Law 4.0 – Challenges of the Digital Age

Judit GLAVANITS – Péter Bálint KIRÁLY (eds)

Editors:

Dr. jur. Judit GLAVANITS, PhD.
associate professor
Dr. jur. Péter Bálint KIRÁLY
PhD student, junior lecturer

ISBN 978-615-5837-45-6 (print)

ISBN 978-615-5837-46-3 (pdf)

Published by Széchenyi István University –
Deák Ferenc Faculty of Law and Political Sciences –
Department for Public and Private International Law
(H-9026 Győr, Áldozat u. 12.)
Web: nkmt.sze.hu

in cooperation and with the financial support of

SmartLaw Research Group

Print: Wasco Trade Kft. (H-9090 Pannonhalma, Ady u. 10.)

CONTENT

Editor's note

On 29th March 2018 the Széchenyi István University Faculty of Law and Political Sciences held a successful conference entitled "Law 4.0 – Challenges of the Digital Age.

The concept of the event was to discuss the current status of regulation of different areas affected by the "Industry 4.0" phenomena. Industry 4.0 means in essence the technical integration of cyber physical systems into production and logistics and the use of the 'internet of things' (IoT) and services in (industrial) processes – including the consequences for a new creation of value, business models as well. Today, we clearly see how the several parties which were involved in Industry 4.0 themselves move it to smart transportation and logistics, smart buildings, oil and gas, smart healthcare and even smart cities. Within the next few years, it is expected that over 50 billion connected machines will exist throughout the world. The introduction of artificial intelligence in the service sector distinguishes the fourth industrial revolution from the third.

What is the role of legal regulation in this "brave new world"? Is there a Law 4.0 already?

The conference papers formulated around the following topics:

1. How law should treat artificial intelligence (AI)?

In 1969 John McCarthy and Patrick J. Hayes from Stanford University stated that "a computer program capable of acting intelligently in the world must have a general representation of the world in terms of which its inputs are interpreted. Designing such a program requires commitments about what knowledge is and how it is obtained." How can we describe the world around us in legal terms to help the machines decide right from wrong? How do we teach AI fundamental rights (and should we even do that)?

2. Security and privacy issues arising from the digitalization

When it comes to data security, most people think of hacking or viruses. But lawyers have additional concerns. Are spreadsheets being traded? What should appear in billing while maintaining client confidentiality? How do you collaborate

without leaving yourself open to a data breach? What data are to be secured while online trading? How does Facebook get the intellectual property rights of the uploaded photos of users? How to protect the privacy of our clients/children? As in the European Union a new regulation on data protection (GDPR) has been adopted, these questions are current.

3. Digitalization of the State

In the EU the Digital Single Market Strategy announced by the Commission is built on three pillars: (1) Access: better access for consumers and businesses to digital goods and services across Europe; (2) Environment: creating the right conditions and a level playing field for digital networks and innovative services to flourish; (3) Economy & Society: maximizing the growth potential of the digital economy. Every single Member State has to make efforts towards a better digital market, which also contains digitalized state services, and better (digