction of the ruling of the judge in the same case, so the employee has an evaluation of his legal position and in the event his position is worth litigating, the digital tool generates the legal documents he needs for the procedure in court. The system his scientifically calibrated and validated. To make the questions, we had to study all available information, from the making of the law, the law itself and all case law. As soon the tool was ready, we tested the system with 400 different cases derived from judicial decisions and in 93% of the cases, the outcome of the digital tool coincided with the ruling of the judge. The system has in the meantime been expanded and it can fully determine the legal position of the employee in a dismissal procedure and thereby generate the documents which the employee needs to enforce that position in court. The tool which the employer can use to estimate his legal chances in the event he wishes to dismiss an employee, is almost ready, and in that case, too, the tool generates the documents necessary to this end (application to the sub district court, etc.).

The system is available online and costs only 38 euros per legal case. This amount does not nearly cover the real expenses, but one of the purposes of the tool is to enhance the accessibility of law. Although the amount is also much lower than the price of advice of a legal expert, not many employees use the tool autonomously. The system is mainly used by large 'legal expenses insurers[9]'' or law firm offices, who use the tool to manage expectations of customers and to give the employees a correct estimation of the feasibility of a case.

3. Possibilities of decision-making tools

The digitalization of employment law has many advantages. It makes justice more easily accessible, since the consumer can fill out tools from home, at any time and mostly independently. There is no limitation or threshold, accept from having a computer with internet. Secondly, it is remarkably cheap. This of course is not always the case, but tools should always be cheaper than hours of human labour if

[8] In the Netherlands employers can set employment contracts for a certain amount of time instead of an indefinite period of time.
[9] In The Netherlands it is called ‚Rechtbijstandsverzekeraar: https://www.rechtsbijstandverzekering.com/eng/#kz.

available and used at sufficient scale. Another benefit of the use of these kinds of tools is the fact they are always asking for every possible situation. Where legal experts leave out some questions because they rest on the story of their client, the systems will – if built correctly – not skip a possible legal argument.

The tools give a reliable and objective prediction of the legal position. Because of this, more people can use their legal rights, simply because they get to know them. Nowadays a high number of employees will probably undertake no actions against the decision of their employer, although their case gives them have a good reason to go to court. On the other hand, numerous employees retain a lawyer without having good legal arguments to do so. They spend money unnecessarily.

With the prediction of the legal position, tailor made documents are generated. Even if the user likes to retain a legal expert, the documents can be adjusted by this expert and this will save much time. This also makes legal advice cheaper, although the tools are not directly used by the employee or employer.

Another way of using the tools by or through legal experts can help the judiciary system become cheaper and better. The conflict can be increased by making both parties fill out the tool, connect the results and see what the real argument is. Undisputed legal arguments stay out of further discussion. It offers an easy way to settle disputes without litigation. Using the tools in that way makes it also easier for a judge to ask about the specific problem instead of checking all details of the case. Compared to the 'old fashioned' way of finding out legal opportunities and decision making, this form of digitalization leads also towards legal certainty and equality. In case law, judges make different decisions due to their discretionary power. This is meant to be a good power, but what if the verdict is based on the good or bad behaviour in court? In criminal law it makes sense to give regret a role, but not in every jurisdiction it does. Is it considered fair that the employee who brings in his cute little children and acts perfectly fine towards the judge, will get a higher severance pay than the employee who is nervous or indifferent? Tools are not influenced by the behaviour or appearance of the user and will generate the same outcome if the same answers are given. If used in court, it is up to the judge to derogate from the outcome of the tool. In that case law is still more certain and equal, due to the fact that motivated deviation gives more insight of decision-making than summing up facts with a conclusion.

4. Limitations of decision-making tools

At first, it should be stressed that making tools that predict the ruling of the judge is highly expensive. To implement all the necessary options such as making interactive decision trees that contain the weighing of arguments, generating tailor-made documents, as well as user options such as multiple types of answers and room for explaining their specific situation, extremely well developed existing software is needed or it must be tailor made. By doing so, communication between legal and technical experts is one of the largest issues. This is what makes most digitalization projects end up as a failure.[10] This failure also has to do with the main aspect of decision-making tools: applying logics, which is not the main skill of legal experts. By developing these tools, all legal options should be specified in 'if …, then …'-algorithms, which is a hard exercise. Even when people are trained to apply logics for solving problems, it is hard to see whether all possibilities are set, if they are connected the right way, *et cetera*. That is, next to knowing technical possibilities and boundaries, not what legal people are trained on. On the other hand, the legal expertise is needed to set the right questions to solve a legal problem and to determine open norms.

An extra difficulty on making these tools is language. Two examples concerning the use of language may illustrate this. Most legal experts tend to use difficult language and legal terms, whilst people of all different levels of education have to be able to use the tools and fill out the proper answers. When converting complicated content to easy, daily used language, the risk is that the meaning of the question changes. It is crucial for the estimation the tool is making, that the right answers are given. This also requires a right way of asking questions. Many people tend to ask more than one question in one

[10] For example, KEI, the system mentioned in paragraph 1, was estimated on € 7,000,000 and costs over € 220,000,000 already.

sentence, but then it is impossible to give a right answer. Also, questions should not be subjective, otherwise the user is tempted to give another answer than the truth.

Besides problems concerning development, there are some ethical limitations of computerized systems. One may be that the 'human factor', especially important in judging employment cases, is being neglected, thus leading to more injustice. A decision-making tool can partly resolve this, by asking questions with regard to those aspects, too, but it will never equal a human decision based on a sense of justice. On the other hand, it can be argued that this human factor and the sense of justice are more likely to entail injustice, like stated before. Also, by making people fill out the tools, we neglect the social role of a legal expert. An employee who just got fired, needs to be heard and the employer has an urgent need to share his anger. A computerized system ignores social facts and emotion. Again, this can be a benefit, since it saves time and law is not to be set by emotions.

Another risk is that the digital system will monopolize legal debates. In legal reality, over time, the tool may become the benchmark, rather than the underlying rules incorporated in the tool. This risk can be controlled if the algorithm in the system and the system itself are transparent, but for whom can that goal be reached?

5. The change of legal education

If the described tools are used on a larger scale, this will lead to significant changes in the legal profession. The billing-by-the-hour model that law firms now use will not be a sustainable model. As described above, it therefore satisfies the description of Susskind's disruptive system. This includes such things as setting up 'legal shops', where justice seekers find low-threshold assistance by engaging acting jurists who use the tools in their advice. In that case there will be a need for, on the one hand, jurists who can work with the tools, and on the other hand, jurists who can build the tools or can assess what questions must be asked in relation to the legislation to achieve an outcome in a specific case. With regard to the first group, it is questionable whether they need a university law degree (master's or higher), or whether a bachelor's degree (in legal studies; higher professional education) could suffice.

In some Dutch bachelor-level legal studies, the use of digital tools is already a mandatory part of the course. This has consequences not only for the labour market, but also for the course. To fulfil the need of developing more tools and considering the described problems that currently arise due to a lack of multidisciplinary educated people, further change of the curriculum is needed. Not only for the development of systems that make law more accessible, but also to reach a sufficient level of quality by doing so.

Conclusions

Digitalization is an ongoing process that will develop even further. To be able to discuss digitalization properly, we need to define categories. In this paper the focus is on decision-making tools based on algorithms set by human interference, that give the user an estimation of his or her legal position. Tools in other categories do not require much legal knowledge or are not suitable for offering good quality and transparent legal help.

Without being complete, I have set out a wide range of opportunities and boundaries of these decision-making tools. Although high effort is necessary to develop more tools, it is definitely worth doing so. Law is there for everyone, not only for legal experts, so we need to use any option to improve the accessibility and quality of legal aid. To secure these purposes, we need to enhance education and training in the legal field. Students and experts should be trained in a more multidisciplinary way, not only in order to develop tools, but also to use them properly and to be able to see whether the estimation is done correctly. In order to keep a high level of quality, we also need to set boundaries and guidelines for the development and use of tools.

Bibliography

1. http://europa.eu/rapid/press-release_IP-17-727_en.htm .
2. http://www.fbdebt.co.uk/2016/10/ebay-style-online-resolutions-court-future-debt-recovery-cases/.
3. https://www.nrc.nl/nieuws/2018/04/10/digitalisering-rechtspraak-moet-opnieuw-a1598839.
4. R. Susskind, 'The End of Lawyers?: Rethinking the nature of legal services' (2010).

EXCEPTIONS TO PATENT PROTECTION ON THE GROUNDS OF ORDRE PUBLIC AND MORALITY

Rudzite Liva[1]

Abstract

Molecular biology and genetics have evolved to a level where specific genes are sought, genetically modified organisms are created, and gene therapy is used. As one of the means of research it is used in the field of creation of genetic modifications as well as in gene recombination. The amount of resources invested in an invention encourage companies and scientists to legally protect the result of innovation by applying for a patent.

Albeit scientists and companies desire to exploit their inventions as commodities, not all inventions may be treated and distributed as such. One of the fields where the broadest controversy has appeared between a desire to remuneration for invested resources and efforts, on the one hand, and argument of inventions as common heritage, on the other hand, is biotechnology and life sciences. In order to balance the conflicting interests various legal mechanisms have been implemented, for instance, list of exceptions, which are not patent eligible, and also introduction of exemption to patent protection on the grounds of *ordre public* and morality. Nonetheless, as the case law demonstrates there exist considerable interpretational diferences amongst the courts and countries especially in the field of patentability of morally and ethically ambiguous inventions, which renders to consider, whether the existing practice does not signalize for a necessity to introduce clarity at a legal level.

Key words: invention, biotechnology, patentability, ordre public, morality

Introduction

On practical level, genetic research was launched in the 19th century but the last six decades have been a milestone in the development of genetics. Genetic studies have basically been influenced by the leading theoretical and philosophical understandings about genetics, which in turn have had a considerable impact on the development of legal frameworks as Charles Darwin's theoretical concept of eugenics[2]; positive eugenics (F. Galton)[3], negative eugenics[4] and new eugenics (R. D. Hotchkiss).[5]

It can be concluded that the uniqueness of a person according to those theories was not an objective but a mean to achieve it. Human nature was perceived as a way of implementing political and economic policies. From the perspective of scientists research was not conducted in order to restrict rights of people, but to aid to strengthen them by eliminating barriers to realization of rights and freedoms, for example, by discovering the genes that cause illness when developing drugs. Detection of a function of each gene gives an impression that solution to the genetic myth is the explanation of all the issues, indicating that, leaving genes under natural pressure, it is not feasible to talk about human free will as it is controlled by genes. An identical view substantiated 'Human Genome Project' at the end of the 20th century with the purpose to decipher the DNA and to create a genomic card, considering that dismissive attitude of the society was exaggerated, because finding out all the genes would mean to finding out who really is a human.[6]

[1] *Mg.iur. University of Latvia; Mg. iur. Riga Stradins University in the field of Medicine Law. Research interests: Law and Technology, Medicine Law, Bioethics, Intellectual Propert Law, International and EU Law.*

[2] R. C. Engs, 'The Eugenics Movement and Encyclopedia' (London: Greenwood Press 2005) xiv.

[3] *Ibid*., xii.

[4] *Ibid*., xiv.

[5] *Ibid*., pp. 88-89.

[6] C. A. Tauer, 'The Human Significance of the Genome Project' [1992] in T. A. Shannon, 'Genetic Engineering. A documentary History' (London: Greenwood Press 1999) p. 108.

The above mentioned standing point contradicts with the categorical imperative of I. Kant (I. Kant), which as a fundamental principle expresses importance to respect separation of the man from other living beings and also prohibits use of human beings only as a means.[7]

Another theories have been developed for example by C. Nägeli who thought that body cells carry the hereditary and A. Weisman who concluded that hereditary derives from the special substance with a complex structure that is present in the nucleus of a cell, namely the chromosome. Single-cell organisms and germs are potentially immortal, but bodies of multi-cell organisms serve only to maintain and protect an external idioplasm. His experiments proved that life-time changes in characteristics did not occur in offsprings.[8]

The above mentioned opinions may be comforted only partly. The body can not be disconnected from the cell because the cell is the basic unit of the body; cells form the body not *vice versa*. It would be more complete to suppose that the body is not surrounded and protected by cells but cells form the body, including the immune system and the skin, which is the largest body organ and the main cell protector.[9] Besides, only through interaction of genes and environment the body becomes complete and forms phenotype[10] and personality. Therefore, discussion about the hereditary (for instance, Lamarck's evolutionary theory expresses the recognition that the acquired features of life are born in the offsprings[11]) mirrors only a part of the comprehensive understanding of the issues, subsequently, it reflects that there exist significant interpretation differences even about the kernel of genetics.

Hence, in order to acquire multilateral understanding about the 'content' of living organisms it is necessary to understand the structure of gene and DNA.

Genetical structure

From genetical side living organisms consist of cells, basic units of the organism. On the basis of the cell type organisms are divided into prokaryotes and eukaryotes. Prokaryotes (bacteria and cyanobacteria) are single-branched, cell-free cells. Eukaryotes are multi-cellular organisms in which cells contain the core. Cells possess copies of the instruction set which forms and directs cells to form body parts. The set of instructions is called genes, which in turn consists of the DNA.[12]

Inside the core of a cell are yarns or chromosomes. A chromosome kit contains from 30'000 to 40'000 genes, which occupy the specific place in the chromosome - locus. In some organs a number of chromosomes in the cell nucleus is much higher than that of the species, for example, in the liver cells.[13] Each cell in the human nucleus contains 46 chromosomes, which consist of double nuclei of the nucleoside DNA.. Nucleotides contain one of the 4 bases (letters), which commands encoded instructions, consisting of three letters, as GGC or ATG, called codons.[14] The sequence of codons is made up of genes while the genes form the set of instructions that determine the order of the amino acid sequence. Amino acids are components of protein while proteins are responsible for cellular activity and are part of the body. The mechanism for using DNA coded information for protein generation is equal for all cells of living beings.[15] For humans 99% of genes are shared with other people, 98.5% of genes – with chimps, 90% - with mice, and 7% with bacteria.[16] Only 3% of DNA is built by genes, the rest is taken by an uncodified derivatives that control protein activity.[17]

---

[7] I. Kant, 'Werkausgabe in 12 Bänden. Die Metaphysik der Sitten' (Frankfurt am Main: Suhrkamp 1991) Bd. 8, p. 600.
[8] M. Loza and V. Loza, 'Ģenētika ar selekcijas pamatiem' (Riga: Zvaigzne 1991) p. 12.
[9] Collective of authors, A. Blugers (ed.), 'Āda: Populārā medicīnas enciklopēdija' (Riga: Galvenā enciklopēdiju redakcija 1985) 3rd ed., p. 13.
[10] M. Rutter, 'Genes and Behavior. Nature-Nurture Interplay Explained' (The USA: Blackwell Publishing 2006) p. 89.
[11] B. R. Wellington, 'The spirit of system: Lamarck and evolutionary biology: „Now with Lamarck in 1995"' (The USA: Harvard University Press 1995) p. 143.
[12] L. H. Hartwell, L. Hood, M. L. Golberg, A. E. Reynolds, L. M. Silver and R. C. Veres, 'Genetics From Genes to Genomes' (New York: The McGrow Hill Companies 2008) 3rd ed., p. 394.
[13] M. Loza and V. Loza, *Ibid*., p. 20.
[14] *Ibid*., p. 39.
[15] B. Lewin, 'Genes' (Singapore: John Willey & Sons 1987) 3rd ed., p. 78.
[16] R. Volkers, 'Zināmais – nezināmais. Gēni un DNS' (Riga: EVE 2004) pp. 36-37.
[17] State v. Johnson, Case No.813 N.W.2d 1 [2012] Minnesota Supreme Court.

Regarding cell types, there exist somatic and germ cells from which only the latest are responsible for forming a new human being. Another differentiation of cell types are totipotent (early development cells, able to develop into all various types of cells needed for a complete and functioning organisms); pluripotent (such as embryonic stem cell lines, able to develop to the most types of tissues but not able to bring a functioning organism into existence); multipotent (able to develop to a limited number of tissue types).[18]

In addition, no connection exists between the number of genes and the number of functions. Genes are those which perform a function, but in a way that they only indicate a direction of the function, but are not responsible for an ultimate manifestation, because that is determined by nature.[19] There are separate genes that cause not only one but several enzyme defects. There are also cases where mutations only affect the tissue of a subtype of gene expression, for example, in the case of Huntington Korea.[20]

Anatomic development

Although individual development of a person during the period up to birth (usually 38 weeks) is gradual, from medical perspective the stage of the embryo and the stage of the fetus are distinguished.[21] The doctrine mirrors different opinions of the distinction line between embryo and fetus. One theory is that there are four stages of the development: 1) gametogenesis (period before conception); 2) prenatal period (from conception till 28 week of development) which consists of: a) blastogenesis (from conception till 15 day which is pre-embryonic or germ period); b) human embryogenesis (from 16 to 60 day after conception when germ is being called 'embryo'); c) fetogenesis (from 61 day till birth when new organism is being called 'fetus' or 'foetus'); 3) prenital period (from 28 week till birth); 4) postnatal period (after birth).[22]

Another theory divides anatomic development into three stages: 1) pre-embryonic stage (first 2 weeks after conception); 2) embryonic period (3-8 week); 3) fetus period (9 week till birth).[23]

Nonetheless, for instance, the Advocate General in his opinion in the case 34/10[24] has considered that there exist differences between the Member States of European Union in the aspect about the status of the embryo - the first considering that human embryo exists from fertilisation (Estonia, Germany and the second taking the view that it is from time when the fertilised ovum has been transplanted into the endometrium (Spain, Sweden).

Recapitulating, it can be seen that there are no consensus not only about the functions of the body at genetical level, but also about the formational stages of body and the physical status of the new organism. Lack of consistent information about the core concepts of genetics has led to the development of various concepts and has created fruitful soil for introduction of controversial inventions and, subsequently, their application of patent protection. Moreover, inconsistency of united understanding about the basic genetical concepts has encouraged development of different approaches amongst the countries which, consequently, hinders development of scientific research and legal certainty.

Patents of biotechnological inventions

In order to obtain patent five basic requirements must be fulfilled – 1) invention, which is new compared with the previous level of technics; 2) criteria of obviousness; 3) commercial utility; 4) an object of invention. The state may prescribe which objects are not to be declared as patentable in their nature or as a result of contradictions with public order and moral considerations; 5) feasibility which refers to a sufficiently clear and comprehensible description of an invention.

[18] UNESCO International Bioethics Commitee Report on the Ethical Aspects of Human Embryonic Stem Cell Research [2001] BIO-7/00/GT-1/2 (Rev.3) 3.
[19] *Ibid*., p. 153.
[20] M. Rutter, 'Genes and Behavior. Nature-Nurture Interplay Explained' (The USA: Blackwell Publishing 2006) p. 130.
[21] G. Brazma, 'Bioētika: Cilvēka dzīvības radīšana un pārtraukšana' (Jelgava: Jelgavas tipogrāfija 2010) p. 6.
[22] M. Pilmane and G. H. Sumahers, 'Medicīniskā embrioloģija' (Rīga: Rīgas Stradiņa Universitāte 2006) p. 17.
[23] J. Merkovs, 'Cilvēka embrioloģijas pamati' (Riga: Literātu brālība 2010) p. 8.
[24] Opinion of Advocate General Oliver Brüstle v. Greenpeace eV Case No.34/10 [2011] CJEU, pp. 67-69.

Depending on the type of invention protection may be obtained on the basis of: 1) product patent; 2) process patents; 3) product-technology patent means that patent protection will automatically be granted to the product when applying for a patent, for example, in the case of gene sequencing patent applications; 4) result of result patent - the application is based on cases where additional research is needed to support inventiveness of the invention.[25]

One of the most ambiguous aspects in the process of granting patents is the criteria of patentable object especially stated discretion for the countries to introduce exceptions on the grounds of public order or *ordre public*, which covers protection of public security and physical integrity of individuals as part of the society[26], and morality, which governs the totality of human behaviour, both personal and social.[27] The concept by itself includes hurdles as it states that there are no unifed binding document which would stipulate standard set of explanatory criteria. On the contrary, sovereignty has been left to the states which by the definition realms multilateralism and hinders transaparency of patent protection.

Therefore, in order to gain understanding of the criteria different regulations should be observed.

TRIPs Agreement

One of the most significant international intellectual property documents is the Agreement on Trade-Related Aspects of Intellectual Property Rights (hereinafter referred to as the TRIPs Agreement) on 1 January 1995[28]. The Article 27 (3) of it states that as objects of inventiveness are not considered: a) diagnostic, therapeutic and surgical methods for the treatment of humans and animals; b) business methods; c) production of plants and animals or their processes, with the exception of micro-organisms. However, members protection of plant varieties shall provide either by patents or by an effective *sui generis* system or by any combination thereof. According to the Article 27(2) members may exclude from patentability inventions prevention within their territory of the commercial exploitation of which is necessary to protect *ordre public* or morality, including to protect human, animal, plant life, health or to avoid serious prejudice to the environment, provided that such exclusion is not made merely because the exploitation is prohibited by their law.

In order the above mentioned exceptions to be applicable it inicially must be proven that not the invention *per se* is contrary to *ordre public* or morality but the commodification of it may cause such harm, therefore the stated restriction is necessary – when no alternative measure could reasonably be applied which could equally prevent the patenting of the invention.[29] The room for the manouvre of the states is very narrow because as it is stated above such exclusion must not be introduced merely because the exploitation is prohibited by their law. Albeit the TRIPs do not contain explicit definition of the terms 'technology' and 'invention' and does not *expressis verbis* include distinction between unpatentable discovery and unpatentable invention, however it explicitly states that naturally occuring biological material as DNA, viruses, plasmids, cell lines and other micro-organisms are patentable (Article 27(3)b). Consequently, it means that, for instance, DNA sequences and cells are patentable no matter, whether are requested as only the layer which includes information or as genetic information *per se*.[30] In addition, member states are not allowed to exclude from patent protection materials priory existing in nature.[31]

Concluding, all TRIPs member states are obliged to itroduce the above mentioned concepts and recognise patentability of naturally existing material as well as cells, DNA sequences. TRIPs attemted to strike balance between the rights to patent holders to benefit from their inventions and the rights of countries to lighten their health priorities through the provisions of affordable medicines, for instance, excluding and from patentability diagnostic, therapeutic and surgical methods, nevertheless it does not

[25] Ethical Aspects of Patenting Inventions Involving Human Stem Cells: EGE notification' [2002] O.J No.16, pp. 6-7.
[26] Plant Genetic Systems / Plant Cell [1995] EPOB No T356 / 93.
[27] C.F. Mooney, 'Public Morality and Law' [Cambridge: Cambridge University Press 1983] Vol.1, No.1, p. 45.
[28] Agreement on Trade-Related Aspects of Intellectual Property Rights [1995] WTO.
[29] WTO Panel Report 'Thailand – Restrictions on Importation of an Internal Taxes on Cigarettes' [1989] BISD 37S/200.
[30] J. Straus, 'Optionen bei der Umsetzung der Richtlinie EG 98/44 uber den rechlitchen Schutz biotochnologischer Erfindungen' [2004] No.12.4.1.
[31] C. Correa, 'Implementing the TRIPs Agreement in the Patent Field – Options for Developing Countries' [1998] Journal of World Intellectual Property 1 pp. 75, 79.

prevented states from biopiratism. Furthermore, the USA have attempted to pursue novel trade agenda, trying to influence the laws and policies of other countries well above and bellow as stated in TRIPs, as allowing to patent diagnostic, therapeutic and surgical methods, thus prioritizing profits of pharmaceutical industry over the universally relevant public health goal of affordable medicine.[32]

Scope in Europe

Aaccording to the Rule 27 in conjuction with the Rule 30 of the Implementing Regulation to the Convention on the Grant of European Patents[33] (hereinafter – EPC) patentable are also: 1) biological material, which is isolated from its natural environment or produced by means of a technical process even if it previously occurred in nature; 2) plants or animals if the technical feasibility of the invention is not confined to a particular plant or animal variety; 3) a microbiological or other technical process, or a product obtained by means of such a process other than a plant or animal variety; 4) an element isolated from the human body or otherwise produced by means of a technical process, including the sequence or partial sequence of a gene, even if the structure of that element is identical to that of a natural element only if the industrial application of a sequence or a partial sequence of a gene is disclosed in the patent application.

Nevertheless, the Rule 28 in conjunction with the Rule 29 stipulate exceptions to patentable invention: 1)processes for cloning human beings; 2) processes for modifying the germ line genetic identity of human beings; 3) uses of human embryos for industrial or commercial purposes; 4) processes for modifying genetic identity of animals which are likely to cause them suffering without any substantial medical benefit to man or animal, and also animals resulting from such processes; 4) plants or animals exclusively obtained by means of an essentially biological process; 5) the human body, at the various stages of its formation and development, and the simple discovery of one of its elements, including the sequence or partial sequence of a gene.

Furthermore, appart from the above mentioned exceptions the Article 53(a) of the EPC states that patents shall not be granted to the inventions the commercial exploitation of which would be contrary to '*ordre public*' or morality; such exploitation shall not be deemed to be so contrary merely because it is prohibited by law or regulation in some or all of the contracting states. The EPC does not contain the definition of the public order or morality. It may be seen that the existing exceptions have been implemented based on the historical pace of interpretation of genetics and patentable invention. As it derives from the Guidelines of EPC[34] the purpose of the exception is to exclude inventions which are likely to induce riot, public disorder or lead to criminal or generally offensive behavior.

Although the Article gives the direction to the national law of the state, however in the case of European patent applications, it is primarily not the position of a particular state to be taken into account, but the European-wide understanding of these concepts. Therefore, in order to obtain the guidelines of the interpretation of the concepts, decisions of the European Patent Office (hereinafter - the EPO) must be observed.

Considering the decisions, it stands out that the understing about the public order and patentability of biotechnological inventions varies depending on the type of invention. For instance, albeit the EPC states that inventions, which may be technically associated with the particular plant or animal variety are not patentable, however the understanding about the plant and animal variety significantly differs. Unlike plant varieties, the EPC does not protect animal varieties from patentability. It has been clearly stipulated in the *Oncomous*[35] decision. Deciding, whether the modified mouse is considered to belong to the animal breed, the EPO stated that the animal is not naturally occurring and the invention is patentable. EPO excluded from the patent application other animals potentially exposed to similar experiments, including

[32] R. Lopert and D. Gleeson, 'The High Price of ''Free'' Trade: U.S. Trade Agreements and Access to Medicines' [2013] Global Health and the Law.
[33] EPO Convention on the Grant of European Patents (European Patent Convention) [1973].
[34] EPO Guidelines for Examination in the European Patent Office [2017].
[35] Onco-Mouse [2004] EPOB No T-315/03.

rodents and non-human mammals, arguing that their use in experiments would not be supported, without providing a detailed explanation.

In *R v. Leland Stanford*[36] decision the EPO evaluated patentability of the mouse, which contained red blood cells, stem cells derived from aborted fetuses or young children with the aim to create anti-cancer cells or obtain grafts. The opponents claimed that it is unacceptable to create human-animal chimeras, to obtain stem cells from aborted fetuses or for less than three years young children as a resource for the creation of human tissues. It is not acceptable in Western countries to patent life or usage of human stem cells in animal modification. Granting of such patents may lead to the restriction of medical research by monopoly holders. Such patents can lead to the spread of inappropriate transplants and dangerous viruses. The EPO pointed that the applicable rule in the present case is the Article 53 (a) of the EPC (*ordre public*). Eventually, the EPO recognised the patent as valid, arguing that, since the invention has a legitimate aim, the EPO cannot act as a moral censor. Rejection of a patent only due to the ethical reasons without taking into account the usefulness of the invention in the development of medicine, is not acceptable.

What stands out from the above mentioned is the approach of the EPO to circumvent the burden of proof to the opponent. That kind of method may not be applicable in the process of awarding patents because the minimum criteria should be ascertainable in any case: the existence of a legitimate objective and proportionality reviewing the principles, theories, and remedies already recognized, which naturally leads to the evaluation of the *ordre public*. As the EPO is the main institution and policy maker on granting European-wide patents, hence in order to develop unified understanding on the process and criteria, necessary prerequisites should be defined and evaluated in every case.

Conversely, in the case of *Stem cells v. WARF*[37] the EPO decided to grant a patent for *in vitro* fertilization of embryonic stem cells. The submiter articulated that the creation of the cells does not apply to the commercialization of the embryo. The EPO stated that in order to evaluate industrial applicability of a product it should at the first be created. Attributing a patent to create a product, is *per se* commercialization. As the use of stem cells results in the destruction of the embryo, it cannot be industrially used and patented.

In the decision of *Plant Genetic Systems*[38] the EPO decided, whether an invention related to the transformation of plant cells in a way that disrupts its DNA is attributable to the plant variety. The EPO stated that due to manipulation and DNA instability, a plant variety could not be detected. Inventions that are not explicitly implicit but implicitly attributable to the whole plant variety are also patentable, since they do not reveal the similarity of their genomes with the plant variety. However, in cases where an invention relates to a genetically modified variety of a known plant, it is not patentable.[39]

It can be concluded that there are more restrictive criteria in relation to plant patentability than to humans or animals. In case of humans, the restriction on the variety has not been established. Genetic modifications can be made to any person, regardless of race or other affiliation.

Directive (EK) 98/44[40]

The Article 5(1) of the Directive (EK) 98/44 states: 1) human body at various its developental stages is not patentable; 2) an element isolated from the body even equal to that occuring in the nature, otherwise produced by means of a technical process, including the sequence or partial sequence of a gene is patentable. The Article 6 stipulates that unpatentable are: 1) inventions where their commercial exploitation would be contrary to *ordre public* or morality; however, exploitation shall not be deemed to be so contrary merely because it is prohibited by law or regulation; 2) processes for cloning human beings; 3) processes for modifying the germ line genetic identity of human beings; 4) uses of human embryos for industrial or commercial purposes; 5) processes for modifying the genetic identity of animals which are

[36] Leland Stanford [2012] EPOB No T 1262/04.
[37] Stem Cells v. WARF [2008] EPOB No G 0002/06.
[38] Transgenic plant / NOVARTIS [1999] EPOB No G0001 / 98.
[39] Plant Genetic Systems / Plant Cell [1995] EPOB No T356 / 93.
[40] Parliament and Council Directive (EK) 98/44 on the legal protection of biotechnological inventions [1998] OJ L213/13.

likely to cause them suffering without any substantial medical benefit to man or animal, and also animals resulting from such processes.Thus, it may be seen that Directive (EK) 98/44 correlates with the EPC and TRIPs.

One of the most significant cases regarding interpretation of Directive (EK) 98/44 is the *Oliver Brüstle* case[41] where the Court of Justice of the European Union (hereinafter – CJEU) stipulated that with the 'embryo' should be understand the potencial being from conception because the aim is to protect the body at various its formational stages. Invention, which include subsequent destruction of embryos, may not be considered as patentable. Exclusion from patentability concerning the use of human embryos for industrial or commercial purposes also covers the use of human embryos for purposes of scientific research, only use for therapeutic or diagnostic purposes which is applied to the human embryo and is useful to it is patentable.

As it may be concluded, the judgment at the *Oliver Brüstle case* introduced considerable clarity at one of the most significant and controversial aspects of patentability of biotechnological inventions. Although the interpretation revealed at the decision about the understanding of 'human embryo' deviates from the previously considered medical understanding and approach conducted in various states, the CJEU ruled in favor of the moral and ethical values, namely, welfare of the society. That kind of binding decisions are essential in order to clarify the ambiguous cencepts introduced in patent law. Raw shift of interpretation burden to states may not only lead to multilateralism as it may be witnessed for instance in *Oncomous* case, but also hinder scientifical development. Therefore, the bodies, which have introduced the international and unified core concepts of patent protection should be those which provides the necessary interpretation and not transfer the onus of proof to the national states. Besides even amongst the various bodies exist interpretational disparities, for instance in the question of feasibility to use embryo in research pursposes[42], hence the binding and united interpretation is crucial. Moreover, as the EPO acts as independent organisation but has equalized the provisons of EPC with those stemmimg from the Directive 98/44, thus the CJEU decisions indirectly affects also the interpretation of EPC. Considering that EPO covers not only EU Member States, thus broader clarity may be introduced and encouraged common market in broader scope.

In addition, as it may be seen the CJEU concluded that embryo may be used in research if it is beneficial for it. Besides European scope does not prohibit patents of therapeutic and diagnostic methods. Therefore, theoretically patents of therapeutic cloning within the aim to use cells as therapeutic method could be granted. It is substantiated by the fact that patent could be claimed not on the basis of product but of process, thus excluding objections of naturally occuring substance. In addition, patent also may be claimed not as the human body *per se*, but on the basis of cell material, DNA sequences which are micro-organisms despite of constructing human body. Moreover, the prohibition stipulated in *Oliver Brüstle* case may not be applicable if it is claimed that the therapeutic method could be beneficial for embryo. Furthermore, the range of rejection arguments could diminish even more if, for instance, it is claimed that this therapeutic method is the only possible treatment. In that case, the patent examiners would be asked to balance the rights to health within the patent protection what could lead to the ethically sensitive debate, whether that kind of invention could be patentable and not exempted on the basis of *ordre public* and morality especially when made in a maneuver which does not include inclusion of nucleotides. To lead the question even further, one may try to seek protection not on the basis of patent but on the basis of copyright of itself or as a trade secret.

This example mirrors that leaving discretion solely to countries to determine the content of *ordre public* and morality could lead to even further inconsistency and understanding of patentable invention. As it is stated, for instance, in Japan, which is one of the leading countries in biotechnological research, there are no solid arguments against therapeutic cloning.[43] As it is evident from the considered regulation

[41] Oliver Brüstle v. Greenpeace eV [2011] CJEU No. 34/10.

[42] Opinion of the European Group on Ethics in Science and New Technologies to the European Commision 'Ethical Aspects of Human Stem Cell Research and Use' [2000] No 15.

[43] C.M. Borowski 'Human Cloning Research in Japan: A Study in Science, Culture, Morality, and Patent Law' [1999] 9 L. Rev.505.

and interpretation in case law the existing concepts lack of clarity and do not provide unifed understanding of patentable invention and, hence do not realm sustainable development of patent system.

Scope in the USA

The U.S. Patent Law[44] does not *expressis verbis* state the prohibition to patent invention which would be contrary to the *ordre public* or morality. In addition, the U.S. law does not *per se* separate discovery from invention as it derives from the Article I, Section 8, Clause 8 of the U.S. Constitution.[45] Discoveries are inventions which require a sort of human ingenuity as established in *Diamond v. Chakrabarty*.[46] Natural laws[47], physical phenomena, abstract ideas[48], natural minerals, and wildlife are not patentable, because of the natural values created by the community as a whole.[49] Diagnostic and therapeutic methods are not excluded from the subject of the patent. Moreover, as stated in *Myriad case*[50] where a claimed invention possessed the naturally existing genetical element that invention may not be patentable because it reflects naturally already existing element. In *Latimer*[51] case court stiplated that naturally existing object may not be considered as invention even afterwards discovered how to be isolated from nature.

It may be concluded that the USA approach differs from the European approach. According to the European approach naturally existing substance may be patentable if the claimed invention may fulfill requirements of patentability. Besides the USA approach does not *per se* support the process-product patent approach as it is in the European approach but rather evaluates them seperately, concluding that product patent may be granted only in case if the abstaintion could affect the realisation of process patent. Nonetheless, that approach may lead to a very broad patents which instead would hurdle social benefit and scientific research.

Conclusions

Development of genetical research and process of granting patents have been significantly influenced and determined by the leading theoretical, political beliefs and lack of sustainable legal clarity. In order to facilitate amplifaction of scientific research and, subsequently, encouragment of social welfare controversial patents have been granted which hinders fruitful development of inventions. Ambiguous criteria of process to grant patent introduce multilateralism amongst the countries instead of facilitation of commodification.

Furthermore, the existing diferences of legal regulation leads to different decisions in process of granting patents which, subsequently, creates even broader ambiguity. Therefore, more concrete criteria should be introduced and more clarified interpretations of the concepts of '*ordre public*' and morality should be provided, thus avoiding from prolonged and expensive application procedures.

Considering that international conditions of granting patents have been introduced in order to provide unified approach and facilitate commodification, therefore, international bodies should provide necessary and binding interpretation instead of transfering the burden to the national states which, consequently, would lead to the increasing disparities and hurdle trade, scientific research and welfare of the society.

Articulation of clear criteria is essential not only when considering existing patent applications, but also to providing sustainable development of transparent patent systems. That is significant considering the invested resources to creat invention. Besides, clear legal concepts would also avail scientists and patent examiners to unitedly balance the interests of the society, on the one hand, and interests of science

[44] U.S. Congress U.S. Patent Act [1952] U.S. Code Title 35.
[45] U.S. Constitution [1787].
[46] Diamond v. Chakrabarty [1980] 447 U.S. 303.
[47] Mayo v. Prometheus [2012] 566 U.S. SC 1289.
[48] Bilski v. Kappos [2010] 561 U.S. 593.
[49] Funk Bros. Seed Co.v. Kalo Inoculant Co. [1948] 333.U.S. 127 130.
[50] Association for Molecular Pathology v. Myriad Genetics, Inc. [2013] 398 U.S. SC. 12.
[51] Ex Parte Latimer [1889] C.D.

and investors, on the other hand. Hence, that will provide an opportunity to fruitfully solve further challenges created by technological and scientific development such as therapeutic cloning as treatment method and aid to use patent protection instead of looking of roundabouts as protecting invention as copyrights or trade secrets.

Bibliography

1. Agreement on Trade-Related Aspects of Intellectual Property Rights [1995] WTO.
2. Association for Molecular Pathology v. Myriad Genetics, Inc. [2013] 398 U.S. SC. 12.
3. Bilski v. Kappos [2010] 561 U.S. 593.
4. A. Blugers (ed.), 'Āda: Populārā medicīnas enciklopēdija' (Riga: Galvenā enciklopēdiju redakcija 1985) 3rd ed.
5. C. M. Borowski, 'Human Cloning Research in Japan: A Study in Science, Culture, Morality, and Patent Law' [1999] 9 L. Rev.505.
6. G. Brazma, 'Bioētika: Cilvēka dzīvības radīšana un pārtraukšana' (Jelgava: Jelgavas tipogrāfija 2010).
7. C. Correa, 'Implementing the TRIPs Agreement in the Patent Field – Options for Developing Countries' [1998] Journal of World Intellectual Property 1.
8. Diamond v. Chakrabarty [1980] 447 U.S. 303.
9. R. C. Engs, 'The Eugenics Movement and Encyclopedia' (London: Greenwood Press 2005) xiv.
10. Ex Parte Latimer [1889] C.D.
11. EPO Convention on the Grant of European Patents (European Patent Convention) [1973].
12. EPO Guidelines for Examination in the European Patent Office [2017].
13. Ethical Aspects of Patenting Inventions Involving Human Stem Cells: EGE Notification' [2002] O.J No.16.
14. Funk Bros. Seed Co.v. Kalo Inoculant Co. [1948] 333.U.S. 127 130.
15. L. H. Hartwell, L. Hood, M. L. Golberg, A. E. Reynolds, L. M. Silver and, R. C. Veres, 'Genetics From Genes to Genomes' (New York: The McGrow Hill Companies 2008) 3rd ed.
16. I. Kant, 'Werkausgabe in 12 Bänden. Die Metaphysik der Sitten' (Frankfurt am Main: Suhrkamp 1991) Bd. 8.
17. Leland Stanford [2012] EPOB No T 1262/04.
18. B. Lewin, 'Genes' (Singapore: John Willey & Sons 1987) 3rd ed.
19. R. Lopert and D. Gleeson, 'The High Price of ''Free'' Trade: U.S. Trade Agreements and Access to Medicines' [2013] Global Health and the Law.
20. M. Loza and V. Loza, 'Ģenētika ar selekcijas pamatiem' (Riga: Zvaigzne 1991).
21. Mayo v. Prometheus [2012] 566 U.S. SC 1289.
22. J. Merkovs, 'Cilvēka embrioloģijas pamati' (Riga: Literātu brālība 2010).
23. C. F. Mooney, 'Public Morality and Law' (Cambridge: Cambridge University Press 1983) Vol.1, No.1.
24. Oliver Brüstle v. Greenpeace eV [2011] CJEU No. 34/10.
25. Onco-Mouse [2004] EPOB No T-315/03.
26. Opinion of Advocate General Oliver Brüstle v. Greenpeace eV Case No.34/10 [2011] CJEU.
27. Opinion of the European Group on Ethics in Science and New Technologies to the European Commision 'Ethical Aspects of Human Stem Cell Research and Use' [2000] No 15.
28. Parliament and Council Directive (EK) 98/44 on the legal protection of biotechnological inventions [1998] OJ L213/13.
29. M. Pilmane and G. H. Sumahers, 'Medicīniskā embrioloģija' (Rīga: Rīgas Stradiņa Universitāte 2006).
30. Plant Genetic Systems / Plant Cell [1995] EPOB No T356 / 93.
31. M. Rutter, 'Genes and Behavior. Nature-Nurture Interplay Explained' (The USA: Blackwell Publishing 2006).
32. State v. Johnson, Case No.813 N.W.2d 1 [2012] Minnesota Supreme Court.
33. Stem Cells v. WARF [2008] EPOB No G 0002/06.
34. J. Straus, 'Optionen bei der Umsetzung der Richtlinie EG 98/44 uber den rechlitchen Schutz biotochnologischer Erfindungen' [2004] No.12.4.1.

35. C. A. Tauer, ‘The Human Significance of the Genome Project’ [1992] in T. A. Shannon, ‘Genetic Engineering. A documentary History’ (London: Greenwood Press 1999).
36. Transgenic plant / NOVARTIS [1999] EPOB No G0001 / 98.
37. UNESCO International Bioethics Commitee Report on the Ethical Aspects of Human Embryonic Stem Cell Research [2001] BIO-7/00/GT-1/2 (Rev.3).
38. U.S. Congress U.S. Patent Act [1952] U.S. Code Title 35.
39. U.S. Constitution [1787].
40. R. Volkers, ‘Zināmais – nezināmais. Gēni un DNS’ (Riga: EVE 2004).B. R. Wellington, ‘The spirit of system: Lamarck and evolutionary biology: „Now with Lamarck in 1995”’ (The USA: Harvard University Press 1995).
41. WTO Panel Report ‘Thailand – Restrictions on Importation of an Internal Taxes on Cigarettes’ [1989] BISD 37S/200.

CURRENT ISSUES OF LEGAL REGULATION OF EMPLOYEE'S PERSONAL DATA PROTECTION IN UKRAINE

Rym Olena [1]

Abstracts

The development of digital technologies and the spread of Internet usage are the features of the times we live in. That is why adoption of new legislation on the creation, dissemination and use of information is required. Almost unrestricted access to the Internet raises the issue of individual privacy protection and requires development of new approaches to personal data processing, including in the field of labor relations. Therefore, there is a pressing need for reforming legal regulation of these social relations. It is important to research and analyze foreign experience of legal regulation to improve the national labour legislation, its application and to meet the needs of the modern science of labour law.

In the context of the European integration process in Ukraine it would be extremely useful to study the long-term experience of legal regulation of employee's personal data protection in the EU.

Realizing the need for having a global approach to solving personal data protection problems, in the recent legal acts of the EU the issue of privacy at work has been highlighted as one of the main spheres of social life.

The directives setting common minimum requirements for the protection of employed person's privacy at work have been adopted. Furthermore, on May 25, 2018, Regulation 2016/679 — General Data Protection Regulation is to come into force. It is expected that this document will introduce more stringent rules for relevant information protection.

However, today, Ukrainian employers who have common business with companies from the EU Member States should be prepared for the new rules for personal data processing since the provisions of Regulation 2016/679 are applicable not only to employers established in the territory of the EU Member States, but also to non-EU companies that work with counterparties and/or clients from the EU Member States.

Analysis of the EU acts on data protection at work allows us to declare existence of sufficiently developed legal basis in this area. Undoubtedly, this contributes to the effective realization and protection of labour rights. Therefore, the study and the usage of the related positive experience of the EU is one of the criteria for measuring further development of the legal regulation of employee's personal data protection in Ukraine.

Keywords: employment, personal data, protection, labour law.

Introduction

Justification and legitimacy of control over employees by the employer are closely related to the issue of personal data processing in the field of hired labour. Slow and fragmentary reform of domestic labour legislation does not in any way contribute to effective protection of employees' personal data.

Adoption of the special Law of Ukraine *On Personal Data Protection*[2] *(* Law No. 2297-VI *)* has been a considerable step forward towards securing the right to privacy, including for the one for employees. At the same time, many legislative provisions are inefficient and cannot guarantee efficient protection of the relevant personal data.

[1] *PhD in Law, Associate Professor, Ivan Franko National University of Lviv, Faculty of Law, Department of Social Law. Scientific interests: labour rights in the system of human rights; labour rights protection; EU labour law; email: olena.dsl.ua@gmail.com.*

[2] Закон України «Про захист персональних даних» № 2297-VI [2010] at http://zakon2.rada.gov.ua/laws/show/2297-17

1. Regulatory basis for employee's personal data protection in Ukraine

Article 32 of the Constitution of Ukraine[3] proclaims the right of individuals to non-interference into his/her private life. Besides, the collection, storage, use, and dissemination of confidential information about a person without his/her consent shall not be permitted, except for the cases determined by law and only in the interests of national security, economic welfare, and human rights.

In order to specify human right secured by article 32 of the Constitution of Ukraine and to determine the mechanisms of its implementation on June 1, 2010 the Verkhovna Rada of Ukraine approved the Law of Ukraine *On Personal Data Protection* (Law No. 2297-VI). The Law regulates legal relations connected with personal data protection and processing and aims to protect individual's and citizen's fundamental rights and freedoms, in particular the right to non-interference into private life, because of personal data processing. It covers activity in personal data processing which is done fully or partially with application of automated devices as well as processing of personal data available in the card index file or designed to be included into the card index file using non-automated tools.

Numerous drawbacks and inaccuracies identified over the period of validity of the Law have led to numerous amendments made in it. Therefore, in fact, starting with January 1, 2014 its new version has been in effect. In particular, the list of the grounds for personal data processing was expanded, legislative grounds for counterparties' personal data were introduced, while the functions of controlling legislation enforcement in the field were assigned to the Verkhovna Rada's Commissioner for Human Rights.

Under the Law, personal data is the data or the integrity of data about an individual who has been identified or who can be specifically identified. It is important to stress that the applicable Ukrainian legislation does not set and cannot set a clear list of data about an individual, which makes up personal data. That is caused by it being impossible to envisage all possible cases of application of the relevant legislative provisions that may arise in the future, due to changes in technology, social, economic and other spheres of societal life.

At the same time, the Constitutional Court of Ukraine, while providing an official interpretation of parts 1 and 2 of article 32 of the Constitution of Ukraine, has pointed out that information on private and family life of an individual (his/her personal data) includes all the data or the integrity of data about the individual who has been identified or who can be specifically identified, viz.: nationality, education, family status, religious beliefs, health status, financial situation, address, data and place of birth, place of residence and stay, etc., data on personal property and non-property relations of this individual with other individuals, in particular, family members, as well as data about events and phenomena that were taking place or are taking place in the daily, intimate, companionship, professional, business and other spheres of the individual's life, but for the data connected to performance of the mandate of the individual holding an office related to state or local self-government bodies' functions performance[4].

In the field of hired labour, personal data stands for the data requested by the employer from the employee under article 24 of the Labour Code of Ukraine. In particular, concluding a labour contract a citizen shall present his passport or any other identity document, employment record, and in cases envisaged by the legislation, – also academic degree (specialty, qualifications), health status document, and other documents[5].

Due to this, the employee's personal data available in the documents (s)he presents at the stage of labour contract conclusion shall be processed by the employer under article 24 of the Labour Code of Ukraine and only for the sake of exercising his/her mandate as the employer in the field of legal relations arising between him/her and the employee under the labour contract.

The employer may also process the employee's data on racial or ethnic origin, political, religious or world outlook views, membership in political parties and trade unions, convictions to criminal penalty

[3] Конституція України № 254к/96-ВР [1996] at http://zakon2.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80

[4] Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України № 2-рп/2012 [2012] at http://zakon3.rada.gov.ua/laws/show/v002p710-12

[5] Кодекс законів про працю України № 322-VIII [1971] at http://zakon2.rada.gov.ua/laws/show/322-08

as well as the data related to health, sexual life, biometrical or genetic data. Since under the applicable legislation no overall ban for processing of this data is valid in case it is necessary for exercising the owner's rights and duties in the field of labour legal relations under the law. And the employer shall ensure appropriate protection of this data.

The employer's mandate as to personal data protection is determined by the general legislative requirements set for protection of that data. In particular, Ukraine's applicable legislation calls any action or integrity of actions like collection, registration, accumulation, storage, adjustment, modification, updating, use and dissemination (spread, use, transfer), de-personification, destruction of personal data, including through information (automated) systems, to be personal data processing. That is receipt of the data from the employee, set in the legislation as necessary for hiring, constitutes personal data collection. And processing of this data as well as its further systematizing shall be considered, respectively, data accumulation and storage. And personal data collection presupposes actions aimed at ensuring their integrity and appropriate mode of accessing it. Thus, the employer should restrict access to place of personal data storage, and in case of electronic bases — distinguish access of officials depending on their mandate and ensure information protection in information systems. The employer's duty is to take technical steps in order to prevent unauthorized access to personal data.

In employees' personal data processing the employer shall ensure its protection. With this in view, special internal documents must be approved locally, viz. a regulation on or a procedure of personal data protection. The employer also needs to get written non-disclosure commitments from employees having access to and processing personal data.

Under article 4 of the Law of Ukraine *On Personal Data Protection (* Law No. 2297-VI)*,* the following shall be subjects of relations connected with personal data: personal data subject; personal data owner; personal data holder; third party; the Commissioner of the Verkhovna Rada of Ukraine for Human Rights. In particular, hired employees shall be considered to be personal data subjects, while employer shall be the owner and holder of this data. Since each employer collects, processes, stores certain data about his/her employees for the sake of establishing, changing or terminating labour relations.

The employer as personal data owner may assign personal data holder with the task of processing this data under a contract concluded in writing. For instance, staff records are managed by a consulting firm with which the employer has concluded the respective contract. This consulting firm may be considered to be employees' personal data holder since it acts on behalf of the organization — personal data owner. And personal data holder may process it only for the purposes and within the scope set in the contract.

Companies, institutions and organizations of all ownership forms, state authorities or local self-government bodies, sole proprietors processing personal data under the law may be personal data owners or holders. Only a state-owned or municipal company managed by a state authority or a local self-government body may be the holder of personal data of which this state authority or this local self-government body is the owner (art. 4 of Law No. 2297-VI).

The status of third parties in the field of personal data protection is determined by article 2 of Law No. 2297- VI. This, in particular, may be any person to whom the owner or the holder has transferred personal data. In the field of hired labour Pension Fund bodies, military registration and enlistment offices, prosecution bodies and other entities which legally enquire about certain employee's personal data may be such third parties.

According to the general rule and in most cases personal data processing under part 5 of article 6, Law No. 2297-VI, shall be made with the consent of the personal data subject. Any documented, in particular, written voluntary will of the individual providing permission for his/her personal data processing in accordance with the stated goal of its processing shall be the personal data subject's consent.

Under the applicable legislation, though, the data about an individual may also be processed without his/her consent. For example, this may be done by the employer in relation to his/her employees' data. This statement is based on the legislative provision on the possibility to process the employee's personal data in case this is necessary to perform the employer's duty as a personal data owner, which is envisaged by the law. Labour legislation, in particular, makes the employer bound to keep primary

recording of employees, provide guarantees to disabled persons and employees with additional employment guarantees, provide additional leaves to employees with children, single mothers, etc. To perform those duties the employer should get the documents confirming the respective individual's status or confirming certain circumstances. And it is due to this legislative norm that employers have legal grounds for working with employee's personal data without getting any consent to its processing.

Provisions of paragraph 2 of part 1, article 11, Law No. 2297-VI constitute an additional ground for possible processing of employees' personal data without their consent. Under it, the data on personnel may be processed on the basis of permission granted under the law. Provisions of article 24 of the Labour Code of Ukraine are often considered to be this law. It should be noted that under this article the citizen must present the set documents while concluding his/her labour contract.

In case the employer decides to get the employee's consent to his/her personal data processing, the consent may be obtained in one of the following forms:

- a separate document signed by the employee;
- a respective electronic note;
- one of the provisions of the labour contract;
- any other form enabling to make a conclusion on the consent having been given (application writing, questionnaire filling-in, etc.).

It should be stressed that even if a person has given consent to processing of his/her data part of which, by its essence, is not necessary for achieving the processing goal set, such processing will be considered non-proportionate and will be classified as violation of personal data protection legislation.

Personal data processing must always be guided by its clear goal. Under part one of article 6, Law No. 2297-VI, the goal of personal data processing must be stated in laws, other regulatory legal acts, provisions, constituent or other documents regulating activity of the personal data owner as well as correspond to legislation on personal data protection.

For instance, employees' personal data is processed to ensure labour relations functioning. Then the respective personal data processing goal must be determined in a local employer's act under which work on personal data protection is arranged in the organization. This could be a regulation on or procedure of personal data processing and protection.

In practice, the term 'personal data processing goal' is used primarily during personal data collection. Thus, under article 12 of Law No. 2297-VI, personal data collection is a component of the process of its processing, envisaging actions in selection or systematization of data about the individual. And personal data subject must be informed about the personal data owner; the composition and content of the personal data collected; his/her rights determined by the legislation; the goal of personal data collection and the persons to who his/her personal data is transferred:

I. at the moment of personal data collection, in case personal data is collected from the personal data subject;
II. in other cases within thirty business days from the date of personal data collection.

For instance, when a person is hired, the employer actually collects his/her personal data. Thus, under article 12 of Law No. 2297-VI the employer shall inform the prospective employee that from the point of view of legislation on personal data protection (s)he will be considered the owner of that data; which personal data the employer will store and process; what his/her goal for doing this will be. At the same time, the employee should necessarily be familiarized with his/her rights in the field of personal data protection. Such rights are enshrined in article 8 of Law No. 2297-VI. In case personal data is transferred to third parties (the bank servicing employees salary payment; academic institution providing advanced training for employees; medical institution making medical examinations of employees, and others), the employee should also be informed thereof. That is, in spite of employer's exemption from the need to get the employee's permission for getting data about him/her in certain cases, the employer still has the duty to bring it to the employee's notice what data about him/her is processed, whom it may be transferred to, etc. Such notification may be arranged as a separate document, or a note can be made in the labour contract (employment application) saying that the employee has been informed about the goal of and

procedure of using his/her personal data under the procedure of its protection set by the company and applicable relevant legislation.

One of the components of personal data processing is its collection that presupposes actions in selection or systematization of the data about an individual and its inclusion into the personal data base. Under the applicable legislation, a personal data base is a named integrity of systematized personal data in an electronic form and/or in the form of personal data card index file. And card index file is any structured personal data available by the set criteria, regardless of whether this data is centralized, decentralized or distributed by functional or geographical principles.

It is important to realize that in spite of insufficiently rigid legal regulation of the respective relations, the employer is the owner of personal data of his/her employees and should ensure its protection following the procedure enshrined in the legislation. (S)he shall not be exempt from liability for violations in the field.

2. The EU rules on employees' personal data protection: what Ukrainian employers may expect

Employee's personal data protection in the European Union is currently secured under provisions of Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data as of October 24, 1995[6]. However, already on May 25, 2018 Regulation 2016/679 of the European Parliament and of the Council as of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, will come into effect[7]. This document is expected to introduce stricter rules for the respective information protection.

Art. 88 of the Regulation is dedicated to the issues of personal data protection in the context of employment. Under it, the EU Member States are granted authorities to set more clear rules for employees' personal data protection via approval of special national laws or approval of the respective provisions in collective agreements. In particular, rules of data processing for personnel hiring purposes, labour contract performance, organizational and management activity in the field of hired labour, ensuring unity and differentiation at workplace, ensuring occupational safety and health of employees at workplace, protection of the employer's or his/her counterparties' property as well as exercising individual and collective labour rights, including the right to terminate labour legal relations, can be specified in this way.

Establishment of the respective rules requires implementation of specific measures aimed at protection of human dignity, legal interests and fundamental rights of employees. And it is important to ensure the best possible transparency of personal data processing and transfer by both one employer, and a group of entities united with common business interests. Under Regulation 2016/679 special importance is attached to transparency and correspondence of the monitoring procedure at workplace. Each EU Member State should inform the competent bodies of the EU about introduction of the respective specifying rules in its territory by May 25, 2018 with no delays.

The following innovations come into the focus of attention of employers as people processing personal data. Processing of employees' personal data, as a privacy component, shall be made by the employer only in case of a real need for that and only in case sufficient legal grounds for that are available. The respective processing must be fair and transparent in relation to employees as well as proportionate to the information collection goal. Since subordination of the employee to the employer and actual employee's dependence on the employer who asks for consent to personal data processing calls into question the correspondence of the exterior form of the employee's will expression to his/her real inner will to give consent to the respective information processing. That is why the circumstances under which

[6] Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281, 23.11.1995, pp. 31–50 at http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31995L0046.

[7] Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119, 4.5.2016, pp. 1–88 at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG.

the employee has granted consent to processing of the data about him/her should always be taken into account.

Taking the above into account, the employer's activity related to collection and processing of the employee's personal data which has been made public by him/her via social media will be considered illegal. For the employer to process the respective personal data a legal ground like legal interest, for example, will be required. In this context the employer, before checking the person's profile in one of the social media must make sure whether the highlighted information is of a professional nature or the one related to the individual's private life. Otherwise, legal permissibility of the respective activity may be called into question and regarded as unauthorized intervention into the employee's private life.

Besides that, collection of information about the employee shall be limited to the data which is necessary and expedient from the point of view of the scope of his/her labour rights and duties.

It should be stressed that information received by the employer about the person looking for a job must be destroyed the moment it becomes clear that the person will not be asked to take the vacant position or the person refuses to take the position offered.

Taking into account the fact that verification of the data about the employee can be arranged by the employer almost on a permanent basis since advanced technologies ensure permanent access to employees' profiles in social media, a rule is introduced under which employees' personal data verification cannot be considered justified if not arranged on general grounds. And employers shall restrain from introduction of the requirement to provide them with access to the employee's profile in social media where the individual makes information about him/her public.

Regulation 2016/679, when it comes into effect, will make personal data base owners bound to take special steps to follow the procedure of the respective information protection. In particular, personal data base owners will have to appoint a specially authorized person in charge of personal data processing, under some conditions. Besides that, the rules of giving and withdrawal of the employee's consent to his/her personal data protection as well as the rules of the employee notification about his/her personal data processing will change. Also, a mechanism of exercising 'the right to be forgotten', for cases when an employee demands that, is introduced.

The consequences of enactment of Regulation 2016/679 in the field of employees' personal data protection can be assessed only some years after it comes into effect. However, already now Ukrainian employers working with companies from the EU Member States must start getting ready for the new rules of personal data processing. Since provisions of Regulation 2016/679 are subject to application not only in relation to employers in the territory of the EU Member States but also in relation to companies not from the EU Member States working with counteragents and/clients from the EU Member States. Therefore, if a Ukrainian company is interested in cooperation with an EU company, it will have to comply with the respective provisions. Besides that, the domestic company must care for its own positive image of a reliable partner for an EU company. Since European companies will not run the risk of working with companies that are not diligent in performance of their duties related to personal data protection in Ukraine.

We consider it to be an indirect effect of the acquis communautaire on Ukrainian legal regulation of the respective relations, which will definitely promote an improved mechanism of employees' personal data protection in Ukraine.

Conclusions

The European rules and principles of employees' personal data protection are mainly reflected in the provisions of the Law of Ukraine *On Personal Data Protection* (Law No. 2297-VI). However, Ukraine needs to envisage additional guarantees of a binding obligation to get the employee's consent to his/her personal data protection, as well as of the duty to notify the employee about the data processing and the goal of such processing. With this in view, the need to develop and approve a number of respective acts of the national legislation that will be European by spirit and by letter is pressing.

Bibliography

1. Закон України «Про захист персональних даних» № 2297-VI [2010] at http://zakon2.rada.gov.ua/laws/show/2297-17.
2. Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281, 23.11.1995, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31995L0046.
3. Конституція України № 254к/96-ВР [1996] at http://zakon2.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.
4. Кодекс законів про працю України № 322-VIII [1971] at http://zakon2.rada.gov.ua/laws/show/322-08.
5. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України № 2-рп/2012 [2012] at http://zakon3.rada.gov.ua/laws/show/v002p710-12.
6. Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119, 4.5.2016, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG.

"ALEXA, WHERE IS MY PRIVATE DATA?" – UNANSWERED LEGAL AND ETHICAL QUESTIONS REGARDING PROTECTION AND SHARING OF PRIVATE DATA COLLECTED AND STORED BY VIRTUAL ASSISTANTS

Dr. Cătălin Stănescu[1]
Nataliia Ievchuk[2]

Abstract

Virtual assistants are a constant presence in our day to day life. Fast technological advancements have increased their usage and capabilities. Depending on the provider, these assistants now know our daily schedule, plan our doctor appointments, do our shopping, play our music lists, control our smart devices/houses, make phone-calls and record our conversations. However, the entire amount of private data is collected and stored on cloud, on private companies' servers, over which users of virtual assistants do not have adequate control. At the same time, the question of ownership over collected private data is still debated upon, while security of private data is entirely handled by the companies, thus putting users in considerable risk.

The paper's starts from issues related to the collection and storage of personal communications through virtual assistants, as emphasized by the recent "Bates" case in the US, where the police sought to seize information captured by an Amazon Echo device in connection to an alleged crime. Left without a decision due to the criminal investigation being dropped, the case unveils significant legal and ethical questions that are relevant also for the EU, regarding ownership of collected data, third party access to it (with or without a court order) and the usage of such data in relation to protection of public interests (such as prevention or solving of a crime).

The paper further assesses the compatibility of virtual assistants cloud services – such as Alexa (Amazon), Siri (Apple), Cortana (Microsoft) or Home (Google) – with personal data protection requirements imposed in the European Union (EU). Based on the terms and conditions applicable to data collected and stored on cloud by virtual assistants coupled with a discussion of the problems raised by the US "Bates' Echo" case, the paper argues that although in appearance such services protect private data, there are still unanswered concerns regarding non-customer third parties.

Keywords: private data, virtual assistants, cloud services

Introduction

Virtual assistants are a constant presence in our day to day life. Fast technological advancements have increased their usage and capabilities. Depending on the provider, these assistants now know our daily schedule, plan our doctor appointments, do our shopping, play our music lists, control our smart devices/houses, place our phone-calls and record our conversations. However, the entire amount of private data is collected and stored on cloud, on private companies' servers, many located overseas, over which users of virtual assistants do not have adequate control. At the same time, while the question of ownership over collected private data is still debated upon, the security of private data is entirely handled by the companies, thus putting users in considerable risk.

[1] Postdoc at University of Copenhagen, LLM.
[2] Legal Counsel at Maersk Container Industry A/S, LL.M.

The paper's starts from issues related to the collection and storage of personal communications through virtual assistants, as emphasized by the recent Bates case in the US, where the police sought to seize information captured by an Amazon Echo device in connection to an alleged crime. It further assesses the compatibility of virtual assistants (VAs) cloud services – taking as example Amazon's Alexa – with personal data protection requirements imposed in the European Union (EU).

It provides a topical analysis of three aspects: the *type* of data collected, the potential origin of the *duty* to protect, and the *sharing* of collected data, by juxtaposing the contractual terms of Amazon with the applicable EU legal provisions. It closes with several conclusions regarding the apparent compliance of cloud services and the potential unresolved issues thereof.

The Bates Case – The Unanswered Question

On 4th of December 2015 a Search Warrant was served on Amazon by the Bentonville Police Department in connection to an alleged murder committed by an Amazon customer, James Bates. As Amazon did not fully comply with it, the police subsequently served a Search Warrant Extension on 29th of January 2016. Once again, Amazon did not supply all of what was requested by both Search Warrants: the account holder information for James Bates and his purchase history.[3]

The Search Warrant served on Amazon was based on the police's belief that Amazon.com was "in possession of records related to a homicide investigation".[4] The records sought by the police consisted in

> "electronic data in the form of *audio recordings, transcribed records*, or other text records related to communications and transactions between an Amazon Echo device […] that was located at James A. Bates' residence […] and *Amazon.com's servers* and other computer hardware maintained by Amazon.com in another location, […], *which are stored and maintained by Amazon.com*,"[5] (emphasis added)

covering the night of the potential murder. In addition, the police requested the purchase and billing history for the Amazon Echo device, the IP address associated with the device utilized by device, all information regarding James Bates's subscription with Amazon, authorized users, activation and termination dates of each associated device as well as all customer service and accounts notes, "which is evidence of the crime".[6]

What happened was that on the 22nd of November 2015 police started an investigation involving James Bates, after one of his friends was found deceased in his hot tub. The full details of the murder are not relevant for the purposes of this paper, but they involved a football game, a lot of drinking the night before the discovery and a body floating in the hot tub. The victim's body was discovered the morning after, by James Bates, who called the police. Since the detectives present at the scene identified signs of struggle, the death was ruled a homicide.

As of the 3rd of December 2015, the court approved a new Search Warrant for James Bates' residence, "specifically for the search and seizure of electronic devices capable of storing and transmitting any form of data that could be related to the investigation."[7] Based on the search, the police discovered an Amazon Echo device in the kitchen. It soon became apparent that those present in the house during the night have placed verbal commands to Alexa, asking it to play certain music.

The discovery of the virtual assistant belonging to the suspect gave hopes to the police that *they might be able to retrieve data that could help solve the homicide investigation and that data could come*

[3] See Search Warrant Return in Circuit Court of Benton County, Arkansas, of 18th of April 2016 (Search Warrant), available online at: https://www.scribd.com/document/335167614/Warrant-served-to-Amazon-re-Echo-data, last accessed on 22.04.2018.
[4] See Extension for Search Warrant in the Benton County Circuit Court, of 29th of January 2016 (Extension for Search Warrant), available online at: https://www.scribd.com/document/335167614/Warrant-served-to-Amazon-re-Echo-data, last accessed on 22.04.2018.
[5] See Extension of Search Warrant.
[6] For a full list of the data required by the police, see *Ibid*.
[7] *Ibid*.

from Amazon.com. Based on what the Extension for the Search Warrant retrieved from Amazon.com's website:

> "[…] Echo is equipped with an array of seven microphones, equipped with sensors that use beam-forming technology to hear users from any direction. With enhanced noise cancellation, Echo can hear users ask a question, even while the device is playing music or if there is background noise. Echo then […] lights up to stream what the user says to their cloud service, where Amazon leverages the Alexa Voice Service to recognize and respond to the user's request."[8]

However, this is not entirely the reason why the police thought the device and the retained data might be of use to them. What they knew was that "[t]he Amazon Echo device is *constantly listening* for the "wake" command of "Alexa" or "Amazon", *and records any command, inquiry, or verbal gesture given after that point, or possibly at all times* without the "wake word" being issued, *which is uploaded to Amazon.com's servers at a remote location*"[9]. Hence, it had reason to believe that "these records *are retained* by Amazon.com and that *they are evidence* related to the case"[10] (emphasis added).

As stated above, Amazon did not comply with the search warrant in full,[11] although representations were made to the police that it was in the possession of the requested data.[12] Moreover, it moved to have the Search Warrant quashed in court.[11] In invoked arguments based on First Amendment and on privacy grounds[13], although the trial might have had more with Amazon's business interest in sending a message to its Alexa users.

In the end, James Bates voluntarily agreed to have the recordings handed over to the police, and Amazon complied[13], thus, leaving the legal battle between the police and Amazon without a judicial solution. Unanswered remains also the overflowing question whether state authorities or law enforcement officers could gain access to personal data collected and stored by third parties, straight from such third parties? If yes, then whom and how is going to protect and vindicate the rights and interests of the person whose data is requested?

The Bates case indicates that such role might in fact be assumed by the third party. Amazon's official position was adamant towards protecting the customer's privacy: "Given the important First Amendment and privacy implications at stake, the warrant should be quashed unless the Court finds that the State has met its heightened burden for compelled production of such materials"[14] otherwise the company "objects to overbroad or otherwise inappropriate demands as a matter of course."[15] Thus, Amazon argued that both Echo users' voice commands and the Alexa Voice Response are protected by the right to free speech, as both could contain details that would reveal much about the users and their

---

[8] *Ibid*.
[9] See Extension for Search Warrant.
[10] *Ibid*.
[11] Amazon handed over a record of transactions, however it did not submit Bates' audio data. See: Brain Heater – After pushing back, Amazon hands over Echo data in Arkansas murder case, 7th of March 2017, available online at https://techcrunch.com/2017/03/07/amazon-echo-murder/, last accessed on 22.04.2018.
[12] Extension for Search Warrant in the Benton County Circuit Court, of 29th of January 2016, available online at: https://www.scribd.com/document/335167614/Warrant-served-to-Amazon-re-Echo-data, last accessed on 22.04.2018. [11] The document is accessible online at: https://www.documentcloud.org/documents/3473747-Amazon-MemorandumSeeking-to-Quash-Echo-Search.html#document/p1, last accessed on 22.04.2018.
[13] Tim Johnson – Can Police Seize Info from Connected Devices? 27th of February 2017, available online at: http://www.govtech.com/public-safety/Can-Police-Seize-Info-from-Connected-Devices.html, last accessed on 22.04.2018. [13] Eliott C. McLaughlin – Suspect Oks Amazon to hand over Echo recordings in murder case, CNN, 26th of April 2017, available online at: https://edition.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murdercase/index.html, last accessed on 22.04.2018.
[14] *Ibid*.
[15] *Ibid*.

interests, for which reason they should be protected from the government.[16] It failed to answer, though, why a search warrant did not constitute a valid legal demand.[17]

The Amazon.com-police dispute in the Bates case also brings forward several concerns and unanswered questions regarding privacy, the main one being how companies protect the private data of their customers. It is worth noticing that in trying to protect its customer's audio recordings, Amazon invoked a Constitutional defense, which in its turn protects free-speech, the matter of privacy being only secondary. At the same time, Amazon.com invoked not only its customer's right to free speech, but also its own, thus asserting joint interests.

Amazon Echo is the 'unlucky' subject in the Bates example. However, Alexa is not the only private assistant out there. Google Home, Apple's Siri, Microsoft's Cortana, Ivee, Homey or Cubic, to name a few, qualify as 'always-on' devices, and thus pose similar questions and face similar challenges. Does recording of communications of consumers in their homes constitute unlawful surveillance under relevant wiretap laws? Do 'always-on' devices affect the privacy rights of consumers?[18] Is the storage of communications on the device under the control of the consumer or is it transferred to a third party? Under what circumstances these communications may be disclosed to others? Have consumers given meaningful consent to the interception and recording of their communications? Does that consent include others in the home? Although stemming from the United States, these questions are relevant to all EU jurisdictions, even (or especially) in the light of the GDPR's coming into force on 25th of May 2018.

Answering all the above would go beyond the purposes and the limits of this paper. Thus, based on the coordinates set by the Bates case, we will first deal with the type of private data collected by Vas after which we will focus on two aspects from a GDPR perspective: **a)** the duty to protect private data, **b)** the circumstances under which the police can obtain access to that information.

Aftermath of Bates: Data Collected by VAs and the 'Duty' to Protect It

Before delving into the issue of data sharing it is important to establish, on the one hand, the kind of information collected and stored by VAs, how it is collected and the purpose behind it, in order to assess the legitimacy of the police's request to gain access to it, and, on the other hand, the origin of the self-imposed duty to protect, undertaken by Amazon in the Bates case. Answers are to be found mainly in the standard terms on which the relationship between Amazon and its customers is based.

The Type of Private Data Collected by VAs

According to its Privacy Notice, Amazon stores any type of information that the customer has given it, notwithstanding whether it was given consciously or not. "We *receive and store any information* you enter on our website or *give us in any other way*"[19] (emphasis added). That is not all. Amazon states that it also receives and stores "*certain type of information*, whenever you interact with us".[20] The example

[16] For details: Thomas Fox-Brewster – Amazon Argues Alexa Speech Protected By First Amendment in Murder Trial Fight, Forbes, 23rd of February 2017, available online at: https://www.forbes.com/sites/thomasbrewster/2017/02/23/amazon-echoalexa-murder-trial-first-amendment-rights/#6df57f495d81, last accessed on 22.04.2018.

[17] Eliott C. McLaughlin, Keith Allen – Alexa, can you help with this murder case? CNN, 29th of December 2016, available online at: https://edition.cnn.com/2016/12/28/tech/amazon-echo-alexa-bentonville-arkansas-murder-case-trnd/index.html, last accessed on 22.04.2018.

[18] See The Electronic Privacy Information Center's Letter to the Federal Trade Commission of 10th of July 2015, urging for an investigation of 'always on' technologies including those used by Google, Samsung, Microsoft, Amazon and others, available on line at https://epic.org/privacy/internet/ftc/EPIC-Letter-FTC-AG-Always-On.pdf, last accessed on 22.04.2018. With respect to private assistants, the letter nominates Alexa, as an "always on voice recognition software" and states that Amazon "has made the Alexa voice recognition software available to third party developers to use on their own internet-connected devices". The problem appears to be that "Amazon has not disclosed the parameters of the company's data collection practices" nor "the extent to which the company will have access to the data collected by […] third party devices.

[19] Privacy Notice, Information You Give Us, available online at: https://www.amazon.co.uk/gp/help/customer/display.html?nodeId=201909010, last accessed on 24.04.2018. [20] Id at Automatic Information.

provided by the company refers to cookies. Nevertheless, in the category of automatic information received and stored one may also enter any background discussions recorded by Alexa while receiving commands.

Additional information stems from the definitions contained in Alexa Terms of Use. Of interest to our paper is "Alexa Interactions" defined as "all information related to your use of Alexa and Alexa Enabled Products, including your voice and other inputs, responses provided to you through Alexa, information we receive in connection with Third Party Services and Auxiliary Products you use, and information and content you provide or receive through the Alexa App."[20]

These interactions are further detailed upon where the Terms state that "you control Alexa with your voice. Alexa streams audio to the cloud when you interact with Alexa. Alexa *processes and retains* your Alexa interactions, such as your *voice inputs,* music playlists and your to-do and shopping lists, *in the cloud* to provide and improve our services"[21] (emphasis added). But there is more to it. According to the Alexa Q&A list, "the audio stream includes a fraction of a second of audio before the wake word."[22] This is rather puzzling. The device is conspicuously always listening, yet not always recording. But if it is not always recording, then how can it record the fraction of second, before the user has said the wake word?

If the above terms are dedicated to the use of Alexa, Amazon also provides a set of terms applicable to all its devices, including Alexa.[23] The relevant provision is the one referring to voice services.[24] Some Amazon devices have features enabling customers to access Alexa voice services or allowing the customer to use its voice to perform certain tasks. The company states that "[w]hen [one] use[s] voice services, we may process [its] voice input and other information in the cloud", allegedly for improving the response or to improve the experience of Amazon services. Notwithstanding the legitimacy of such reason, it is obvious that audio recordings may, depending on the various circumstances, retain and give Amazon access to private data belonging to others than the Alexa user. Hence, if we accept an implied delegation of duties from customers to the company, it is unclear whether such delegation covers also third parties present at some point in time near the device.

The audio recordings requested by the Police in the Bates case qualify as both "Alexa Interactions" and automatic data and are part of the type of information stored. This is what the police was after when it served the Search Warrant on Amazon. Based on the above, the police were not wrong in their assumption and hope that the Alexa device might have picked up something of use to the murder investigation, when the persons present in Bates's house placed commands to Alexa. Nevertheless, automatic information may be not only private and sensitive, but may involve other parties, which did not consent to the Alexa Terms of Use or Amazon's Privacy Notice. Hence the question whether simple presence near an Alexa device or placing commands to it suffice to retrieve or store other persons' private data and on what basis is that data processed, stored or potentially shared with third parties is relevant and remains unanswered.

A Duty to Protect and Business Interests

In its filing to quash the Search Warrant, Amazon emphasized its *duty* towards its customers and the latter's *expectation* to have their personal data protected by the product and service provider.[25] This would imply that a delegation of responsibility regarding data protection had taken place, from the

[20] *Ibid*.

[21] Alexa Terms of Use, at point 1.3. Alexa Interactions, available online at: https://www.amazon.co.uk/gp/help/customer/display.html?nodeId=201809740, last accessed on 24.04.2018.

[22] Alexa and Alexa Device FAQs, Question 2, How do I know when Amazon Echo, Echo Plus or Echo Dot are streaming my voice to the Cloud? available online at https://www.amazon.co.uk/gp/help/customer/display.html?nodeId=201602230, last accessed on 24.04.2018.

[23] Amazon Device Terms of Use, Definition of "Amazon Device, available online at: https://www.amazon.co.uk/gp/help/customer/display.html?nodeId=202002080, last accessed on 24.04.2018.

[24] *Ibid* at point 1, letter c).

[25] Accessible online at: https://www.documentcloud.org/documents/3473747-Amazon-Memorandum-Seeking-to-QuashEcho-Search.html#document/p1, last accessed on 22.04.2018 [27] Alexa Terms of Use.

customer to the company. However, the extent of the delegation, the standard of care in exercising the duty to protect private data of customers as well as the coverage of other ancillary parties whose data might be stored or processed by the company remain unclear.

The delegation appears to have a contractual origin, as it stems from the applicable Terms and Conditions and the ancillary documents that set the basis for the legal relationship between Alexa users and Amazon. From the outset Amazon establishes that by using Alexa customers are bound by its terms and conditions. Unacceptance simply means that one may not use Alexa.[27] Hence, it is not a negotiated agreement, but a standard contract imposed on all users. Moreover, Amazon retains the unilateral right to amend the terms at its own discretion by "posting the revised terms on the Amazon.co.uk website",[26] thus making it the customers' sole responsibility to keep informed with any changes in their legal relationship with Amazon. These aspects may have legal implications,[27] especially regarding the validity of the contract under the UCPD and, subsequently, regarding the validity consent. Moreover, as these terms are unilaterally imposed by the company, besides the standards set by the law there would be a significant level of *self regulation* from the side of the company, which automatically raises concerns regarding validity and enforcement by users of the self-adopted standards.

The previous paragraphs seem to indicate that the matter of data protection lies where self-regulation meets corporate interests. As the following section emphasizes, more answers regarding the sharing of private data with state agencies should come from both the applicable terms and conditions that govern the contractual relationship between company and VA users, and from data privacy laws, governing the rights and obligations of all parties involved in providing and using VA services.

The Sharing of Private Data Collected by VAs

In the US, the Bates case revealed that new data sources, which were not known ten years ago, go somewhat unregulated by policies or laws that were adopted in the 1980s and focused on telecommunications companies' phone records. This urged for updating policies that balance privacy and law enforcement activities.[28] Put differently, situations as the one in the Bates case reveal the *re-active* attitude of legislators, who fail to keep up with the rapid advancement of technology.

In the EU however, the General Data Protection Regulation (GDPR) was adopted with an eye to the past and one to the future, as its aim is to ensure adequate private data protection as a fundamental human right, notwithstanding the future developments of technology. The ensuing analysis covers the conditions under which private data can be shared or not with law enforcement bodies, as they appear from Amazon's applicable Terms and Conditions,[29] and juxtaposes them to the EU legal framework to verify their compatibility with the law.

Amazon's Terms and Conditions

With respect to the sharing of information, Amazon informs its EU customers that their "account and other personal information" will be released when the company "believe[s] is appropriate to comply with the law, enforce or apply [their] Conditions of Use and other agreements."[30] *Prima facie*, this provision

[26] Id at point 3.3. Changes to Alexa; Amendments. A similar provision is to be found in the Device Terms of Use, point 3, letter c).

[27] For issues stemming from the standard Terms and Conditions of Amazon, see also: S. LAW, AT THE CROSSROADS OF CONSUMER PROTECTION, DATA PROTECTION AND PRIVATE INTERNATIONAL LAW: SOME REMARKS ON VEREIN FÜR KONSUMENTENINFORMATION V AMAZON EU § 42 (2017), pp 765-766.

[28] Mythili Sampathkumar – Amazon Echo could become key witness in murder investigation after data turned over to police, 9th of March 2017, available online at: https://www.independent.co.uk/news/world/americas/amazon-echo-murderinvestigation-data-police-a7621261.html, last accessed on 22.04.2018.

[29] Given this section's focus on European law, the Terms and Conditions are those applicable to Amazon Media EU S.a.r.l. and Amazon.co.uk's Privacy Notice and Conditions of Use

[30] Privacy Notice, Protection of Amazon.co.uk and Others, available online at: https://www.amazon.co.uk/gp/help/customer/display.html?nodeId=201909010, last accessed on 24.04.2018.

appears to be in compliance with legal provisions governing the use and protection of private data in the EU.

However, the title of the section – Protection of Amazon.co.uk and Others – should raise concerns. The first is the degree of control retained by Amazon, which grants itself by unilateral contract total discretion in sharing the customers' data. The second, is the (self)-entrusting of Amazon with legal assessment of third party requests and with self-help rights in case of vindication of its own interests or claims. The third, stems from the purpose of such total discretion, which is self-preservation and not necessarily the customers' best interest. Here, as emphasized in Bates, self-preservation may be equated to business interest, which could result in attempts to protect private data in order to avoid losing customers. The fourth, relates to the vagueness of terms: to what specific law is Amazon referring when it speaks of compliance? Is it criminal, consumer or data protection law? And from which member state? In this aspect, the arbitration clause[31] imposed currently on the Amazon consumers may also cause additional hardship to aggrieved customers.

Another concern refers to the issue of consent, which, based on the following provision of the Privacy Notice, appears to have been divided in two. One the one hand, there is *an implied, total consent* that is granted to Amazon under the Protection of Amazon clause. On the other hand, there is *an express, limited consent* that might be required in "*other"* circumstances.[32] In other words, Amazon has full discretion of releasing and sharing the private data of the customer, whenever its assessment of the law or its (legal or business) interests commands it. Hence, in a case similar to Bates, Amazon could choose either to share or not to share the customer's data with the police, whichever it may deem fit. One should notice though that such discretion refers solely to Amazon's contractual relationship with the customer, and not to its obligations stemming from the law and its relationship with law enforcement or state agencies. Notwithstanding its origin and potential legal boundaries, such discretion would have unforeseen circumstances with regard to the private data of non-customers, that were recorded by Amazon devices.

Given all the above and the power retained by Amazon, not only in handling, but also (self)-regulating the use and sharing of customers' private data, the relationship between customers and Amazon is one mainly based on trust and lacking in clear standards and possibilities of enforcement. Nevertheless, trust itself does not suffice, given that customers are limited in their possibility of binding Amazon into not disclosing their private data. This appears to be at the core of Amazon's Privacy Notice, where the Preamble states that Amazon appreciates the customers' trust in its careful and sensible using and sharing of private information.[35] The importance of the Notice cannot be overstated given that it "applies to all information that we have about you and your account."[33]

Perhaps the most important issue posed by the Bates case is that of sharing the collected private data, specifically with state bodies and law enforcement. The European terms and conditions appear to leave the issue at the discretion of Amazon, unless applicable legal provisions dictate otherwise. Hence, the following subsection is dedicated to the law governing the sharing of private data with law enforcement bodies in the EU.

The Law

The picture regarding sharing private data with state bodies and law enforcement would not be complete without an analysis of the EU legal framework regarding data protection. According to the EU rules any operation on personal data, including its collection, recording, structuring, storage, disclosure, deletion and others, is considered to be a processing of personal data.[34] The upcoming GDPR states that

[31] Privacy Notice.

[32] Privacy Notice at With Your Consent. The provision reads as follows: "Other than set out above [Protection of Amazon.co.uk and Others] you will receive notice when information about you might go to third parties and you will have an opportunity to choose not to share the information."[35] Privacy Notice.

[33] *Ibid.* at Conditions of Use, Notices & Revisions.

[34] Art. 4 of GDPR. [38] Art. 5 of GDPR.

personal data shall be processed in compliance with six principles related to processing of personal data[38] where lawful processing is one of them.

To be lawful, processing shall be based on a legitimate ground, such as a consent, performance of a contract, legal obligation of a controller, performance of a task in legal interest or legitimate interests of a controller.[35] However, Member State legislators may restrict the scope of rights of a data subject[40], obligation of communication of a data breach[36], or application of principles for processing[42], provided such a restriction "respects the essence of the fundamental rights and freedoms and is necessary and proportionate measure in a democratic society to safeguard"[37], among others, the prevention, investigation, detection or prosecution of criminal offences and others.[44]

For example, it is worth having a look at the approach of the UK legislator. In the UK law the corresponding provision to the GDPR one mentioned above can be found in the Data Protection Act (DPA)[38]. According to the DPA, if a disclosure of personal data is required for the prevention or detection of crime and if application of "non-disclosure provisions" to such disclosure will likely prejudice a prevention or detection of such investigation, such personal data shall be exempt from the non-disclosure provisions.[39] Non-disclosure provisions mean, on the one hand, principles relating to processing of data[40], and, on the other hand, certain rights of a data subject (right to prevent processing, rectification, blocking, erasure and destruction).[41]

Even relying on such exemption, the data controller still needs to have a legal ground for disclosure. In a case similar to Bates, it could be "the administration of justice, functions conferred on any person by or under enactment, or the functions of a government department"[42].

Thus, as a disclosure of personal information is exempt from the rest of the principles relating to processing of personal data (provided there is a risk of prejudice), including non-processing for incompatible purposes, data controller may disclose data based on another purpose (crime detection and prevention) than it was initially collected for, without being in breach of the data protection legislation.[43]

In this case, however, data controller is not obliged to disclose information, but only may decide to do it. The decision shall be made taking into consideration the circumstances of each case, whether the requested data is needed for the crime prevention or detection, and whether non-disclosure will prejudice the investigation.[44] Therefore, in case of a request by the police, it is solely for a data controller to decide whether to disclose personal data of data subjects to investigating authorities or not.

A subsequent question is whether the situation would change if, instead of a request, the data controller received a court order obliging it to provide access to the personal data under its control. In UK law, a similar exemption from the non-disclosure provisions applies if the disclosure is required by a rule of law, any enactment or by the order of court.[45] However, in this situation the data controller is not in a position to choose whether to comply with a court order or not. It must comply. And even in case of any objections by the data subject as to the disclosure of his/her personal data, the legal obligation prevails.[46]

---

[35] Additional grounds are set up for processing of sensitive data (see Art. 9 GDPR) [40] Arts. 12-22 of GDPR.
[36] Art. 34 of GDPR. [42] Art. 5 of GDPR.
[37] Art. 23 of GDPR. [44] Art. 23 of GDPR.
[38] See Section 29 of Data Protection Act 1998 (DPA). It will be replaced by a new Data Protection Bill 2017 (Bill 2017) to be adopted in UK as a complementary law to GDPR, available at https://publications.parliament.uk/pa/bills/cbill/20172019/0153/18153.pdf (under revision, not final version).
[39] Section 29(3) of DPA.
[40] In particular lawful and fair processing principle, except to the extent processing is based on a legitimate ground and other principles set out in subsections (b) to (e) of Art. 5 of GDPR
[41] Section 27(4) DPA. For analogues provisions in the Bill 2017 see Sec. 1 of Part 1 of Sch.
[42] Sch. 2 (5) or Sch. 3 (7) DPA in case of sensitive data processing; Sec. 46 of ICO Guidance "Using the crime and taxation exemptions" (s29), 20152605, Version: 1) available at: https://ico.org.uk/media/for-organisations/documents/1594/section-.pdf (ICO Guidance 2015). Equivalent in GDPR is Art. 6 (e) "performance of task carried out in the public interest". For analogues provisions in the Bill 2017 see Art. 8.
[43] Art. 27, 29(3) DPA; sec. 47 ICO Guidance 2015. For analogues provisions in the Bill 2017 see Sec. 1 and 2 of Part 1 of Schedule 2.
[44] Sec. 35-36 ICO Guidance 2015.
[45] Sec. 35 DPA. For analogues provisions in the Bill 2017 see Sec. 5 of Part 1 of Schedule 2.
[46] ICO Online Guide to DPA, available at https://ico.org.uk/for-organisations/guide-to-data-protection/exemptions/

This is in accordance with the provisions of the Law Enforcement Directive,[47] which governs data privacy issues in connection to investigation or prevention of a crime. The purpose of this Directive is outlined in Recital 27:

> "for the prevention, investigation and prosecution of criminal offences, it is necessary for competent authorities to process personal data collected in the context of the prevention, investigation, detection or prosecution of specific criminal offences beyond that context in order to develop an understanding of criminal activities and to make links between different criminal offences detected"[48].

As a rule, an individual shall have a right of access to the information collected about him/her by any data controller. It is also valid in case of investigations carried out by authorities, but with a possibility of limitation. The Directive authorizes Member States to enact legislation "delaying, restricting or omitting the information"[49] to individuals – data subjects, provided such measure is a "necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural persons concerned"[50]. The purpose of the measure is to ensure that investigation, detection and prosecution of crimes is not obstructed.

To conclude, in case of a court order, the data controller bears a duty to provide access to the personal data under its control, and neither customer's objection, nor business or other interests of the data controller, can preclude data sharing. Moreover, once the private data is in the possession of law enforcement or state bodies, the access of the data subject may be restricted for the purpose of safeguarding the investigation. Thus, it would be safe to assume that a case between Amazon and the police, similar to the dispute related to Bates, is unlikely to occur in the EU.

Conclusions: GDPR Meets VAs – To Be or Not to Be Compliant

In the US, the Bates case revealed, once more, that new data sources that were not known ten years ago go somewhat unregulated by policies or laws that were adopted in the 1980s and focused on telecommunications companies' phone records. This urged for updating policies that balance privacy and law enforcement activities.[51] Put differently, situations as the one in the Bates case reveal the *re-active* attitude of legislators, who fail to keep up with the rapid advancement of technology. In the EU however, the GDPR was adopted with an eye to the past and one to the future, as its aim is to ensure adequate private data protection as a fundamental human right, notwithstanding the future developments of technology. It will be for the upcoming years and challenges to prove whether the GDPR is the appropriate tool and can serve as an example for other jurisdictions.

The paper assessed the compatibility VA cloud services with personal data protection requirements imposed in the EU. It found that the amount of data collected by VAs is significant, which proves both the importance of the topic and the need to properly address the issue of data protection collected and stored via cloud services. It also emphasized the dilemma of data protection lying at the juncture of contractual duties, legal obligations, self-regulation, and business interests.

Regarding the sharing of private data collected from customers Amazon's terms and conditions appear to be compliant with the upcoming GDPR. We therefore conclude that a legal battle with law enforcement authorities, similar to the Bates case in the US, is either unlikely to occur in the EU, or unlikely to succeed.

---

[47] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, applicable as of May 6, 2018 (Law Enforcement Directive).

[48] Recital 27 Law Enforcement Directive.

[49] Recital 44 Law Enforcement Directive.

[50] Recital 44 Law Enforcement Directive.

[51] Mythili Sampathkumar – Amazon Echo could become key witness in murder investigation after data turned over to police, 9th of March 2017, available online at: https://www.independent.co.uk/news/world/americas/amazon-echo-murderinvestigation-data-police-a7621261.html, last accessed on 22.04.2018.

Nevertheless, both the Bates case and the provisions of the standard terms and conditions of Amazon, leave open a number of questions and concerns for future research or court decisions. Among them, the most important appears to be the one dealing with protection of data collected by VAs from non-customer third parties while in the vicinity of such devices. However, how and if such private data is adequately protected is a matter to be dealt with in another article.

COUNTER-TERRORISM MEASURES INTERFERING WITH PRIVACY: RECENT *ADD-ONS* TO COMPROMISING WAR ON TERROR

Steponėnaitė Viltė Kristina[52]

Abstract

High number of measures have been introduced to fight (prevent) terrorism on the international and regional levels over the last few decades, including individual restrictive measures such as travel ban and asset freeze and various instruments resulting in broad surveillance and retention of personal data. Both international and European Union measures proved to be interfering with fundamental human rights such as right to fair trial and privacy rights and resulting in serious violations. Rather quickly developing war on terror led to creation of neo-democracies where some liberties are rather illusionary than guaranteed. Both international and European institutions, including European judiciary, are still struggling to find a proper balance. Besides, it may be also reasonably argued that people are forced to give up their rights without actually gaining up security.

The paper focuses on particular counterterrorism measures related to mass digital surveillance and data retention, i. e. the ones interfering with privacy rights, in the end also portraying these measures in a broader context, demonstrating that failure to ensure fundamental human rights is common to various counter-terrorism policies. In is being concluded that, as long as there is no fundamental incompatibility between interests at stake, i. e. security interests and relevant fundamental human rights, it is not a dead end situation. In case of counterterrorism measures related to digital surveillance and data retention, the focus shall be currently placed on (i) reviewing and designing measures that would succeed in proportionality test (including review of Passenger Name Record Directive (2016/681) and bilateral Passenger Name Record agreements) (regional level) and (ii) developing detailed international standard of privacy rights in order to prevent the systematic clash (international level).

Keywords: counter-terrorism, digital surveillance, data retention, data protection, privacy.

Introduction

Since 11 September, 2001 (further as 911) attacks (however not only as a reaction to these in particular) there was a high number of measures introduced (or developed) to fight (prevent) terrorism. These measures include data surveillance as a tool of counter-terrorism action and have been developed on national, regional and international levels extensively, both in a form of legislation and international agreements. Examples include the legal acts as enacted by the United States Congress in the immediate aftermath of the 911 attacks which introduced passenger and cargo screening, several countries such as Argentina, Brazil, Denmark, Mexico, Japan, the Russian Federation, the United Arab Emirates, Saudi Arabia, South Korea and the United Kingdom have introduced (or are considering introducing) national legislation imposing on air carriers operating within their jurisdiction to provide passengers' data to their authorities[53], European Union introduced Data Retention Directive[54], negotiated agreements on passenger name record with the United States, Australia and Canada. Being enacted in a rush, partially because of the desire of urgent political response, some of the measures have been found to be adopted on a wrong legal basis and/or being incompatible with the fundamental human rights. Leaving aside the

[52] *Viltė Kristina Steponėnaitė is a PhD student at Vilnius University, Faculty of Law, researching United Nations and European Union targeted restrictive measures, with a particular focus on their interaction with human rights, and lecturer of European Union Economic Law at Vilnius University, Faculty of Economics and Business Administration, with a particular focus on European Union substantive law, consumer, privacy and data protection law.*

[53] E. Carpanelli and N. Lazzerini, 'PNR: Passenger Name Record, Problems Not Resolved? The EU PNR Conundrum After Opinion 1/15 of the CJEU' [2017] Air & Space Law 42 No. 4&5, p. 378

[54] European Parliament and Council Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105/54 (Data Retention Directive).

purely national measures the paper portrays two of the most recent regional and international examples, namely, the cases of Data Retention Directive and draft European Union – Canada Passenger Name Record Agreement, as illustrating precisely some of the key problems of the current counter-terrorism policy.

The case of Data Retention Directive

One of the legislations adopted under stress is the European Union directive concerning personal data retention, enactment of which accelerated soon after the train bombings in Madrid on 3 March, 2004. The proposal of four European Union Member States was initially dropped mostly because of the human rights concerns and competing initiatives, however not long after another attack in London on 7 July, 2005 the agreement was found and Data Retention Directive came into force, aiming, among the other things, to monitor telecommunications data as mobile telephones were reportedly used for and during the recent attacks and telecommunications information was considered to be very important for the investigations[55]. After all the Data Retention Directive required that providers of publicly available electronic communications services or public communications networks retain data necessary to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to identify the location of mobile communication equipment, data which consist, inter alia, of the name and address of the subscriber or registered user, the calling telephone number, the number called and an internet protocol address for internet services. Those data made it possible to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also made it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period[56]. Overall, even withouth requiring to retain the content of the communications, the data enabled the ones processing it to draw very precise conclusions concerning the private lives of the persons. Furthermore, requiring to retain these data the Data Retention Directive appeared to be very broad in number of respects, including the range of crimes for which the data could have been used and the retention period (up to 24 months). The directive referred to serious crime broadly instead of terrorism and serious organised crime only, leaving lots of discretion to Member States. Member States were also left with the wide discretion deciding upon the retention period which was set to be no less than 6 months and no more than 24 months. Bearing in mind the principles of the European Union data protection it came as no surprise that legallity of such potential wide-ranging interference (both by the private actors and by the competent national authorities afterwards) with the human rights, namely, with the respect for private and family life and with the protection of personal data (which is generally acceptable if

[55] The directive generally aimed to harmonise the European Union Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. The was applied to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It was not applied to the content of electronic communications, including information consulted using an electronic communications network. Member States were obliged to adopt measures to ensure that the data specified in the directive were retained and that particular data included (a) data necessary to trace and identify the source of a communication, e. g. the calling telephone number and the name and address of the subscriber or registered user, (b) data necessary to identify the destination of a communication, e. g. the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed and the name(s) and address(es) of the subscriber(s) or registered user(s), (c) data necessary to identify the date, time and duration of a communication, e. g. concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication, (d) data necessary to identify the type of communication, e. g. concerning fixed network telephony and mobile telephony: the telephone service used, (e) data necessary to identify users' communication equipment or what purports to be their equipment, e. g. concerning mobile telephony the calling and called telephone numbers, and also various (f) data necessary to identify the location of mobile communication equipment. Member States had to ensure that the data were retained for periods of not less than six months and not more than two years from the date of the communication.

[56] Digital Rights Ireland Ltd and Others, Court of Justice of the European Union at Joined Cases C 293/12 and C 594/12 [2014] ECLI:EU:C:2014:238 26.

proportionate) aroused suspition and the case was brought to the Court of Justice of the European Union (further as the CJEU).

The CJEU have not expressed doubts that the measures introduced are suitable for their purposes (not to confuse with the efficiency which is not estimated by the CJEU, at least not in the context of counter-terrorism measures), however it was quick to conclude that they are not necessary (failing to meet the second criterion of the proportionality test). Finding the interference with privacy rights of practically the entire European population[57], the court has basically found five major faults dooming the legality of the Data Retention Directive. Firstly, there was no limit on the personal scope of application, affecting all persons using electronic communications, therefore anyone without any link to any crime (not even a serious one). Secondly, there were no limits for the national competent authorities to access the personal data. There were also no rules concerning the timeframe for the retention of data and there were no sufficient safeguards concerning security and protection of the personal data provided and, lastly, there was no requirement to retain data within the European Union[58].

Overall, the Data Retention Directive provided an opportunity to interefere with one's privacy significantly and a measure like this, though suitable generally, should have succeeded in the necessity test and this is precisely what it failed to do, as CJEU discovered. Looking back today, when the most rigorous and far-reaching privacy framework in the world history is just on the other side of the corner, this judgment may look like a common sense result, however back then (only four years ago) it was argued to be a major leap forward[59], forming a strong case favoring privacy protection in the digital age[60], testifying a growing priority to data protection. The judgment generally outlined the limits of the bulk collection of data which where upheld and expanded in 2015[61], 2016[62] and 2017[63].

Both the following Schrems judgment as adopted by CJEU on October 6, 2015, invalidating the Safe Harbor arrangement, which governed data transfers between the EU and the US, and Tele2 Sverige judgment as adopted by CJEU on 21 December 2016, providing preliminary judgment concerning general and indiscriminate retention of traffic and location data, have contributed to this direction. While invalidating Safe Harbor agreement CJEU emphasized that European Union legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights[64] must, according to the settled case-law, lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data[65], making unlimited interference by institutions and lack of effective remedy not acceptable. Afterwards in Tele2 Sverige and Watson case the court confirmed that while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify the legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight[66]. Accordingly, legislation which covers, in a generalised manner, all subscribers and registered users and all means of electronic communication as well as all

[57] *Ibid*., p. 56.
[58] *Ibid*., pp. 58-71.
[59] F. Fabbrini, 'Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States' [2015] Harvard Human Rights Journal p. 81.
[60] *Ibid*., p. 68.
[61] Schrems v. Data Protection Commissioner, Court of Justice of the European Union at C-362/14 [2015] ECLI:EU:C:2015:650.
[62] Tele2 Sverige AB and Others, Court of Justice of the European Union at Joined Cases C-203/15 and C-698/15 [2016] ECLI:EU:C:2016:970.
[63] Opinion, Court of Justice of the European Union in procedure 1/15 [2017] ECLI:EU:C:2017:592.
[64] Charter of Fundamental Rights of the European Union [2000] OJ C-364/1 (Charter of Fundamental Rights).
[65] Meanwhile there were no data about rules in the United States that would have been intended to limit interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States, interference which the State entities of that country would be authorised to engage in when they pursue legitimate objectives, such as national security. Schrems v. Data Protection Commissioner, Court of Justice of the European Union at C-362/14 [2015] ECLI:EU:C:2015:650 88-91.
[66] Tele2 Sverige AB and Others, Court of Justice of the European Union at Joined Cases C-203/15 and C-698/15 [2016] ECLI:EU:C:2016:970 103.

traffic data, and provides no differentiation, limitation or exception according to the objective pursued (is not restricted to retention in relation to (i) data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to fighting crime) exceeds the limits of what is strictly necessary and cannot be considered to be justified[67].

The case of draft European Union – Canada Passenger Name Record Agreement

Another attempt to fight (prevent) terrorism with processing personal data is illustrated by bilateral passenger name record (further as PNR) (draft) agreements[68] by and between European Union and the United States, Canada and Australia. Besides putting countries at risk of conflicting obligations[69], being is costly, time-consuming and resulting to legal-uncertainty for air carriers while they are operating with many other third countries which have no similar agreements, these agreements create the framework for transfers which leads to interference with the respect for private and family life and with the protection of personal data. In the aftermath of the judgments portrayed above it came as no surprise that the draft European Union – Canada agreement as being renegotiated[70] has become a matter of concern and the European Parliament decided to call for an opinion of the CJEU, making it the first call for an opinion on the draft international agreement's compatibility with the Charter of Fundamental Rights.

The court upheld the appropriateness of the measures, however again found the failure to succeed at the proportionality test and therefore concluded that the agreement cannot be concluded in its current form[71]. Firstly, it found there was no justitification to transfer sensitive data and it was not necessary for the purpose to protect public security against terrorism and serious transnational crime, secondly, if found that the continued storage of the PNR data during their stay in Canada and after their departure was not limited to what is necessary. Indeed, while the agreement provides opportunity to store data for a very long period of 5 years, it is not limited to the cases of some objective evidence showing such a need, making an opportunity to retain the data without even a merely indirect connection with the objective pursued.

Surprisingly, however, in contrast with the previous decisions, the court provided some rather detailed guidelines for a further development. Taking into account those guidelines, it may be concluded that the CJEU considered there are six key problems in the draft agreement, namely, (i) lack of clarity and precision on what PNR data shall be transferred (it shall be noted that three out of nineteen headings of PNR data as provided in the agreement are quite vague expressions, potentially covering sensitive data); (ii) lack of specific, reliable and non-discriminatory models and criteria for the automated processing; (iii) lack of limitations on the use of the transferred data (by databases to fight against terrorism and serious transnational crime only); (iv) lack of legal basis to disclose data to third countries; (v) lack of individual notification regarding the use of the PNR data; (vi) lack of guarantee of the oversight of the rules to be provided by an independent supervisory authority (so, basically, lack of remedy which is another major issue).

Such an opinion may serve as an encouragement for the Passenger Name Record Directive[72] with some of its generic rules (as shall be brought into force by the Member States by 25 May, 2018) to be brought before the court and encourages review of the existing PNR bilateral agreements with Australia

[67] *Ibid*., pp. 105-107.

[68] PNR agreements generally concern data – information provided by passengers when they book tickets and when checking in for flights, as well as data collected by air carriers for their own commercial purposes. It usually includes passengers' contact details, travel initeraries, seat numbers, meal preferences. Alone looking innocent such data being analysed provide a detailed portrait of one's private life, at the same time enabling detection and monitoring of suspects, being a handy tool for law enforcement authorities to fight serious crime and terrorism.

[69] E. Carpanelli and N. Lazzerini, *Ibid*., p. 381; C. C. Murphy, 'EU Counter-Terrorism Law. Pre-Emption and the Rule of Law' (Hart Publishing 2015) p. 158.

[70] The first European Union – Canada agreement expired in 2009 and the second one was signed in 2014. The Council reqested for the approval of the European Parliament.

[71] Opinion, Court of Justice of the European Union in procedure 1/15 [2017] ECLI:EU:C:2017:592.

[72] European Parliament and Council Directive on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime 2016/681 [2016] OJ L 119/132

and the United States, whether they, as obviously predating the discussed case law, are compatible with the European Union primary law. Regardless small differences, the scholars argue, there are solid elements to conclude that both the Passenger Name Record Directive and the remaining two agreements can hardly escape a finding of incompatibility with the Charter of Fundamental Rights[73], of course if following the same reasoning by the court.

Overall, despite the increasingly demonstrated attention to human rights, these cases demonstrate threat to privacy as continuosly being introduced by counter-terrorism measures. Furthermore, it may be reasonably argued that war on terror continuosly overrides number of other fundamental human rights. Firstly, there is no dispute that measures against states had severe impact on the whole population and caused severe derogations from the very basic human rights. Secondly, targeted (individual) restrictive measures as implemented by the United Nations Security Council and the European Union (European Council), despite all of the improvements implemented during the last few decades, including the establishment of the Office of the Ombudsperson within the United Nations, are still being implemented without ensuring the very basic rights to a fair trial and an effective remedy.

All of this being relevant leaving aside the fact that, though the CJEU refrains from denying/evaluating the importance (and the appropriateness) of various counter-terrorism measures, it may be reasonably argued that people are giving up their freedoms without actually gaining up security.

These problems are partially related to what may be called as the general shift from prevention to pre-emption. Prof. Cian Murphy, one of the most published scholars in the field, defines pre-emption as involving taking intrusive action against potential threats based on, at best, mere suspicion. According to Murphy a pre-emptive approach to counter-terrorism is indicated by two fundamental changes: (i) from action based on past harm to the one based on future worse-case scenarios and (ii) from accepting a certain risk of harm as normal to holding all such risk unacceptable[74]. Furthermore, it entails changes to (i) the type of action taken (including broad surveillance), (ii) target of the action (including entire population) and (iii) the actors that are empowered (executives (governments), law enforcement agencies, private actors), gaining significant powers[75]. It is being argued that it is evident in policy documents such as the Action Plan on Combating Terrorism, in the preambles to various legislative acts and in the operative text of those acts, also, that European Union counter-terrorism seeks to eradicate any space in which violent politics could develop[76], and therefore takes measures affecting all individuals, regardless their prior criminal record[77] (the case of mass surveillance and generalised suspicion), and takes measures not necessarily only after particular crime was committed (the case of targeted restrictive measures). This is relevant on the United Nations level as well. And measures like these, bearing in mind their breadth and the type of empowered actors, inevitably poses a greater risk to a proper balance with human rights.

However, as long as there is no fundamental incompatibility between interests at stake, i. e. security interests and relevant fundamental human rights, it is not a dead end situation. Without underestimating the importance of review of the international and regional documents in the short term, international instruments shall be developed, ideally through the legally binding international treaties. In case of counterterrorism measures related to digital surveillance and data retention, the focus shall be currently placed on (i) reviewing and designing smaller scale measures that would succeed in proportionality test (including review of Passenger Name Record Directive (2016/681) (regional level) and bilateral Passenger Name Record agreements), at the same time (ii) developing detailed international standard of privacy rights in order to prevent the systematic clash (international level).

[73] E. Carpanelli and N. Lazzerini, *Ibid*., p. 377-402.
[74] C. C. Murphy, 'EU Counter-Terrorism Law. Pre-Emption and the Rule of Law' (Hart Publishing 2015) p. 219.
[75] *Ibid*., pp. 220-223.
[76] C. C. Murphy, 'EU Counter-Terrorism & the Rule of Law in a post-'War on Terror' World' in M. Scheinin (ed) 'European and United States Counter-Terrorism Policies, the Rule of Law and Human Rights' [2011], http://ssrn.com/abstract=1958335.
[77] C. C. Murphy, 'EU Counter-Terrorism Law. Pre-Emption and the Rule of Law' (Hart Publishing 2015) p. 178.

Conclusions

Technological development enabled monitoring, storing, analysing records of massive amounts of personal data, which, combined with security interests and faulty regulations (or the lack of them), resulted in governments and private subjects enabled to dispose enormous amount of personal data of a very large number of innocent people. These decisions resulted in significant interference with the fundamental human rights and condemning case law; number of regulations have been declared (or is expected to be declared) void as introducing unproportional measures and lacking proper safeguards, compromising already controversial war on terror in the end.

Bearing in mind that the CJEU advances a strict proportionality during the last decade, it is highly likely that the existing international PNR agreements, the PNR Directive and other similar documents will be challenged (and challenged successfully) if not reviewed/designed properly on time. Accordingly, review and design of smaller scale documents is encouraged (and the most likely) solution in the short term, however for the long term international solutions through international agreements are the ones which shall be introduced as well.

Bibliography

Books

1. C. C. Murphy, 'EU Counter-Terrorism Law. Pre-Emption and the Rule of Law' (Hart Publishing 2015)

Articles

1. C. C. Murphy, 'Fundamental Rights and Security: The Difficult Position of the European Judiciary' [2010] European Public Law 16 No. 2 289–308
2. E. Carpanelli and N. Lazzerini, 'PNR: Passenger Name Record, Problems Not Resolved? The EU PNR Conundrum After Opinion 1/15 of the CJEU' [2017] Air & Space Law 42 No. 4&5.
3. F. Fabbrini, 'Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States' [2015] Harvard Human Rights Journal.

Legislations

1. Charter of Fundamental Rights of the European Union [2000] OJ C-364/1 (Charter of Fundamental Rights).
2. European Parliament and Council Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105/54 (Data Retention Directive).
3. European Parliament and Council Directive on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime 2016/681 [2016] OJ L 119/132 (Passenger Name Record Directive) .

Cases

1. Digital Rights Ireland Ltd and Others, Court of Justice of the European Union at Joined Cases C-293/12 and C-594/12 [2014] ECLI:EU:C:2014:238.
2. Schrems v. Data Protection Commissioner, Court of Justice of the European Union at C-362/14 [2015] ECLI:EU:C:2015:650 88.
3. Tele2 Sverige AB and Others, Court of Justice of the European Union at Joined Cases C-203/15 and C-698/15 [2016] ECLI:EU:C:2016:970.
4. Opinion, Court of Justice of the European Union in procedure 1/15 [2017] ECLI:EU:C:2017:592.

Other

1. C. C. Murphy, ‘EU Counter-Terrorism & the Rule of Law in a post-‘War on Terror’ World’ in M. Scheinin (ed) ‘European and United States Counter-Terrorism Policies, the Rule of Law and Human Rights’ [2011], http://ssrn.com/abstract=1958335.

TAXATION OF THE DIGITAL BUSINESS MODELS IN THE INTERNATIONAL TAX LAW – NEW CHALLENGES FOR EFFECTIVE TAXATION OF INCOME

Tim Artur[1]

Abstract

Digital business models have revolutionized the world in which we are living now. With the use of the digital business models it is possible to pursue economic activity on a large scale, without a physical presence in the territory of a certain jurisdiction. Such a form of economic activity was a rule in the conventional economy. On the presumption of the physical presence, which was supposed to be the only way to pursue economic activity, the whole global order of the international tax law was grounded. Therefore the issue of effective taxation of the digital economy is nowadays as high on the global, political agenda as e.g. climate change.

In the article the Author presents the essence of the features of the digital economy, relevant for direct tax purposes, explains the phenomenon of non-effective-taxation of the digital business models and outlines means of reaction, coined by the OECD and the European Commission to protect fiscal interests of source states. For the reason of the limited length the Article, the analysis is limited to the direct business activities on the ground of the international tax conventions.

Keywords: digital economy, digital business models, international tax law, European Union

Introduction

Taxation of the digital economy is nowadays as high on the international, political agenda, as these matters, which have been traditionally recognized as the most vital issues of the whole international society – just as the climate change.[2] In the present reality it is possible to pursue economic activities from any place in the world – in addition even with the velocity of light (with use of the optic fibers). Traditional rules of the international taxation are applied also to these business models, which are grounded in the intangible presence, what results in the non-effective taxation of income generated in a source state. In the Article the digital economy and the digital business models will be outlined, having regard their key-features for the international tax law. Furthermore, general rules of the international tax law as well as the essence of the non-effective taxation of the digital business models will be presented.

The purpose of this article is to answer to the question if measures, currently adopted by the international society, are sufficient to the effective taxation of the digital business models on the ground of the international conventions. For the reason of the limited length of the Article, that issue will be just outlined and limited only to the direct business activities. Adopted methodology consists of analysis of the legal acts, international tax agreements, official documents of the OECD and the European Union as well as international tax doctrine.

1. Digital economy and digital business models

Digital economy was called "the preeminent driver of economic growth and social change"[3] as long ago as 1999. Also then the relation between understanding of that phenomenon and the wisdom of decisions made in the scope of law was strongly remarked. The digital economy was grounded on the

[1] *Polish tax adviser, Polish insolvency and restructuring adviser (Official receiver), Polish customs agent, PhD Candidate at the Faculty of Law and Administration, University of Lodz, Poland.*

[2] As an example, M. A. Kane invokes the G20 Summit in Brisbane, Australia. See gen.: M.A. Kane, 'A defense of source rules in international taxation' [2015] Yale Journal on Regulation, Iss. 2, Art. 4, p. 312.

[3] N. F. Lane, Assistant to the President of the United States of America for Science and Technology, Director of the Office of Science and Technology Policy in the White House from August 1998 to January 2001.

technological revolution connected with the discovery of a new "general purpose engine"[4]. Just after the first revolution (related to a steam engine) and the second one (related to an electric motor and oil), there occurred the third revolution, concerning technological innovations and information revolution - the digital revolution. [5] According to Y. Moulier Boutang, we are living now in the age of the "cognitive capitalism", which came after the age of the "industrial capitalism". [6] In the cognitive capitalism, profit is no longer dependent on material capital, but on "exploitation of digital goods, which can be defined in the language of bits (zeros and ones)"[7]. To stress the importance of the current changes and to name the upcoming system, there has been even coined a new term of the "Industry 4.0"[8] - one of the consequences of the digital revolution, recognized by some scholars is a change of the whole economic system, in which we are living now. Thus, the digital business models have today for the world economy that same importance as steam-based business models in the 19th and 20th century, what proves the importance of new rules, which have to be urgently implemented into the international tax law system, in light of the non-effective taxation of new, digital business models. Nowadays, digital business models are being used not only by multinational enterprises, such as Amazon, Google or Facebook (so called Multi-National Enterprises, hereinafter: MNEs), but also by numerous small and medium entrepreneurs (hereinafter: SMEs). The tendency to use the digital business models is still growing.[9]

2. Tax relevant differences between traditional and digital business model

Information and communication technology (hereinafter: ICT) has influenced all sectors of the human activity - such as retail (i.a. by allowing customers to place online orders), transport and logistics (i.a. by enabling the tracking of cargo), financial services (i.a. by enabling customers to conduct transactions online), manufacturing and agriculture (i.a. by controlling modern robots), education (i.a. by video conferencing), healthcare (i.a. by enabling remote diagnosis), broadcasting and media (i.a. by creating new means to deliver media and to gain information). [10] Indisputably, more and more enterprises become nowadays digital. The scope of the digital economy covers such important categories as Personal Computing Devices, telecommunications networks, software, so called "content", "use of data", cloud-based processes.[11] In the nearest future, a rapid growth of the following issues grounded in the digital economy is predicted: so called "internet of things", virtual currencies, advanced robotics, 3D-Printing, so called "the sharing economy", access to government data, reinforced protection of personal data.[12] It should be noticed that the digital economy is also a base to extract from its scope of application completely new branches such as "the App Economy"[13]. Also the process of globalization is based on the digital revolution.[14] Some authors claim that globalization leads to creation even the new economic system "on the whole-planetary scope, constituting a new quality in the global economy"[15]. The predictions are stated that the third technological revolution is not the last one in twenty-first century. To stress the importance of the current changes and to name the upcoming system, there has been coined even the

[4] P. A. David, 'The Dynamo and the Computer: An Historical Perspective on the Modern Productivity Paradox' [1990] The American Economic Review Vol. 80, No. 2, p. 355.
[5] I. Pietrzyk, 'Globalizacja i regionalizacja gospodarki światowej, in: Gospodarka światowa w warunkach globalizacji i regionalizacji rynków' (Warszawa 2009) p. 21.
[6] T. Rosenbuj, 'Taxing digital' (Barcelona 2015) p. 21.
[7] *Ibid*., p. 21.
[8] "Industrie 4.0.", Bundesministerium für Bildung und Forschung, Zukunftsbild, bmbf.de, accessed 19 April 2018.
[9] European Commission, 'Commission Staff Working Document: Europe's Digital Progress Report 2017' (Brussels 2017) pp. 71 et seq.
[10] OECD, Public Discussion Draft, BEPS Action 1: Address the tax challenges of the digital economy, (Paris 2014) pp. 23-24.
[11] OECD, 'Addressing the Tax Challenges of the Digital Economy. Action 1 - 2015 Final Report' (Paris: OECD Publishing 2015) OECD/G20 Base Erosion and Profit Shifting Project, pp. 36-41.
[12] *Ibid*., pp. 42-46.
[13] OCED, The App Economy, "OECD Digital Economy Papers", No. 230/2013.
[14] E. Oziewicz, 'Globalizacja we współczesnej gospodarce światowej i jej skutki' in E. Oziewicz (ed.), 'Przemiany we współczesnej gospodarce światowej' (Warsaw 2006) p. 240.
[15] I. Pietrzyk, *Ibid*., p. 22.

new term “Industry 4.0”[16]. Furthermore, the following, relevant for the tax law purposes, key-features of the digital economy are being identified in the legal doctrine[17]:

I. **Mobility**, which should be considered under three aspects: mobility of intangibles, mobility of users and customers, mobility of business functions.[18]

II. **Reliance on data and users participation** - it is estimated that just some kind of digital activities (online and mobile financial transactions, social media traffic and GPS coordinates) generate 2,5 exabytes (billions of gigabytes or millions of terabytes) of data every day. Such scale of using and processing information caused a creation of a special term describing that phenomenon – the term of "big data".[19]

III. **Network effects -** decisions of users may have a direct impact on the benefits gained by the others, what has been called a "network effect". Every digital device requires a counter-device, compatible to it. Exempli gratia, using phone without existing any other user in the world possessing another phone is pointless.[20]

IV. **Use of multi-sided, flexible and reach business models** - a multi-sided business model is grounded on the cooperation between groups of persons and the link between profits generated by the one group and decisions undertaken by the others. There are two kinds of that business model – involving positive and negative externalities. An example of the first one is a payment card system, which requires the cooperation between merchants (entities accepting cards) and customers (entities using cards). The decision to use card influences on the decision of merchants and also generates profit for the other sides (e.g. banks or terminal operator). A negative externalities refers to providing services or goods without payments or at a cost lower than the cost of production, but with a profit gained from advertisers or entities collecting certain data about users. Multi-sided business model is also being characterized by the two features: flexibility and reach. The flexibility means that digital resources can be stored to create value for a long time and there is a lot of possibilities to adapt collected data. The reach refers to the location of that same model in different countries, without any restrains regarding to the requirement of the physical presence.[21]

V. **Tendency toward monopoly or oligopoly in certain business models** - the digital economy also promotes monopoly or oligopoly, by the reason of a significant innovativeness the following technological inventions and a possibility to gain a dominant position in a quick way, what causes cumulation of goods by just a few of entrepreneurs. That effect is also stimulated by the single standard of using platforms or devices, constructed with the patentable technologies.[22]

VI. **Volatility** due to low barriers to entry and rapidly evolving technology - the progress in miniaturization and slight cost of Internet access results in reducing barriers to entry for digital businesses. The capital expenditure on development and researches still fosters creating innovations and new products and thereby poses challenges before the legislators.[23]

Ottawa Ministerial Conference on Electronic Commerce in 1998 stated that the same principles that governs the taxation of conventional commerce, should equally apply to taxation of the e-commerce. To such principles belong neutrality, efficiency, certainty and simplicity, effectiveness and fairness, flexibility.[24] The neutrality requires from the tax law to be neutral and equitable between conventional and

[16] "Industrie 4.0.", Bundesministerium für Bildung und Forschung, Zukunftsbild, bmbf.de, accessed 19 April 2018.
[17] OECD, ‘Addressing the Tax Challenges of the Digital Economy. Action 1 - 2015 Final Report’ (Paris: OECD Publishing 2015) OECD/G20 Base Erosion and Profit Shifting Project, pp. 64-65.
[18] See gen. *Ibid*., pp. 65-67.
[19] See gen. *Ibid*., pp. 68-70.
[20] See gen. *Ibid*., pp. 70-71.
[21] See gen. *Ibid*., pp. 71-72.
[22] See gen., *Ibid*., pp. 72-73.
[23] See gen., *Ibid*., p. 73.
[24] OECD, Taxation and Electronic Commerce. Implementing the Ottawa taxation framework conditions (Paris 2001) p. 10.

digital economy. The efficiency means that - from the business perspective - compliance costs and - from the government perspective - administration costs, shall be minimized as far as possible. Certainty and simplicity require the tax law to be clear and simple to understand for the taxpayers. The tax law should produce the right amount of tax at the right time, with minimizing the level of evasion (Effectiveness and fairness) and also should be flexible, keeping pace the technological development (flexibility). The above-stated principles are a suggestion how the fair taxation of the digital business models shall be understood.[25]

3. Effective taxation of the digital business models

Bilateral tax treaties based on the OECD and UN Model Conventions are the most popular measure of the avoidance of the juridical double taxation.[26] Pursuant to art. 7 OECD and UN Model Convention (and all of the double tax treaties), profits of an enterprise are taxable only in that state, where the enterprise resides. However, if the entrepreneur has a permanent establishment within the territory of the source state, then that state is also entitled to tax such an income and certain method of avoidance of double taxation shall be applied. Permanent establishment concept can be generally described as taxable presence of a non-resident, which is created by the "agreed minimum form of physical presence in that country"[27] (commonly referred to as a "PE-threshold"). The permanent establishment concept (germ. *Betriebstätte*) appeared for the first time in the legislation of Prussia in 1885.[28] On the ground of the international conventions that term occurred first in Germany-Italy Double Tax Treaty[29]. Since the works done by the League of Nations, the permanent establishment concept has been just further specified.[30] Nowadays on the ground of both the OECD and UN Model Convention, profits of enterprise are still taxed under the rules concerning the permanent establishment concept, what makes that institution one of the most important concepts in the international tax law.[31]

The definition of the permanent establishment has been introduced in the article 5 OECD and UN Model. Pursuant to art. 5 par. 1 OECD Model Convention, for the purposes of the Convention, the term "permanent establishment" means a fixed place of business through which the business of an enterprise is wholly or partly carried on. That definition indicates on the three conditions required to establish a permanent establishment:

I. existence of a place of business (such as office, machinery or equipment),
II. place of business must be fixed, what means that it has to be established with a certain degree of permanence,
III. the business must be carried on by the enterprise through that fixed place of business.[32]

The term of "place of business" - which is the first premise and the crucial one for the issue of taxation of the digital economy - has broad meaning and covers premises, facilities or installations used for carrying on the business of the enterprise, which do not have to be used exclusively for that purpose. It should have also a certain amount of space at entrepreneurs disposal, but the legal title for that place is irrelevant to recognize a permanent establishment.[33] Even possessing the place in an illegal way can provide to establishing a place of business in the meaning of art. 5 par. 1 OECD Model Convention.[34] However, besides the physical and tangible character, that place has to be also at the disposal of that

[25] See gen. *Ibid*., pp. 10-11.
[26] Z. Kukulski, 'Konwencja modelowa OECD i Konwencja modelowa ONZ w polskiej praktyce traktatowej' (Warszawa 2015) p. 239. For the reason of the limited lenght of the Article, the issue of juridical double taxation, as well as uni- and multilateral measures of the avoidance of the juridical double taxation will not be outlined.
[27] European Commission, 'Expert group on taxation of the digital economy. Working Paper: Digital Economy - Facts & Figures' (Brussels 2014) p. 16.
[28] W. Morawski, 'Wytyczne komitetu spraw podatkowych OECD' in B. Brzezinski (ed.), 'Model Konwencji OECD' (Warszawa 2010) p. 318.
[29] Z. Kukulski, *Ibid*., pp. 34-35.
[30] W. Morawski, *Ibid*., p. 318.
[31] Z. Kukulski, *Ibid*., p. 173.
[32] OECD, Commentary on art. 5, in: Commentaries on the articles of the Model Tax Convention, OECD (Paris 2010) par. 2.
[33] *Ibid*., par. 4.
[34] *Ibid*., par. 4.1.

enterprise.[35] The other conditions and kinds of the permanent establishments will not be analyzed in the Article. It should be only noted that the preparatory or auxiliary activities cannot constitute the permanent establishment.[36] The Commentary on the OECD Model Tax Convention (which has particular importance for the uniform interpretation of tax treaty provisions) strongly stresses that the permanent establishment can be constituted even if business activities are pursued by the automatic equipment, instead of staff, and the most important issue in the interpretation of the term "place of business" in the context of the digital economy is a requirement of the physical presence in the territory of certain jurisdiction.[37]

Therefore, basing on the Commentary, the digital presence cannot constitute the permanent establishment. In the context of the digital business models the only way to constitute the PE is either a dependent agent or a place of business in the meaning of art. 5 par. 1 OECD and UN Model Convention (such as server), located within the territory of a source state, which does not pursue preparatory or auxiliary activities. Other interpretation by tax authorities or national courts will constitute a breach of basic rules of interpretation of the double tax treaties. As a result of applying such rules to the digital economy, the digital business models become non-effective taxed in a source state. The reason of that is a lack of physical presence while pursuing economic activities in the territory of a certain state, what results in the lack of possibility to constitute the PE-threshold.

Together with the aggressive tax planning methods, a lack of effective taxation of the digital economy can be destructive not only to the budget of single states, but also the economy of the whole region. As an example of such a practice can be invoked the Amazon case. According to the European Commission, income of Apple was taxed in Ireland with an effective tax rate 0,005%, what was deemed to be an illegal state aid. Ireland was obliged to exact from the MNE 13 billion euro of taxes (as a result of applying a tax rate of only 1%). For failure in fulfilling that obligation, the Commission referred Ireland in 2017 to the Court of Justice of the European Union.[38] Furthermore, a lack of taxation in the source state cannot be treated as either tax evasion or tax avoidance. The fundamental rules of taxation of income are not adjusted to pursuing economic activities in a digital way. However, the issue of non-effective taxation of the digital business models is vital not only in the cases, concerning obtaining by the digital entrepreneur the tax residence of a low-tax jurisdictions. Even when such an entrepreneur is world-wide taxed in the high-tax jurisdiction, a source state cannot participate in generated income.

Another issue, connected with the taxation of the digital business models is determining the residency of digital entrepreneurs – what is a result of mobility of the digital economy. Nowadays it is possible to manage the enterprise from any place in the world – in addition with the velocity of light. In the case of dual residence of an entrepreneur, on the ground of the international tax treaties following the UN and OECD-Model, the place of permanent physical presence shall prevail – regardless if it is an individual or a company. In the first case, a criterion of permanent home will be decisive.[39] In the latter case – location of the place of effective management will prevail.[40] In both cases it is possible to pursue economic activity from the territory of one state (in which permanent home or place of effective management is located) with a significant digital presence in the territory of the second state, without creating the permanent establishment, based on the physical presence, and therefore by making it impossible for the source state to participate in income derived in its territory.[41]

Having regard above exemplified issues, the taxation of digital business models is becoming now the most vital issue in the international tax law - not only for the reason of using the digital economy as a method of aggressive tax planning, but also as creating a high level of legal uncertainty, by application of

[35] *Ibid*., par. 4.2.
[36] Art. 5 par. 4 OECD Model.
[37] OECD, Commentary on art. 5, in: Commentaries on the articles of the Model Tax Convention, OECD (Paris 2010) par. 10.
[38] Press statement of the European Commission of 4th October 2017, http://europa.eu/rapid/press-release_IP-17-3702_en.htm, accessed 19 April 2018.
[39] Art. 4 par. 2 OECD Model Convention.
[40] Art. 4 par. 3 OECD Model Convention.
[41] For the reason of the limited length of the article, possible departures from the Model will not be described. It should be only noted that other wording of art. 4 certain tax convention may occur.

outdated rules in a completely different economic reality to these business models, which have been created as a natural result of the digital transformation of common reality.

4. OECD and European Union approach

Progressive range of aggressive tax planning methods and obsolete rules of international taxation have been wider analyzed at the world-wide level in the OECD Project called BEPS (Base Erosion Profit Shifting). The first one from the 15 action plans of BEPS was concerning the taxation of the digital economy and resulted in publishing in 2015 the Report[42]. As it is summarized in the legal writing in accordance with the title of the Report, OECD has rather "addressed", than "met" the challenges posed by the digital economy before the tax law[43] and the most difficult tasks are still to be achieved by the international society.[44]

Although the European Commission held that the digital economy had influenced on all of the sectors of the economy and social activities[45], the European Union is still called as "vulnerable"[46] to tax planning activities, made by entrepreneurs using digital business models, for the reason of the current shape of the international tax law institutions. A lack of effective means of taxation of the digital business models resulted in application institutions established outside the scope of the tax law - namely rules concerning competition law and state aid. In the spring 2018, European Commission presented communicate, concerning effective taxation of the digital business models within the European Union.[47] In the communicate it was stated that effective average tax rate applied to the traditional international business model is at the level of 23.2%. Digital international business models are taxed with an effective tax rate of only 9.5%.[48] European Commission presented an idea of the new directive corporate taxation, based on a significant digital presence. As a second step of its action plan, the European Commission suggested the integration of that provision into the proposals for a Common Consolidated Corporate Tax Base. European Commission proposed also an interim measure taxing certain digital service revenues, namely digital services tax - tax imposed on gross annual revenues of certain digital enterprises. The tax rate would be at the level of 3%. Both of the proposed solutions take the form of directive, which shall be adopted on the ground of art. 115 TFEU[49] in a special legislative procedure. It should be noted that art. 115 TFEU requires unanimity in the Council. Meanwhile, in June 2018, the EU-Nordic states (Denmark, Sweden, Finland) officially rejected the proposal of the new, interim digital tax.[50] Some objections were taken also by Luxembourg, Cyprus, Malta and the United Kingdom.[51] Even when unanimity in the Council would not be achieved, cooperation between interested member states may be established in the European Union as the enhanced cooperation procedure, which requires participation of at least nine member states in the undertaken actions (art. 326 et seq. TFEU). However, such a procedure clearly leads to the division of the EU into the groups: member states fighting non-effective taxation of the digital business models and these, which are not participating in actions, coordinated at the European level.

It should be emphasized that not only sovereign jurisdictions makes an effort to the effective taxation of the digital economy – such an impulse comes also from the entrepreneurs, who do not implement tax planning structures, but act in the European market in the most natural for their business

[42] OECD, 'Addressing the Tax Challenges of the Digital Economy. Action 1 - 2015 Final Report' (Paris: OECD Publishing 2015) OECD/G20 Base Erosion and Profit Shifting Project.
[43] M. Olbert and C. Spengel, 'International Taxation in the Digital Economy: Challenge Accepted?' [2017] World Tax Journal, Vol. 9, No. 1.
[44] Prof. Ph. Baker summarized the OECD actions as it follows: "Impressive output so far, but the hardest parts are yet to come", BEPS Appraisal. Interview with Philip Baker QC, Journal of International Taxation 1/2015, str. 29.
[45] European Commission, 'Commission Staff Working Document: Europe's Digital Progress Report' (Brussels 2017) pp. 71 et seq.
[46] That term is used by the Dutch European Parliament Member, P. Tang, in the Report: P. Tang and H. Bussink, 'EU Tax Revenue Loss from Google and Facebook' [2017], p. 3: https://paultang.pvda.nl/, accessed 9 April 2018.
[47] European Commission, Communication from the Commission to the European Parliament and the Council "Time to establish a modern, fair and efficient taxation standard for the digital economy", Brussels, 21.3.2018, COM(2018) 146 final.
[48] *Ibid*., p. 6.
[49] Treaty on the Functioning of the European Union, Consolidated Text Official Journal of the European Union, 26.10.2012, C 326 pp. 47 et seq.
[50] M. Andersson, K. Jensen and P. Orpo, 'Nordic states urge U-turn on EU digital tax plans', euobserver.com, accessed 15 June 2018.
[51] A. Rhode, 'Some (bad) news on the EU Digital Tax', linkedin.com, accessed 15 June 2018.

way. According to the research provided by PwC - 47% companies feel that article 5 of the OECD Model Convention (concerning permanent establishment and non-taxation of the digital business models in the source state) is no longer adapted to deal with the complexity of their business, 63% companies agree that tax authorities have become more aggressive in assessing permanent establishments and 86% indicates that increased mobility triggers an increased permanent establishment risk.[52]

Conclusions

Fundamental institutions of the international tax law were created in the 19th and 20th century[53] - when the traditional business models, based on a physical presence within the territory of a certain jurisdiction, were the only way to conduct business. Therefore, at that time, the fair and rational manner of tax claims' allocation could be grounded on a physical presence rule.[54] Nowadays, the basic feature of the digital economy is a lack of physical presence, while pursuing activities, which in the traditional economy required such a presence. The essence of presented issue is that the digital business models enable to pursue economic activity without a physical presence in the territory of a certain jurisdiction. In such a case, the profit, generated on a wide scale, remain non-taxed in the source state. Currently applicable rules were created in the completely different economic reality – they are not just based on the conventional economy, but they were established in the century, when the conventional economy was the only form of conducting business. In such a reality, rules of the international tax law have to be revisited. The necessity of amending the international tax law system is being recognized not only both by the OECD and the European Commission, but also by the digital enterprises. Measures implemented by certain states and aimed to tax digital business models in an effective way can create a significant level of legal uncertainty for private entities, especially small and medium enterprises, pursuing economic activities with the use of the digital business models. There are many ideas how that change should be made. Until march 2018 both the efforts undertaken on the OECD- as well as on the European Union level were not sufficient enough to make a proper and unhesitating reaction on the non-effective taxation of the digital business models. Rules coined and proposed by the European Commission are a significant step in the way to the effective taxation of the digital economy in the international tax law and a great starting point for the further-going legal discourse, although the predictions may be stated, that the unanimity in the Council would be difficult to achieve. That conclusion causes a significant risk for European economic integration, which should be aimed at fighting non-effective taxation of the digital business models, having regard that goal is difficult to be achieved at the domestic level solely and requires strong, immediate reaction of the international community.

Bibliography

1. M. Andersson, K. Jensen and P. Orpo, 'Nordic states urge U-turn on EU digital tax plans', euobserver.com, accessed 15 June 2018.
2. BEPS Appraisal. Interview with Philip Baker QC, Journal of International Taxation 1/2015.
3. "Industrie 4.0.", Bundesministerium für Bildung und Forschung, Zukunftsbild, bmbf.de, accessed 19 April 2018.
4. P. A. David, 'The Dynamo and the Computer: An Historical Perspective on the Modern Productivity Paradox' [1990] The American Economic Review Vol. 80, No. 2.
5. European Commission, 'Commission Staff Working Document: Europe's Digital Progress Report 2017' (Brussels 2017).

[52] PwC, 'Permanent Establishments 2.0. At the heart of the matter', p. 2, pwc.com/tax, accessed 19 April 2018.

[53] Currently used in the international tax law fundamental institutions, were coined mainly in the late 19st and early 20st century, such as German concept of the permanent establishment (Germ. *Betriebstätte)*, which was implemented to the treaty on avoidance of double taxation, concluded between Prussia and Austria-Hungary in 1899. See gen. A. A. Skaar, 'Permanent Establishment: Erosion of a Tax Treaty Principle' (Boston 1991) p. 75.

[54] *E.g.* through an office, a factory, a workshop, a mine, a quarry. This exemplification is still included in the OECD Model Tax Convention, as well as in all of the treaties on avoidance on double taxation.

6. European Commission, Communication from the Commission to the European Parliament and the Council “Time to establish a modern, fair and efficient taxation standard for the digital economy”, Brussels, 21.3.2018, COM(2018) 146 final.
7. European Commission, ‘Expert group on taxation of the digital economy. Working Paper: Digital Economy - Facts & Figures’ (Brussels 2014).
8. European Commission, Press statement of the European Commission of 4th October 2017, access: http://europa.eu/rapid/press-release_IP-17-3702_en.htm [19th April 2018].
9. M. A. Kane, ‘A defense of source rules in international taxation’ [2015] Yale Journal on Regulation, Iss. 2.
10. Z. Kukulski, ‘Konwencja modelowa OECD i Konwencja modelowa ONZ w polskiej praktyce traktatowej’ (Warszawa 2015).
11. W. Morawski, ‘Wytyczne komitetu spraw podatkowych OECD’ in B. Brzezinski (ed.), ‘Model Konwencji OECD’ (Warszawa 2010).
12. OECD, ‘Addressing the Tax Challenges of the Digital Economy. Action 1 - 2015 Final Report’ (Paris: OECD Publishing 2015 OECD/G20 Base Erosion and Profit Shifting Project..
13. OCED, 'The App Economy, “OECD Digital Economy Papers”, No. 230/2013.
14. OECD, ‘Commentaries on the articles of the Model Tax Convention’ (Paris 2010).
15. OECD, Public Discussion Draft, BEPS Action 1: Address the tax challenges of the digital economy, (Paris 2014).
16. OECD, ‘Taxation and Electronic Commerce. Implementing the Ottawa taxation framework conditions’ (Paris 2001).
17. M. Olbert and C. Spengel, ‘International Taxation in the Digital Economy: Challenge Accepted?’ [2017] World Tax Journal, Vol. 9, No. 1.
18. E. Oziewicz, ‘Globalizacja we współczesnej gospodarce światowej i jej skutki’ in E. Oziewicz (ed.), ‘Przemiany we współczesnej gospodarce światowej’ (Warsaw 2006).
19. I. Pietrzyk, ‘Globalizacja i regionalizacja gospodarki światowej, in: Gospodarka światowa w warunkach globalizacji i regionalizacji rynków’ (Warszawa 2009).
20. PwC, ‘Permanent Establishments 2.0. At the heart of the matter’, pwc.com/tax, accessed 19 April 2018.
21. A. Rhode, ‘Some (bad) news on the EU Digital Tax’, linkedin.com, accessed 15 June 2018.
22. T. Rosenbuj, ‘Taxing digital’ (Barcelona 2015).
23. A. A. Skaar, ‘Permanent Establishment: Erosion of a Tax Treaty Principle’ (Boston 1991).
24. P. Tang and H. Bussink, ‘EU Tax Revenue Loss from Google and Facebook’ [2017], https://paultang.pvda.nl/, accessed 19 April 2018.

ODR AND THE RULE OF THE INTERNET

Zukauskaite Migle[1]

Abstract

Legal community is still trying to tame alternative dispute resolution (ADR) and the concept of a neutral third party. However, there is already another, perhaps even wilder, beast out there. It has different names, it can take different forms: electronic Alternative Dispute Resolution (eADR), Online Dispute Resolution (ODR), Dispute System Design (DSD) just to name a few. We might be familiar with the idea of the fourth party – ODR being just another platform (video conference, chat room, e-mail) where traditional ADR procedure can take place. However, the Internet and technology are way further than we think. Our everyday shopping malls, such as eBay, Alibaba or Amazon, have implemented a wide variety of algorithms-based dispute resolution systems: blind bidding, drop-out list questionnaires, limited space answer boxes and others. Moreover, entire units are dedicated to finding solutions how to prevent these disputes before they even arise. These units are not working in the dark – thousands of claims are being submitted every day, giving them a huge amount of data needed to identify patterns and possible causes of problems. These platforms are not looking for justice. They are looking for peace. Preferably, together with a happy costumer, positive reviews and growing profits.

We, as a society, elect a parliament and grant it the legislative power, therefore, we are ready to obey the rules. However, online rules are not created by the legislature. They are created by IT personnel or even service users themselves. It is said that the rule of law can only exist over a defined territory, but if we cannot define the territory of the Internet, is there a place for law? Or is it now just the rule of the Internet?

Keywords: ADR, ODR, dispute resolution, the internet

Introduction

As rightly suggested by E. Katsh and C. Rule, there is a simple matrix: 'The number of disputes increases whenever transactions and relationships increase.'[2] The Internet has managed to raise both. Various text, speech or video-based applications have diminished the hurdle of distance in people's communication, while e-commerce has elevated the volume of B2C transactions to the levels which would have been unimaginable in offline world. Hence, when the Internet, together with laptops, tablets and smartphones, gained momentum, it not only enabled its users to communicate and enter into contracts from almost everywhere and anytime. It as well opened the doors to millions[3] small value disputes. If all of these disputes reached the courts, every judicial system would simply crash. Moreover, the Internet is not subject to the jurisdiction any sole sovereign entity[4], therefore, choosing the right redress mechanism become a huge burden for consumer.

The market was quick to provide a solution – first private ODR schemes were introduced as early as 1996, just several years later after the Internet has been fully opened to the general public[5]. ODR systems offered a number of ways to deal with low-value high-volume claims. Even though, during the

1 PhD candidate in Vilnius University, Faculty of Law. Topic of the dissertation: 'Mediator as a Facilitator in Dispute Resolution'. Scientific guest in Max Planck Institute Luxembourg, trainer for mediators with Hunt ADR, Ltd, UK., teaching at Vilnius University.

[2] E. Katsh and C. Rule, 'What We Know and Need to Know about Online Dispute Resolution' [2016] S. C. L. Rev 67 (2) p. 340.

[3] eBay and PayPal dispute resolution centres are handling approximately 60 million disputes annually. See: A. H. Raymond and S. J. Shackelford, 'Technology, Ethics, and Access to Justice: Should an Algorithm be Deciding Your Case?' [2014] Mich. J. Intern'l L 35 (3) pp. 491-492.

[4] S. K. Bharadwaj H., 'A Comparative Analysis of Online Dispute Resolution Platforms' [2017] AJOLIS 2 (3) p. 84.

[5] O. Rabinovich-Einy and E. Katsh, 'A New Relationship between Public and Private Dispute Resolution: Lessons from Online Dispute Resolution' [2017] Ohio St. J. on Disp. Resol. 32 p. 711.

first ten years many of these ODR websites have come and gone because of cost related issues[6], contemporary ODR providers are using more and more automated systems[7], which require non or very little human intervention, and thus, lower the costs of maintenance. Not surprisingly, many governmental and non-governmental organisations see ODR as a way to broaden access to justice, especially in the setting of B2C relationship[8]. It gives a ground to believe that ODR is here to stay.

1. The rule of the Internet

Modern ODR systems are usually established on two bases: as a part of self-contained platform or as a full-service platform[9]. The first type is dedicated to resolving disputes within a community, such as eBay or AirBnB. The users of the platform normally agree and are bound by the platform's terms and conditions. Another typical feature of such platforms is that the owner works as an intermediary between service provider and the buyer, therefore, is willing to satisfy the interests of both. However, it is hard to state that these platforms are completely unbiased or impartial. Moreover, they have effective enforcement mechanisms, for example suspending accounts, posting negative feedback or freezing payments, which gives them a huge power over its customers. The second type is usually offering a full spectrum of services open to everybody. They might be designated for a certain type of disputes or accommodate various types as long as they can be resolved by a settlement. Such platforms usually work independently from service providers and can be operated by both, private and government bodies.

To our liking, ODR systems are able to effectively solve millions of disputes safeguarding court systems from a flood of low-value high-volume claims. However, some authors emphasize that all private ODR providers are the creatures of a contract and therefore, remains largely unregulated[10]. This is not exactly true. Every 'if' on the Internet has its 'then'. Thus, while they might not be regulated by the rules of law, they are widely regulated by the rules of the Internet. The questions then are, who and how are creating them.

1.1. From the fourth to the third party

It is common to refer to ODR as a fourth party to a dispute, considering human intermediary (be it an evaluator, mediator, arbitrator or mock jury) as a third. Taking into account that in the beginning ODR was no more than regular ADR procedure conducted using some communication tools (e-mail, phone, video conferencing or even holograms), such reference to the fourth party was reasonable. However, both, ODR and IT technologies has progressed immensely from the time they were created and now are as close to their ancestors as online gaming is to board games[11].

Definitions of ODR have been changing accordingly. While in the beginning they were mainly related to 'communication at a distance' technologies enabling ADR procedures to be conducted in other than face-to-face environment[12], current articles provide a more complex definition. Some strongly argue

[6] A. H. Raymond and S. J. Shackelford, 'Technology, Ethics, and Access to Justice: Should an Algorithm be Deciding Your Case?' [2014] Mich. J. Int'l L 35 (3) p. 514.

[7] A. H. Raymond and S. J. Shackelford, *Ibid*.

[8] See: Civil Justice Council, Online Dispute Resolution for Low Value Civil Claims [e-version] [2015] accessed 19 April 2018. Accessible via the internet at: https://www.judiciary.gov.uk/reviews/online-dispute-resolution/, p. 2; European Commission Communication COM(2010)245 'A Digital Agenda for Europe' [2010], http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245&from=EN, accessed 20 April 2018, p. 13; ABA, A Report on the Future of the Legal Services in the United States: Executive Summary [e-version]. [2016] accessed 19 April 2018. Accessible via the internet at: http://abafuturesreport.com/, p. 5.

[9] A. H. Raymond and S. J. Shackelford, *Ibid*., p. 501.

[10] A. H. Raymond and S. J. Shackelford, *Ibid*., p. 501.

[11] E. Katsh and C. Rule, 'What We Know and Need to Know about Online Dispute Resolution' [2016] S.C. L. Rev. 67 (2) p. 330.

[12] For example: as 'any mediation, arbitration or dispute resolution that takes place outside of court and at least partially online' in J. Krause, 'Settling It On the Web' [2007] ABA Journal, http://www.abajournal.com/magazine/article/settling_it_on_the_web, accessed 19 April 2018, as 'the use of information technology particularly the Internet, in the conduct of alternative dispute resolution processes' in Y. Farah, 'Critical analysis of online dispute resolutions: the optimist, the realist and the bewildered' [2005] C.T.L.R. 11 (4) p. 123; as 'forms of dispute resolution, such as negotiation, mediation, and arbitration, which are offered on the Internet and are conducted through written digital communications' in O. Rabinovich Einy, 'Technology's Impact: The Quest for a New Paradigm for Accountability in Mediation' [2006] Harv. Negot. L. Rev 11 p. 255.

that neither the mere use of technology in the already existing judicial systems, nor technology created solely to facilitate the document receipt, search or storage, nor stand-alone online communication software allowing parties to voice complaints amount to ODR[13]. Others have come up with significantly wider term stating that ODR is the application of information and communications technology not only to the resolution of disputes, but as well to their prevention and management[14].

The former definition is the closest to today's reality, as it takes into account that a dispute can be resolved by a system in its entirety, while not abandoning traditional ADR tools being transferred to online world. Lots of platforms are now using a mix of both: automated ODR systems as well as human intermediaries conducting ADR online. They start the procedure with an assisted negotiation involving just the software and the parties and transfer the dispute (or a part of it) to an online mediation or adjudication only when parties reach a dead end in their assisted negotiation. However, many disputes nowadays are resolved in the first (software based) phase without any human intervention. This explains why it is important to exclude mandatory human assistance from the definition of ODR. It as well explains why in some cases ODR no longer plays a role of a fourth but rather of a third party.

1.2. How automated ODR systems work?

The software used in these automated ODR systems is usually driven by three types of algorithms: rule-based, case-based or genetic models[15]. The first one is encoded taking into account a set of rules (for example, legal acts) and teaching an algorithm to apply these rules. The second one is based on the assumption that similar solutions applied to similar problems in a similar context will lead to similar and predictable outcomes[16]. These cookie-cutter cases[17] are highly common in disputes emerging from e-commerce transactions. As most of these online communications leave a 'digital trail', which allows collecting data, it is relatively easy to create a database of cases and apply algorithms of the second type in online environment. However, both, the first and the second types are highly sensitive to changes of rules or laws, which can render the whole code or database useless[18]. The third type is based on a genetic model, which allows parties to determine their interests assigning numeric value to them and then, using methods of crossover, heredity and mutation design possible solutions, which would best fit the needs of both parties[19]. Modern ODR systems normally rely on a mixture of these algorithms in a form of assisted negotiation, usually starting with rule-based models requiring answers to simple yes and no questions, which are then used to define if a disputant is eligible to using the system. They are followed by brainstorming solutions taking into account prior cases on the database or fitness of the solution to both parties by the numeric value that was assigned to them.

1.3. Capabilities of automated ODR systems

Main functions of an intermediary, especially in mediation, can be described as calming down the parties, helping them to clarify their interests, identify options and brainstorm possible solutions. Fully automated ODR systems are now capable of all of them. Firstly, asynchronous nature of the communication gives parties time to think and vent emotions before entering the answer; message drafts provided on the system prevent parties from using offensive language; not having to see the other party reduces the threat of rising levels of frustration and intimidation; online environment allows parties to be assisted by their beloved ones or lawyers and consequentially feel more confident and relaxed. Secondly, it becomes easier to clarify interests using drop-down list questioners[20], which are usually based on

[13] A. H. Raymond and S. J. Shackelford, *Ibid*., p. 500.
[14] E. Katsh and C. Rule, *Ibid*., p. 329.
[15] D. Carneiro, et al., 'Using genetic algorithms to create solutions for conflict resolution' [2013] Neurocomputing 109 p. 16, 17.
[16] For example, http://cybersettle.com/ blind-bidding system.
[17] M. A. Bulinski and J. J. Presco, 'Online Case Resolution Systems: Enhancing Access, Fairness, Accuracy, and Efficiency' [2016] Mich. J. Race & L. 21 (2) p. 208.
[18] D. Carneiro, *et al*., *Ibid*., p. 17.
[19] D. Carneiro, *et al*, *Ibid*., p. 18.
[20] Such questioners normally have 'other' as a choice allowing to submit an answer in one's own words if need be.

experience of prior disputes of that type in the database; limited space answer boxes require a person to think through their reply in order to communicate what is really important; assigning a numeric value to certain identified interest helps parties prioritize, while visual graphs and reports of their answers gives a possibility to double check[21]. Thirdly, optimization algorithms can create different bundles representing party's positions, assisting in this way with identification of options, which can remain private to the party[22]. Lastly, automated systems can help brainstorm by suggesting models that worked on prior cases or creating an updated version of parties' proposals by merging several of them.

On top of the functions that automated ODR systems are able to mimic from traditional ADR, there is another important function that is not attributable to human intermediaries: prevention. First of all, data processing tools are able to find patterns of the disputes and identify their causes, which can then lead to further improvements of the website[23], especially if it is a self-contained platform, dealing with disputes inside a specific community[24]. Moreover, in order to manage expectations and provide parties a possibility to make an informed decision before submitting a claim, ODR systems are offering a 'solution explorer' phase. This phase might consist of relevant (legal) information presented in comprehensible manner or a list of options to try before engaging into the resolution phase, such as providing mail drafts for contacting another party directly[25].

1.4. Threats posed by ODR

Having the advantages of traditional ADR procedures, ODR adds speed, efficiency and the comfort of home setting on top of that. It can as well offer solutions that human intermediaries are not capable of. However, all that comes for a price. Automated ODR systems lack transparency, legal reasoning and ability to see the wider picture of the dispute.

It is a common metaphor to compare automated ODR systems with black boxes, emphasizing that parties can only see the input and the output, and not the process or motives why certain result was reached. If the solution proposed by automated ODR system is of advisory nature and in all cases require the consent of the parties to settle the dispute in a suggested way, it is not that big of a problem. However, many self-contained ODR systems issue decisions and, as mentioned above, have effective means to enforce them without delay. Such situation raises concerns related to justice and legality of the final outcome. The reasons for that are numerous. Firstly, the majority of algorithms they use are programmed by IT experts, who are not necessarily experts in law, let alone consumer rights. This problem is even bigger taken into account, that giant platforms can reach consumers in various jurisdictions, possibly applying different legal standards. Secondly, case-based or rule-based algorithms can only take into account what was a priori specified by the developer. This might omit important details from information on which the decision is based, leading to distorted outcomes. Thirdly, platforms, as private bodies, can have an agenda of their own. In majority of cases it is not justice, but rather growing profits or speedy procedure. A research conducted by eBay has shown that the costumer who is less likely to use the platform again is not the one losing the dispute, but the one whose dispute resolution process lasted several weeks[26]. The easiest way to expeditated the procedure is to exclude human component. However, this can lead to ridiculous outcomes, such as the infamous case of PayPal requiring a buyer to destroy a $2,500 worth violin in order to get his money back, while leaving the seller without the money and the violin[27].

Even though automated ODR systems, especially self-contained platforms, pose a number of threats, taken into account the number of low-value disputes they resolve every year, it would be

[21] For example, Smartsettle. See: O. Rabinovich-Einy and E. Katsh, 'A New Relationship between Public and Private Dispute Resolution: Lessons from Online Dispute Resolution' [2017] Ohio St. J. on Disp. Resol. 32 p. 714.
[22] A. H. Raymond and S. J. Shackelford, *Ibid*., pp. 515-516.
[23] O. Rabinovich-Einy and E. Katsh, *Ibid*., pp. 714, 721.
[24] Types of ODR service providers are discussed further in the article.
[25] For example, https://civilresolutionbc.ca/how-the-crt-works/getting-started/small-claims-solution-explorer/.
[26] E. Katsh and C. Rule, *Ibid*., p. 335.
[27] See: https://www.cbsnews.com/news/paypal-makes-ebay-customer-destroy-2500-violin-seller-left-empty-handed/.

unreasonable to prevent these platforms from operating ODR systems, as this significantly alleviates the backlog of cases in courts. However, there has to be some standards that could ensure that the main goal of such systems is just outcome, which among others, takes into account consumer rights. While the code of algorithms solving disputes on self-contained ODR platforms can amount to trade secret and no profit oriented giant marketplace would be willing to open the black box and reveal all the details of the resolution process, governments and international actors should look for ways to guarantee that the parties to the dispute are able to require recourse to human homologation of a dissatisfactory outcome reached by an automated ODR system.

2. ODR and the Rule of Law

On international (or supranational) level only two documents could be found that are at least partially regulating the use of ODR in dispute resolution[28]. It is UNCITRAL's Technical Notes on Online Dispute Resolution[29] and EU regulation on consumer ODR. Thankfully, more and more national or regional governmental authorities are taking steps in order to assure that their citizens are able to benefit from just, speedy and comfortable dispute resolution. Both international documents together with several attempts on national level will be concisely discussed below.

2.1. EU regulation on consumer ODR

EU is in large part based on the idea of the single market. However, growing numbers of e-commerce transactions[30] added some new undertones to this idea, namely enlarging it to the digital dimension[31]. In 2010 it was indicated in the Digital Agenda for Europe that commercial content could flow across borders if (amongst others) dispute resolution was facilitated and costumer trust established[32]. Not long after, in 2013 two interlinked and complementary legislative instruments were introduced: Directive on consumer ADR[33] and Regulation on consumer ODR[34]. The latter was supposed to ensure that consumers would have access to simple, efficient, fast and low-cost ways of resolving disputes which arise from the sale of goods or the supply of services online[35].

Regulation on consumer ODR established a web-based platform, fully operated by the Commission, serving as a free of charge single point of entry for all consumers[36] facing a dispute which has arisen from cross-border or domestic online transaction. However, it has to be emphasized that the platform itself does not solve the disputes: it provides an electronic complaint form, informs the respondent party, transmits the claim to an identified competent ADR entity and offers other administrative functions, which, as discussed above, as a stand-alone practice cannot be attributed to ODR. The same could be said about ODR contact points in the Member states, as their main function is related to facilitation of the communication between the parties and ADR authority. Moreover, Regulation on consumer ODR neither provides a definition of what could be considered as ODR, nor describes exact procedure how ODR should be conducted. The only explicit procedure-related requirement for ADR entities, which are handling the dispute, is to reassure that resolution process will not require the physical presence of the parties.

[28] European Parliament and Council Regulation (EU) 524/201 on online dispute resolution for consumer disputes [2013] OJ L165/1 (Regulation on consumer ODR).

[29] UNCITRAL 'Technical Notes on Online Dispute Resolution' (New York: United Nations 2017), http://www.uncitral.org/pdf/english/texts/odr/V1700382_English_Technical_Notes_on_ODR.pdf, accessed 20 April 2018.

[30] In 2016 66 % of EU population was buying online. See: European Commission, 'Use of Internet and e Privacy: Europe's Digital Progress Report 2017' [e-version] p. 5, https://ec.europa.eu/digital-single-market/en/download-scoreboard-reports.

[31] See: https://ec.europa.eu/digital-single-market/.

[32] European Commission Communication COM(2010)245 'A Digital Agenda for Europe' [2010], http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245&from=EN, p. 5, accessed 20 April 2018.

[33] European Parliament and Council Directive 2013/11/EU on alternative dispute resolution for consumer disputes (Directive on consumer ADR) [2013] OJ L165/53.

[34] European Parliament and Council Regulation (EU) 524/201 on online dispute resolution for consumer disputes [2013] OJ L165/1 (Regulation on consumer ODR).

[35] Regulation on consumer ODR, para. 2.

[36] Traders can initiate a resolution of a dispute against consumer, as long as the Member state where consumer is habitually resident allows for such disputes to be resolved via ADR.

However, it has a crucial benefit in the eyes of consumers – all ADR providers on the platform are subject to quality standards stated in the Directive on consumer ADR[37].

To sum up briefly, the implementation of Regulation on consumer ODR might have facilitated the access to fast consumer dispute resolution stemming from e-commerce transactions, however it did so through creating an online administrative body which enables consumers to easily find a credible ADR body which could resolve the dispute, leaving the actual world of ODR processes largely unregulated.

2.2. UNCITRAL Technical notes

UNCITRAL started to see ODR as a potential project for one of its working groups as early as 2000, however actual works on ODR procedural rules started only in 2010 after the proposal of American delegation. Initially the Working Group III was aiming to create several instruments: (1) procedural rules; (2) accreditation standards, and minimum requirements for ODR providers and platforms; (3) guidelines and minimum requirements for ODR neutrals; (4) principles for resolving ODR disputes; and (5) a cross-border enforcement mechanism[38]. However, after 5 years drafters of the instrument were still not able to agree on the set of rules and therefore, Commission ordered to change the work towards a non-binding descriptive document, reflecting elements of an online dispute resolution process and finish the work in one-year time, regardless if the outcome is reached or not[39]. UNCITRAL Technical Notes on Online Dispute Resolution[40] is the outcome of this process. As noticed by M. Stegner, after several years of effort, UNCITRAL could only agree upon non-binding guidelines, summarizing already well-known principles. She further notes that the result achieved was not satisfactory[41]. It is hard to disagree.

Firstly, as noted above, the principles established in the document, such as fairness, transparency (in a sense of disclosing any relationship between the ODR administrator and particular vendor), independence (in a sense of avoiding conflicts of interests) and due process have been recognized in ADR society for decades[42]. Technical Notes failed to elaborate further on how these principles could be applied in purely online setting where a dispute is entirely (or in a big part) resolved by an algorithm rather than a human.

Secondly, UNCITRAL document suggests using and ODR platform – a technology-based intermediary that could be able to generate, send, receive or otherwise process communications, which is similar to the one, established in the EU. However, the former, as opposed to the latter, is a requirement for every ODR provider. Even though it is of high importance for proper functioning of ODR systems, that such administrative functions as sending and receiving of documents could be performed online, ODR platform in the sense of UNCITRAL document is nowhere close to EU ODR platform. The biggest disadvantage compared to the latter, is that these private platforms will not be able to assure a certain level of quality, whereas, as discussed above, on the EU ODR platform disputes could only be transmitted to registered ADR authorities fulfilling the requirements of the Directive on consumer ADR. On the other hand, one has to admit that this was not the purpose of the provision.

Lastly, Technical Notes take a big step forward and try to describe an ODR procedure. The procedure consists of the three-steps dispute resolution model comprising assisted negotiation, facilitated settlement and final stage. While first one does not require human intervention allowing parties to communicate via the platform, the second, starting if the prior state was not successful or was intentionally skipped, should include a neutral person facilitating the dispute. Technical Notes do not provide any examples or explanation what this third stage should consist of, as the drafting parties could not agree on

[37] European Parliament and Council Regulation (EU) 524/201 on online dispute resolution for consumer disputes [2013] OJ L165/1 (Regulation on consumer ODR) art. 4(i).

[38] A. H. Raymond and S. J. Shackelford, *Ibid*., p. 510.

[39] M. Stegner, 'Online Dispute Resolution: The Future of Consumer Dispute Resolution' [2017] 5 Y.B. on Int'l Arb. p. 358.

[40] UNCITRAL, 'Technical Notes on Online Dispute Resolution' (New York: United Nations 2017) http://www.uncitral.org/pdf/english/texts/odr/V1700382_English_Technical_Notes_on_ODR.pdf, accessed 20 April 2018.

[41] M. Stegner, *Ibid*., p. 360.

[42] For example, European Commission Justice Directorate, 'European Code of Conduct for Mediators' [2004] http://ec.europa.eu/civiljustice/adr/adr_ec_code_conduct_en.pdf, accessed 20 April 2018, art. 2; 3.

that during the years of deliberations[43]. Taking into account the operation model of several examples of existing ODR providers[44], the most reasonable guess would be adjudication type proceedings ensuring that the resolution will have a definite outcome. However, such three-phased model is already widely used[45], and does not create almost any additional value in practice, except from being an example to consider when setting up a new ODR business.

On the other hand, Technical Notes has its advantages. Firstly, it offers a wider scope of application. Even though these guidelines are as well intended for use in disputes arising from cross-border low-value sales or service contracts concluded using electronic communications, they could be applied not only in B2C, but as well in B2B relationships. Secondly, it sums up some other good practice, such as suggesting being guided by the code of ethics, describes a procedure of administration of claims via the ODR platform and establishes, that all communications should be able to take place and be stored entirely online.

To summarize, Technical notes were trying to target it all, however, lack of consensus on difficult (and important) matters, descriptive and non-binding nature precluded the drafters from taking everything into account profoundly. Indeed, as stated in the Technical Notes, these guidelines were not intended to be exhaustive or exclusive, nor are they suitable to be used as rules for any ODR proceeding[46]. It is as well stated that the purpose of the Technical Notes is to foster the development of ODR and to assist ODR administrators, ODR platforms, neutrals, and the parties to ODR proceedings. However, these statements only make it harder to find areas of practical application of the guidelines, other than being a starting point for further considerations.

2.3. National ODR schemes

Even though ODR has a huge potential to reduce the backlog of cases and, possibly, expenses of court systems, not that many countries have dared to introduce it in public level. Majority of those who did developed projects on regional level and only in particular types of disputes. However, some have already started applying ODR schemes in a wider scope.

Good intentions of the UK. Money Claim Online[47] scheme was introduced under the Practice Direction 7E supplementing Civil Procedure Rules[48]. It provides an online scheme to claim for a specified amount of money under £100,000 against a single defendant (or two, if the amount is specified for both), who has an address within England and Wales. However, it is hard to call it a resolution scheme, as a claimant can only request the court to order the defendant to pay if he or she has admitted owing the money or has not responded to the claim. In all other cases parties would have to go to court or turn to ADR. Therefore, Money Claim Online is not much of a help where there actually is a dispute.

However, UK has to be praised for its attempts to form the Online Court intended for simple low-value disputes, not requiring a lawyer. Several reports[49] where suggesting creating a three-tier system including interactive triage (providing an early evaluation of a dispute), assisted online facilitation (provided partly by automated systems and human neutrals) and online judgement (binding and enforceable, provided by members of the judiciary). However, the adoption of Prisons and Courts Bill[50], which would have laid the legal background for such developments, was abandoned due to the threat of

[43] M. Stegner, *Ibid*., p. 359.
[44] For example, Rehtwijzer 2.0 or Civil Resolution Tribunal in British Columbia.
[45] For example, SquareTrade.
[46] UNCITRAL, 'Technical Notes on Online Dispute Resolution' (New York: United Nations 2017) http://www.uncitral.org/pdf/english/texts/odr/V1700382_English_Technical_Notes_on_ODR.pdf, accessed 20 April 2018, art. 6.
[47] See: https://www.gov.uk/make-money-claim.
[48] UK Civil procedure rules, Practice direction 7E, http://www.justice.gov.uk/courts/procedure-rules/civil/rules/part07/pd_part07e, accessed 20 April 2018.
[49] See: Civil Justice Council, Online Dispute Resolution for Low Value Civil Claims [2015] p. 6, https://www.judiciary.gov.uk/reviews/online-dispute-resolution/, accessed 20 April 2018,; Lord Justice Briggs, 'The final report of Civil Courts Structure Review' [2016] pp. 58-60, https://www.judiciary.gov.uk/publications/civil-courts-structure-review-final-report/, accessed 20 April 2018.
[50] UK Public Bill Committee, Prisons and Courts Bill 170 [2017], https://publications.parliament.uk/pa/bills/cbill/2016-2017/0170/17170.pdf, accessed 20 April 2018.

early parliamentary general election in UK in 2017 and no new proposals on the subject have been made so far[51].

Pioneering Netherlands. Rechtwijzer 2.0[52] was first introduced in 2014 as a tool to help divorcing couples draft their settlement agreements. However, it has later expanded its services to disputes emanating from landlord-tenant, dismissal, consumer, debt restructuring and other cases. It was created for the Dutch Legal Aid Board with support of Dutch Ministry of Security and Justice. The website offers a wide range of ODR tools and automated features, such as drop-down questioners, offering message drafts or solutions used in prior similar cases, while at the same time giving the parties a possibility to tell their side of the story. It as well provides legal information relevant to the dispute at hand. Moreover, parties can always turn to experienced mediators or adjudicators to resolve difficult questions (in other words, this website as well offers a three-tier system). The settlement agreement, when reached, is reviewed by an expert to make sure that it will be legally valid. Being a platform operated by governmental institution it as well requires parties to authenticate their identities through e-identification system used by Dutch government. However, it has to be emphasized that people are using this website on voluntary basis and are under no obligation by the law to do so. Even without being mandatory, Rechtwijzer 2.0 could definitely be considered as one of the best outcomes of dispute systems design in the market today, especially in the public sector.

Legal reality in British Columbia (Canada). Based on the same software as Rechtwijzer 2.0, Civil Resolution Tribunal[53] was taken one step further by the amendments to Civil Resolution Tribunal Act[54]. As from June 1, 2017 people having disputes of $5000 and less are obliged to submit their claims through an online[55] Civil Resolution Tribunal[56]. In order not to prevent computer illiterate people from defending their rights and submitting claims, the provincial government offers front line support via phone, mail or in-person assistance[57]. However, with time this problem will vanish.

As well as platforms described above, the tribunal offers a three-tier system consisting of negotiation, facilitation and adjudication. Disputes stemming from debt or damages, recovery of personal property, opposing claims to personal or property demanding performance of an agreement about personal property or services can be submitted before it. Even though the negotiated consent or final decisions of the tribunal can be filed in the Provincial Court for enforcement, the party, dissatisfied with the decision of adjudicator can file a notice of objection in 28 days, which will make the decision unenforceable and transfer the dispute to the Provincial Court and de novo proceed with the litigation there.

The Civil Resolution Tribunal is an excellent example of ODR broadening access to justice and decreasing the case load of the courts, while at the same time neither infringing parties' right to a fair trial, nor preventing computer illiterate people from effective ways to solve their disputes. Being implemented in phases, Civil Resolution Tribunal is under a constant change and growth, therefore, we might soon witness bigger and more diverse claims being transferred to the jurisdiction of the tribunal. While it is still too soon to talk about practical down sides of such systems, the model of Civil Resolution Tribunal is something that every national government in developed countries should take into consideration.

Conclusions

Even though many still tend to see ODR as a way to have traditional ADR processes conducted through online communication, it is no longer entirely true. Algorithm-based fully automated ODR systems are now capable of resolving disputes without any intervention of human intermediary, in many cases

[51] See: https://services.parliament.uk/Bills/2016-17/prisonsandcourts.html.
[52] See: https://rechtwijzer.nl/.
[53] See: https://civilresolutionbc.ca/.
[54] British Columbia, Civil Resolution Tribunal Act [2012] SBC Chapter 25 as amended by
[55] However, the tribunal may hold an in-person hearing if the it considers that the nature of the dispute or that extraordinary circumstances make an in-person hearing necessary in the interests of justice.
[56] British Columbia, Civil Resolution Tribunal Act [2012] SBC Chapter 25, art. 3.1 (4); British Columbia, Civil Resolution Tribunal Small Claims Regulation [2017] B.C. Reg. 111/2017, art. 2.
[57] See: https://civilresolutionbc.ca/get-person-help-service-bc/.

outperforming their human counterparties. ODR is quick, effective, comfortable and able to significantly reduce the backlog of cases in courts; however, it poses a question if justice is not being a trade-off for such benefits. While full-service ODR systems usually offer a three-tier ODR scheme and a way to ensure that agreements reached are legally valid, they are more likely to be independent and impartial, hence, arriving to just solutions. However, it would be more difficult to come to such conclusion with regards to self-contained platforms. Such platforms have a lot of control over their community, especially through effective, in many cases monetary, enforcement mechanisms. Allowing them to solve consumer disputes with no or little regulation or at least human scrutiny, can pose serious problems to their customers, as history has already shown.

The legislation on the subject of ODR is still neither numerous, nor very informative. While governments are hesitating to make decisions or find a consensus, number of online disputes and private ODR bodies is growing. Setting quality standards for ODR providers and ensuring that a binding decision reached by automated ODR systems could be subject to appeal before a human intermediary, could raise the probability of just and legal outcomes reached by ODR systems. The sooner government bodies step in either by providing legal framework for private ODR providers or by offering an equally comfortable, however transparent ODR body with an easy way to enforce settlements or decisions, the more likely it is that internet users, including consumers and businesses, will be adequately protected. When some promising developments, such as EU ODR platform and Civil Resolution Tribunal in British Columbia, have already been introduced, it would be a pity not to take them as a good base to start with.

Bibliography

Legislation

1. British Columbia, Civil Resolution Tribunal Act [2012] SBC Chapter 25.
2. British Columbia, Civil Resolution Tribunal Small Claims Regulation [2017] B.C. Reg. 111/2017.
3. European Parliament and Council Directive (EU) 2013/11 on alternative dispute resolution for consumer disputes [2013] OJ L165/53 (Directive on consumer ADR).
4. European Parliament and Council Regulation (EU) 524/201 on online dispute resolution for consumer disputes [2013] OJ L165/1 (Regulation on consumer ODR);
5. UK Civil procedure rules, Practice direction 7E, http://www.justice.gov.uk/courts/procedure-rules/civil/rules/part07/pd_part07e, accessed 20 April 2018.

Articles

1. S. K. Bharadwaj, 'A Comparative Analysis of Online Dispute Resolution Platforms' [2017] AJOLIS 2 (3).
2. M. A. Bulinski and J. J. Presco, 'Online Case Resolution Systems: Enhancing Access, Fairness, Accuracy, and Efficiency' [2016] Mich. J. Race & L. 21 (2).
3. D. Carneiro, et al., 'Using genetic algorithms to create solutions for conflict resolution' [2013] Neurocomputing 109
4. Y. Farah, 'Critical analysis of online dispute resolutions: the optimist, the realist and the bewildered' [2005] C.T.L.R. 11 (4).
5. E. Katsh and C. Rule, 'What We Know and Need to Know about Online Dispute Resolution' [2016] S. C. L. Rev 67 (2).
6. O. Rabinovich Einy, 'Technology's Impact: The Quest for a New Paradigm for Accountability in Mediation' [2006] Harv. Negot. L. Rev 11.
7. O. Rabinovich-Einy and E. Katsh, 'A New Relationship between Public and Private Dispute Resolution: Lessons from Online Dispute Resolution' [2017] Ohio St. J. on Disp. Resol. 32.
8. A. H. Raymond and S. J. Shackelford, 'Technology, Ethics, and Access to Justice: Should an Algorithm be Deciding Your Case?' [2014] Mich. J. Intern'l L 35 (3).
9. M. Stegner, 'Online Dispute Resolution: The Future of Consumer Dispute Resolution' [2017] 5 Y.B. on Int'l Arb.

Other sources

1. ABA, A Report on the Future of the Legal Services in the United States: Executive Summary [2016], http://abafuturesreport.com/, accessed 20 April 2018.
2. Civil Justice Council, Online Dispute Resolution for Low Value Civil Claims [2015], https://www.judiciary.gov.uk/reviews/online-dispute-resolution/, accessed 20 April 2018.
3. European Commission Communication COM(2010)245 'A Digital Agenda for Europe' [2010], http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245&from=EN, accessed 20 April 2018.
4. European Commission Justice Directorate, 'European Code of Conduct for Mediators' [2004] http://ec.europa.eu/civiljustice/adr/adr_ec_code_conduct_en.pdf, accessed 20 April 2018.
5. European Commission, 'Use of Internet and e Privacy: Europe's Digital Progress Report 2017' [e-version], https://ec.europa.eu/digital-single-market/en/download-scoreboard-reports.
6. J. Krause, 'Settling It On the Web' [2007] ABA Journal, http://www.abajournal.com/magazine/article/settling_it_on_the_web, accessed 19 April 2018.
7. Lord Justice Briggs, 'The final report of Civil Courts Structure Review' [2016], https://www.judiciary.gov.uk/publications/civil-courts-structure-review-final-report/, accessed 20 April 2018.
8. UK Public Bill Committee, Prisons and Courts Bill 170 [2017], https://publications.parliament.uk/pa/bills/cbill/2016-2017/0170/17170.pdf, accessed 20 April 2018.
9. UNCITRAL, 'Technical Notes on Online Dispute Resolution' (New York: United Nations 2017) http://www.uncitral.org/pdf/english/texts/odr/V1700382_English_Technical_Notes_on_ODR.pdf, accessed 20 April 2018.

IMPACT OF CYBER TECHNOLOGIES ON THE MECHANISM OF COMMISSION OF OTHER CRIMES

Žukovaitė Inga[1]

Abstract

The purpose of the presentation is to unfold the importance of the use of cyber technologies on the mechanism of commission of other criminal acts and to show how this also impacts the qualification of acts. The presentation objectives: to highlight the potential points of contact between crimes against property and cyber crimes, explore the possibilities of qualifying criminal acts on the theoretical level and the problems in case law, provide proposals on the possibilities of establishing new properties of crime elements.

Cyber crimes, differently to crimes against property, are new generation crimes targeting an object existing on the electronic space. There are still discussions ongoing in the doctrine on the single definition and categories of the crime of this type. Cyber crimes may be classified into crimes when the computer is used as a supporting instrument (computer assisted crimes) and into computer focused crimes. One of the most common types of crimes on the electronic space – cyber-deception and theft means actions on the electronic space when financial valuables, e.g., banking card numbers, login passwords, personal data, are stolen or acquired through deceit. The fight against online crimes where payment instruments or their data are used is one of the priorities of the EU law enforcement. Practical examples show that electronic payment instruments or their data are often acquired, in particular, for the commission of crimes against property (e.g., seizure). When such crimes are being committed, electronic payment instruments and other data, which are not the subject-matter of crimes against property, are stolen together with another person's property and are later used for the commission of financial operations on the electronic space. That gives rise to controversial questions and problems pertaining to the legal assessment of criminal acts by concurrence and related to delimitation of the subject-matter which results in case law differences.

Considering the developments of new technologies on the electronic space, the presentation also explores the issue of legal assessment of such cases when the offender, making use of different remote computer control equipment (e.g., drones, robots), exerts the impact of violence on the victim thereby overcoming the victim's will to resist and facilitating access to the targeted property. The existence of such cases in practice makes reconsider whether the provisions of the present Criminal Code of the Republic of Lithuania are adequate for proper legal assessment of such situations and make proposals to the legislator concerning the introduction of new qualifying attributes in the elements of property crimes.

Keywords: cyber crime, IT developments, robbery, crime against property.

Introduction

New IT developments and never-ending progress makes us wonder how this phenomenon impacts crime, which is one of the most sensitive life areas of society. The effect of new technologies on crime, as one of the areas of social life, is beyond question – that necessitates a revision of descriptions of the constituent elements of criminal offences and an assessment of adequacy of legal regulation in response to social life developments, which is more and more seen as being equivalent a progressive use of information technologies with an unwitting and widespread move of financial life to the electronic space.

With improving information technologies and rapid transfer of business, financial and other activities to the electronic space, traditional crime is spreading to the electronic space. The number of such offences

[1] *PhD student, Department of Criminal Justice, Faculty of Law, Vilnius University, with a dissertation on "The he corpus delicti of the crime of robbery", the speaker carries out research in the area of property crimes at Vilnius University, explores the modalities of violent crimes and crimes against property.*

in Lithuania as well as worldwide is on the increase and is estimated to spread further. The case law deals with an increasing number of crimes committed through the use of computers, information systems or IT operation facilities, e.g. online fraud, manipulation of payment systems, information and data exchange in order to commit crimes (e.g. sale of stolen items), blackmail, etc.[2]

It should be noted that the existence of a new crime type – computer crimes – have long been discussed along with efforts to define a uniform notion of such crimes and find the relationship between these crimes and other criminal offences. Although reference to computer crimes most often implies everything what is related to crimes online, it should be noted that information technologies also impact the mechanism of commission of other crimes, which leads to new questions and legal challenges in unfolding the content of constituent elements of crime and in qualifying criminal offences in case law, poses difficulties to law-makers in reinforcing the constituent elements of criminal offences in law. Therefore, the development of new technologies is an obvious new challenge in the area of implementation of criminal law.

The impact of new technologies on the mechanism of commission of new crimes in general is a wide-ranging topic, therefore, this research overviews the main aspects related to the trends inherent in the mechanism of commission of crimes against property (thefts, robbery, fraud) in the context of progressive development of information technologies.

1. Outcome of progress in new technology developments: problem of the concept of electronic crimes

One of the most important outcomes resultant from the impact of new technology developments on crime and crime commission mechanism is the emergence of a new crime group referred to as electronic crimes. Electronic crimes are often described by different terms, which can be synonymous in certain cases: 'computer crime', 'computer-related crime', 'high-tech crime', however, the concept 'electronic crime' is more often used in legal literature. In the most general sense, electronic crimes can imply any unlawful activities where information technologies are used. The term of computer crimes has been, over time, replaced by the concept of electronic crime, which has also been established in law on the international level – in the 2001 Budapest Convention on Cybercrime, which was ratified in Lithuania by a law in 2004. [3] Irrespective of these developments, the absence of a uniform term and concept of these crimes in a challenge for the doctrine.

You can come across an opinion in the doctrine that a computer crime means the acts dangerous for the public as provided for by criminal law when the act targets computer information, meanwhile crimes which impact computer equipment and installations are attributed to crimes of a different type. That means that computer crimes include only the acts, which are referred to in separate sections of criminal laws and target computer information as an inherent object and subject-matter.

It should be noted that the role of information technologies in crime can be two-fold. First of all, computers or their networks can be used as an instrument to commit 'traditional' crimes. For example, such crimes as fraud, forgery, theft, money laundering, blackmail, sexual harassment and others have existed before the internet or computers. New information technologies simply allowed them to move to the digital space and have opened new methods and instruments to commit such crimes. Under such approach, conventional crimes, when committed in non-traditional ways by means of information technologies, may be considered as electronic crimes. On the other hand, computers or information systems not only can be means or instruments to commit crimes but also become the targets of crimes, such as hacking of computer systems, disruption of operations of information systems, spread of computer viruses, etc.

[2] Local authorities and transfrontier crime: proceedings: Enschede (Netherlands), 20-22 September 2001 / International Conference organised by the Congress of Local and Regional Authorities of Europe (CLRAE) of the Council of Europe, in co-operation with the City of Enschede, Netherlands and the Dutch Section of the Council of European Municipalities and Regions (CEMR) (Strasbourg: Council of Europe 2002) p. 43.

[3] Republic of Lithuania Law on the Ratification of the Convention on Cybercrime (Official Gazette, 2004, No. 36-1178).

Thus, an electronic crime can mean both traditional crimes and new-type violations (unauthorised access, etc.). Taking into account the role of information technologies, distinction is made between ordinary crimes committed by using computers and specific computer crimes.[4] Other authors point out that computer crimes may be classified into two groups: crimes involving interference with computer operations and crimes where computers are used as a necessary instrument.[5] Thus, a broader perception of electronic crimes prevails in the doctrine where such crimes include the acts dangerous for the public as provided for by criminal law when the act targets computer information or the acts were a computer is used as a crime instrument. Such offences include fraud where computers are used, copyright violations made through the use of computers.[6]

An analysis of these definitions reveals that the doctrine develops two concepts of electronic crimes: the first treats electronic crimes only as the crimes which relate to a safe processing of information (in the narrow sense), and the second – as all unlawful acts if their object was processing of electronic information and an offence has been committed as a result of such processing (also includes fraud committed by means of electronic payment instruments, unauthorised use of electronic payment networks of banks, use of software) (in the broad sense). Electronic crimes within the broadest meaning could include two groups of criminal offences – ordinary criminal offences committed on the electronic space and criminal offences relating to the dissemination of information with unlawful content on this space.[7]

An overview of the concept of electronic crimes shows that electronic crimes do not include such offences as, for example, computer theft, computer theft by robbery, etc. Such offences are not treated as electronic crimes, they are attributed to the group of property crimes due to the specifics of the subject-matter of the crime.

2. 'Old crimes and new instruments' – case law trends

The impact of the use of information technologies on 'old crimes' not only means a change in the crime commission mechanism but also a complexity inherent in the offence qualification – research of the case law shows that the classical constituent elements of property crimes (theft, fraud, robbery) are no longer adequate for a precise assessment of the dangerousness of the offence.

A research of the case law of the court of cassation of Lithuania developed after the entry into force of the 2000 Criminal Code of the Republic of Lithuania (hereinafter – the CC) shows the main trend – a considerable impact of the use of information technologies on the mechanism of commission of property crimes, which is related to the specifics of the criminal offence of fraud. Moreover, the spreading use of information technologies made the case law reconsider the concept of theft and robbery when it was exposed to situations where electronic payment instruments, data of such instruments, etc. were obtained as a result of thefts or robbery.

The elements of crime most common in case law are the acts of an unlawful acquisition, storage, transfer or disposal of another person's electronic payment instrument and an unlawful initiation or performance of a financial operation by means of another person's electronic payment instrument. Unlawful acquisition of electronic payment instruments or their data has been criminalised in Article 214 and the use of such instrument or data – in Article 215 of Chapter XXXII 'Crimes and Misdemeanours against the Financial System' of the CC. It may be stated that the act provided for in Article 214 of the CC is one of the types of electronic identify theft. [8] Examples from case law show that electronic payment

[4] V. Kalpokas, 'Nusikaltimai elektroninėje erdvėje: kriminologinės sampratos dilemos [Crimes on the Electronic Space: Criminological Concept Dilemmas]' [2009] Teisės problemos, No. 1 (63), p. 79.

[5] D. Sauliūnas, 'Informacinių technologijų teisė' [Law of Information Technologies] NVO Teisės institutas (Vilnius 2004) p. 509.

[6] M. Kiškis, R. Petrauskas, I. Rotimskis and D. Štitilis, 'Teisės informatika ir informatikos teisė [Law IT and IT Law]' (Vilnius: Mykolas Romeris University 2006) pp. 230-263.

[7] R. Marcinauskaitė, 'Nusikalstamomis veikomis elektroninėje erdvėje pažeidžiamos pagrindinės baudžiamojo įstatymo saugomos vertybės nustatymo problema [The Problems of Identification of the Main Object of Cyber Offences].' (Mykolas Romeris University 2011) Social Science Studies, No. 3 (3), pp. 897-941.

[8] D. Štitilis, P. Pakutinskas, M. Laurinaitis and I. Dauparaitė, Inga, 'Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai [Online Identity Theft: Social, E. Business and Legal Regulation Aspects]' (Mykolas Romeris University 2011) pp. 250-255.

instruments or their data are often obtained, in particular, during crimes against property (e.g., robbery, theft). They can also be obtained through deceit; at times, there is no indication of a specific way of unlawful acquisition in court decisions.

It should be noted that the initial wording of Article 214 of the CC contained the following constituents of criminal offence elements – seized or otherwise acquired. These constituents were interpreted as meaning the actions by which persons get a false, forged or another person's payment instrument or equipment, computer application or another means designated or adapted for the production or false, forged payment instruments or their parts or for forging genuine payment instruments. Such actions include buying, barter, getting as a gift, finding, etc. Seizure of another person's payment instrument means obtaining it by way of a theft or robbery. Another person's payment instrument can also be unlawfully obtained through property extortion, deceit or in another unlawful way[9].

Reference to seizure as a constituent element in the law has led to a conflict of legislative provisions because the same constituent elements existed in the elements of theft and robbery. This issue was addressed in the case law by laying down the rule of qualification of acts, which requires to qualify a seizure of an electronic payment card together with other assets separately only under Article 214 of the CC.[10]

The elements of Article 214 of the CC, however, have been changed by the legislator. Seizure as a constituent element has been removed from the wording of this Article as currently in force and approved on 21 July 2007 and only unlawful acquisition as a constituent element remains. This has brought about the issue concerning the qualification of offences when an electronic payment instrument is seized by theft or robbery. After seizure as a constituent element has been removed from Article 214 of the CC, should seizure of an electronic payment card be assessed under other Articles of the CC (Articles 178 and 180 of the CC) or should the constituent element 'unlawful acquisition' as provided for in Article 214 of the CC be interpreted more extensively as including the acts of seizure. The answer to this question has been provided in the case law of the court of cassation with reference to different subject-matters of the criminal offence rather than the character of the offence.

The subject-matter of seizure provided for in the CC is closest to the subject-matter of theft – 'another person's property' (Article 178(1)).[11] When the concept of property is interpreted in crimes against property, it should be taken into consideration that this concept is a category of civil law.[12] Following Article 4.38 of the Civil Code, things and other property is an object of ownership. The word 'other property' used in this Article includes ownership rights, which are not tangible things but have a value and may participate in circulation, for example, the right of claim by a bank to repay a loan. [13] The concept of property in terms of theft and robbery, however, is narrower because property, as the subject-matter of crimes, has to belong to another person, have an economic value and movability.

It was noted in the works of researchers as early as in 2004 that there is no clear position in the doctrine how to treat the seizure of bank payment cards when it is assumed that a personalised card has no economic value on its own and, for this reason, has no characteristics of property.[14] Payment cards as such have no autonomous monetary value,[15] they are only an instrument enabling the use of funds held

[9] Resolution No. 55 of 29 December 2005 of the Senate of the Supreme Court of Lithuania regarding the case law in criminal cases related to criminal acts against the financial system (Articles 214, 215, 219, 220, 221, 222, 223 of the CC).

[10] Resolution No. 55 of 29 December 2005 of the Senate of the Supreme Court of Lithuania regarding the case law in criminal cases related to criminal acts against the financial system (Articles 214, 215, 219, 220, 221, 222, 223 of the CC).

[11] O. Fedosiukas, 'Turtinė nauda kaip nusikalstamos veikos dalykas: sisteminė normų analizė [Property Gain as a Subject-Matter of Crime: Methodical Analysis of Norms]' [2004] Jurisprudencija, T. 60 (52), p. 84; Resolution No. 52 of 23 June 2005 of the Senate of the Supreme Court of Lithuania 'Regarding the case law in criminal cases of theft and robbery'. Case Law. [2005] No. 23. Vilnius, p. 3.

[12] Subject-matter in robbery is not of blanket nature, therefore, civil law norms are only referred to as examples. Taking into consideration of the interpretation of blanket provisions in the doctrine, e.g. P. Švedas, 'Blanketinės dispozicijos Lietuvos Respublikos baudžiamajame kodekse [Blanket Dispositions in the Criminal Code of the Republic of Lithuania]' [2010] Teisė, 77, the disposition of robbery is not blanket.

[13] E. Baranauskas, I. Karulaityté-Kvainauskiené, J. Kiršiené, V. Pakalniškis, et al, 'Civil Law. General Part.' (Vilnius: Mykolas Romeris University 2007) p. 99.

[14] O. Fedosiukas, 'Turtinė nauda kaip nusikalstamos veikos dalykas: sisteminė normų analizė [Property Gain as a Subject-Matter of Crime: Methodical Analysis of Norms]' [2004] Jurisprudencija, T. 60 (52), p. 87.

[15] O. Fedosiukas, 'Turtinė nauda kaip nusikalstamos veikos dalykas: sisteminė normų analizė [Property Gain as a Subject-Matter of Crime: Methodical Analysis of Norms]' [2004] Jurisprudencija, T. 60 (52), p. 85.

in the account. For this reason, robbery offences when handbags, wallets or other items with electronic payment cards are seized should be also qualified under Article 214 of the CC. Thus, one of the proposals was to assess such offences separately under Article 214 of the CC and treat the offences when cards are seized during such robbery together with other things as concurrence. Such idea has seemingly took its root in the case law and the courts, when hearing cases, express the position that bank payment cards are not the subject-matter of crimes against property. On the other hand, an analysis of case law shows that courts do not always consistently maintain this position when qualifying criminal offences in their case law.

A research of the case law of the court of cassation shows that there are still cases when electronic payment cards are erroneously attributed to the subject-matter of robbery, their value is estimated and the offence does not undergo additional qualification under Article 214 of the CC. Such cases most often happen when handbags or wallets with all belongings held therein are seized from victims during robberies – all things, including bank payment cards, social security certificates, drivers licences are erroneously considered as the subject-matter of robbery when estimating their material value[16]; or during large-scale robberies when a large number of things is seized, including payment cards (also in case of minors, who are not subjects when cards are seized apart from other things) and they are attributed to the things as a whole and their value without going into details in the charges.[17] In the case law of more recent years we can also come across such erroneous examples where both bank cards and, for example, car documents, are considered as the subject-matter of robbery and their manufacturing value is included into the amount of the subject-matter of robbery.[18] Case law examples prove that the approach to such items as bank payment cards obtained through robbery is not consistent – in some cases, the robbery of things is assessed separately and excludes the subject-matter of robbery, e.g., cassation rulings No. 2K-470/2010, 2K-222/2010, 2K-30/2013, 2K-181/2013, while in other cases, they are included into the total value of the property seized through robbery, for example, cassation rulings No. 2K-117/2010, 2K-225/2012, 2K-274/2013. Such legal approach is incorrect. It is advisable that it would be most accurate to treat such situations as the concurrence of theft or robbery and of the criminal offence provided for in Article 214 of the CC.

Use of electronic payment cards after their unlawful acquisition is inextricably linked with the criminal offence of fraud.[19] Technological revolution has increased opportunities for crimes against property, in particular, fraud. As authors note, the offences of this type become in particular relevant with rapid improvements of information technologies and their spread in the area of finance. Online and mobile banking, payments by payment cards, online stores allow forecasting that the number of criminal offences of this type will be increasing in future.[20] The electronic space opens vast avenues for the commission of crimes of this type.

It can be said that the assessment and qualification of the use of electronic payment cards and their data, for example, in order to acquire money from the bank, has changed the relationship between the offences of theft and fraud and expanded the concept of fraud. That is the result of the impact of electronic technologies on the mechanism of crime commission. Such method of appropriating money from the bank by means of electronic payment cards may no longer be regarded as merely the theft of money and should be treated as fraud. Such approach did not establish itself among lawyers from the very beginning and a move to it has been made only with the knowledge and understanding of the change that has taken place in banking when the classical banking has been replaced by electronic where all operations are processed by man-made computer applications. Here banking operations are made by the electronic system where the person is identified according to the code, therefore, if the code is entered

[16] Ruling of the Supreme Court of Lithuania in criminal case No 2K-174/2009.
[17] Ruling of 17 February 2009 of the Supreme Court of Lithuania in criminal case No 2K-63/2009.
[18] Ruling of 25 September 2012 of the Supreme Court of Lithuania in criminal case No 403/2012.
[19] Order the Prosecutor General of the Republic of Lithuania regarding the methodological recommendations for the investigation of online scams (telephone scams) and the qualification of criminal offences, 10 February 2014, No. I-37.
[20] A. Piesliakas, 'Veikų dėl neteisėto disponavimo svetima elektronine mokėjimo priemone (BK 214 ir 215 straipsniai) kvalifikavimo problemos [Qualification Problems of the Crimes of Illegal Disposal of a Non-Cash Payment Instrument]' [2007] Mokslo darbai, Jurisprudencija 8 (98), pp. 71-80.

and a command is given by the person without authorisation to carry out transactions with the money held in the account, he presents himself as another person who has such authorisation to the operational system or to the bank and thereby misleads the electronic system and the bank.[21] All these actions have inherent constituent elements of deceit. In this way, the criminal offence of electronic fraud gradually found its way in the case law and is defined as the seizure of money or other assets by using a computer (money remittances, payments, fast credits).

The case law indicates that very often offender's conduct consists of an integrated scheme of acts finalised by electronic fraud but consisting of other crimes in order to obtain the instruments of this crime. The crime of this nature renders the person criminally liable not only for the traditional crime of fraud as provided for in Article 182 of the CC but also under other Articles of the CC which cover unlawful possession and acquisition of electronic payment instruments. A research of case law shows that in such cases the person's conduct is also qualified on the basis of Articles 214 and 215 of the CC. Unauthorised access to online banking also raises questions in the case law and doctrine on the relationship between offences under Article 1981 (illegal access to an information system) and Article 215 of the CC. It is suggested in the doctrine to qualify such offence under both Articles on the grounds that the identify verification data of electronic payment instruments of other persons are used through different actions – when accessing online banking and later initiating or performing a financial operation.[22] Such position is also supported in the case law of the court of cassation (e.g. ruling No. 2K-138/2015).

3. New technologies – new qualifying constituent elements?

When establishing crime elements in law, the legislator takes into consideration the fact that criminal offences of the same type can differ by the degree of their dangerousness, which is predetermined by objective and subjective constituent elements of the criminal offence. Apart from general constituent crime elements of the relevant type, qualified crime elements also have constituents which increase the dangerousness of the crime of this type or of the person who commits it, therefore, liability for the commission of such offence is more stringent. The expressions of qualifying constituent elements in the criminal law are predetermined both by the composition of the main elements of crimes and by the public values of that period as well as by the reality of crime in certain existence conditions of the State.

One of the best examples is the development trends of constituent elements qualifying robbery. The main elements of robbery as laid down in Article 180(1) of the CC have a distinctive variety of constituent elements characterising the method of commission of this offence and this predetermines that this offence can manifest itself in a large variety of ways: from the most primitive force on the street where a handbag is seized to an organised group scheme to use firearms against persons in a burglary in order to seize high-value property. The legislator, holding that robbery may be effected in a large variety of forms which differ in their dangerousness, also laid down qualifying constituent elements in paragraphs 2 and 3 of Article 180 of the 2000 CC. Some elements relate to the use of things dangerous to the health or life of persons (knife, non-firearm, other item applied specifically in order to injure a person, firearm, explosive) in the commission of robbery; others – with an exclusive access by the perpetrator to property (robbery by breaking into the premises as a constituent element) or with specific attributes of the subject-matter of robbery.

Rapid development of information technologies and their usage opportunities lead to the question of legal assessment of such cases when the offender, making use of different remote computer control equipment (e.g., robots, drones), exerts violent impact on the victim thereby overcoming the victim's will to resist and facilitating access to the targeted property or when a threat to the victim is expressed by a robot remotely controlled by the offender rather than by the offender in person. Such cases make

[21] A. Piesliakas, *Ibid*., Articles 214 and 215 of the CC, pp. 71-80.

[22] R. Marcinauskaitė, 'Neteisėto prisijungimo prie informacinės sistemos kriminalizavimo ypatumai ir kvalifikavimo problemos [The criminalization peculiarities and qualification problems of unlawful access to information system]' [2016] Vytautas Magnus University, Law Review, No. 2 (14), pp. 250-266.

reconsider the adequacy of the provisions of the current Criminal Code of the Republic of Lithuania for appropriate legal assessment of such situations in order to answer the question whether the use of such things within in the scope of the qualifying constituent element, i.e. whether it increases the degree of danger of the offence and, if so, whether there is no need to supplement the elements of robbery with a new qualifying constituent element.

In answering the question whether the use of various items controlled remotely by a computer in a robbery could increase the dangerousness of the offence and should be assessed as a qualifying constituent element it should be noted that the use of various items makes robbery a more dangerous offence because it poses a much higher risk for the victim's health. The use of such things is attributed to the group of qualifying constituent elements, which is distinguished according to the instruments used in robbery. An instrument is understood in terms of criminal law as any item which is used in the commission of a criminal offence [...] and which is used to encroach the subject-matter or object of a crime.[23] Not any items can be regarded as instruments because it is not the use of any item that can cause a higher threat than usual and create a stronger impression of risk and damage for the victim. The use of items with specific attributes against the victim, however, can considerably weaken the outcome of the victim's efforts to resist a property seizure and also have a very negative effect on the person's physical or mental health, restrict the freedom of his/her actions and pose risk to his/her health. Very often such robbery is generally referred to as armed robbery where the possession of arms is treated as the use of an additional instrument to commit robbery. As far as armed robberies are concerned, they are often regarded as criminal offences requiring a much higher degree of organisation, more profitable and committed by skilled professionals.[24] Armed robbery can manifest itself in highly diverse forms and degrees of the use of force and in the selection of different types of instruments.

It is recognised in the doctrine that the use of instruments in robbery can be both direct and indirect.[25] Use can be understood as a direct action involving a certain item used according to its purpose, and as indirect which can be unaccompanied by any specific impact with that item on the victim and only by a verbal tacit expression by the offender about the existence of such item or its potential impact on the victim. The cassation rulings under research show that the court of cassation has been called a number of times to interpret the legal aspects of the concept of use. The case law of the court of cassation holds that use means not only a direct utilisation of the injuring attributes of a crime instrument but also using it for threatening – orally, by gestures, manifest demonstration.[26] That proves that the concept of use is not limited to a direct use of the item according to its specific purpose.

As information technologies are improving, it is not unlikely that offenders will no longer have to exert violence on the victim on their own – that will become possible by using remotely controlled robots, drones, etc. Where the use of such items poses risk to the health of the victim and causes physical pain, such items express a real threat or their use otherwise deprives the victim of the opportunity to resist (e.g. a remotely controlled device is used to inject a needle with intoxicating substances into a person). It follows from the above that such robberies when remotely controlled computer devices are used could also be regarded as qualified constituent elements from the legal perspective. Such devices are used in order to allow the offender to avoid a direct contact with the victim, to remain less recognisable; on the other hand, the use of such items increases the power advantage of the offender with respect to the victim as his/her resistance to property robbery is suppressed.

Another important issue is whether the existing legal regulation is adequate in order to assess the dangerousness of an offence in the above-discussed situations, i.e. which of the qualifying constituent elements laid down in Article 180 of the CC could include the use of such items. As far as the use of knifes, non-firearms, other items applied specifically in order to injure a person, firearms or explosives, as

[23] A. Abramavičius, A. Baranskaité, A. Čepas, G. Švedas, et al, 'Commentary to the Criminal Code of the Republic of Lithuania. General Part (Articles 1-98)' (Vilnius: Legal Information Centre 2004) p. 133.

[24] R. Matthews, 'Armed Robbery [interactive]' (UK: Willan publishing 2002) p. 41, http://books.google.lt/books?id=QMX2z_pZGqUC&pg=PA20&dq=robbery+crime&hl=en&sa=X&ei=uTleU_OnKfDR4QTKuoHYAQ&ved=0CEgQ6AEwBQ#v=onepage&q=robbery%20crime&f=false, accessed 2 March 2016.

[25] E. Mezzetti, 'Trattato di diritto penale, parte speciale, Reati contro il patrimonio' (Milano: Dott. A.Giuffre Editore 2013) p. 253.

[26] Ruling of 7 June 2005 of the Supreme Court of Lithuania in criminal case No 2K-408/2005.

the constituent elements provided for in the Article, are concerned, it may be assumed that the most appropriate and realistic option which can potentially cover the use of such items in robbery is the use of other item specially designed to injure a person, as a constituent element. The case law shows that household items, sports items, animals, medical devices, etc. are most often held to be within the scope of this constituent element. When deciding whether an item should be considered as applied specifically in order to injure a person in each specific case, the following circumstances should be taken into consideration: (1) the method of use of the item during robbery and/or (2) anticipated purpose for which that item has been taken by the offender.[27] Not only items, which the offender prepares in advance or adjusts for the commission of robbery or during robbery, but also items, although not prepared in advance but pre-selected and taken for the same purposes, are considered as items applied specifically in order to injure a person. It follows from such interpretation that the existing regulation of the CC is adequate for a legal assessment of the cases when various instruments controlled by computer technologies are used in robbery as constituent elements which increase the dangerousness of the offence.

Conclusions

- The use of information technologies for unlawful purposes expands the list of crime commission methods and leads to more complex qualification combinations of offences when it is not sufficient to limit oneself to qualification of classical crimes against property.
- Taking into consideration the impact of remote computer control devices on the victim, as able to exert physical violence or otherwise deprive the victim of the possibility of resistance, the use of such items should be treated as a constituent element qualifying an offence.
- It follows from the existing legal regulation that the qualifying constituent elements of Article 180 of the CC are adequate in order to include the use of such devices and the establishment of new qualifying constituent elements is unnecessary.

Bibliography

1. A. Abramavičius, A. Baranskaitė, A. Čepas, G. Švedas, et al, 'Commentary to the Criminal Code of the Republic of Lithuania. General Part (Articles 1-98)' (Vilnius: Legal Information Centre 2004).
2. E. Baranauskas, I. Karulaitytė-Kvainauskienė, J. Kiršienė, V. Pakalniškis, et al, 'Civil Law. General Part.' (Vilnius: Mykolas Romeris University 2007).
3. Criminal Code of the Republic of Lithuania. Official Gazette, 2000, No. 89-2741.
4. O. Fedosiukas, 'Nuosavybė ir turtas Civiliniame ir Baudžiamajame kodeksuose [The Ownership and Property in the Civil and Criminal Codes]' [2002] Jurisprudencija, Vol. 28 (20).
5. O. Fedosiukas, 'Turtinė nauda kaip nusikalstamos veikos dalykas: sisteminė normų analizė [Property Gain as a Subject-Matter of Crime: Methodical Analysis of Norms]' [2004] Jurisprudencija, T. 60 (52).
6. V. Kalpokas, 'Nusikaltimai elektroninėje erdvėje: kriminologinės sampratos dilemos [Crimes on the Electronic Space: Criminological Concept Dilemmas]' [2009] Teisės problemos, No. 1 (63).
7. M. Kiškis, R. Petrauskas, I. Rotimskis and D. Štitilis, 'Teisės informatika ir informatikos teisė [Law IT and IT Law]' (Vilnius: Mykolas Romeris University 2006).
8. Local authorities and transfrontier crime: proceedings: Enschede (Netherlands), 20-22 September 2001 / International Conference organised by the Congress of Local and Regional Authorities of Europe (CLRAE) of the Council of Europe, in co-operation with the City of Enschede, Netherlands and the Dutch Section of the Council of European Municipalities and Regions (CEMR) (Strasbourg: Council of Europe 2002).
9. R. Marcinauskaitė, 'Nusikalstamomis veikomis elektroninėje erdvėje pažeidžiamos pagrindinės baudžiamojo įstatymo saugomos vertybės nustatymo problema [The Problems of Identification of the Main Object of Cyber Offences].' (Mykolas Romeris University 2011) Social Science Studies, No. 3 (3).

[27] Ruling of 23 October 2007 of the Supreme Court of Lithuania in criminal case No 2K-661/2007.

10. R. Marcinauskaitė, 'Neteisėto prisijungimo prie informacinės sistemos kriminalizavimo ypatumai ir kvalifikavimo problemos [The criminalization peculiarities and qualification problems of unlawful access to information system]' [2016] Vytautas Magnus University, Law Review, No. 2 (14).
11. R. Matthews, 'Armed Robbery [interactive]' (UK: Willan publishing 2002), http://books.google.lt/books?id=QMX2z_pZGqUC&pg=PA20&dq=robbery+crime&hl=en&sa=X&ei=uTleU_OnKfDR4QTKuoHYAQ&ved=0CEgQ6AEwBQ#v=onepage&q=robbery%20crime&f=false, accessed 2 March 2016.
12. E. Mezzetti, 'Trattato di diritto penale, parte speciale, Reati contro il patrimonio' (Milano: Dott. A.Giuffre Editore 2013).
13. Order the Prosecutor General of the Republic of Lithuania regarding the methodological recommendations for the investigation of online scams (telephone scams) and the qualification of criminal offences, 10 February 2014, No. I-37.
14. A. Piesliakas, 'Veikų dėl neteisėto disponavimo svetima elektronine mokėjimo priemone (BK 214 ir 215 straipsniai) kvalifikavimo problemos [Qualification Problems of the Crimes of Illegal Disposal of a Non-Cash Payment Instrument]' [2007] Mokslo darbai, Jurisprudencija 8 (98).
15. Republic of Lithuania Law on the Ratification of the Convention on Cybercrime, Official Gazette, 2004, No. 36-1178.
16. Ruling of 27 April 2004 of the Supreme Court of Lithuania in criminal case No 2K-319/2004.
17. Ruling of 7 June 2005 of the Supreme Court of Lithuania in criminal case No 2K-408/2005.
18. Ruling of 17 February 2009 of the Supreme Court of Lithuania in criminal case No 2K-63/2009.
19. Ruling of the Supreme Court of Lithuania in criminal case No 2K-174/2009.
20. Ruling of 25 September 2012 of the Supreme Court of Lithuania in criminal case No 403/2012.
21. Resolution No. 55 of 29 December 2005 of the Senate of the Supreme Court of Lithuania regarding the case law in criminal cases related to criminal acts against the financial.
22. Resolution No. 52 of 23 June 2005 of the Senate of the Supreme Court of Lithuania 'Regarding the case law in criminal cases of theft and robbery'. Case Law. No. 23. Vilnius, 2005.D. Sauliunas (ed), 'Informacinių technologijų teisė' [Law of Information Technologies] NVO Teisės (Vilnius 2004).
23. D. Štitilis, P. Pakutinskas, M. Laurinaitis and I. Dauparaitė, Inga, 'Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai [Online Identity Theft: Social, E. Business and Legal Regulation Aspects]' (Mykolas Romeris University 2011).
24. P. Švedas, 'Blanketinės dispozicijos Lietuvos Respublikos baudžiamajame kodekse [Blanket Dispositions in the Criminal Code of the Republic of Lithuania]' [2010] Teisė, 77.
25. P. Veršekys, 'Vertinamieji nusikalstamos veikos sudėties požymiai [Evaluative features of corpus delicti]' [2013] Doctoral Dissertation, Vilnius University.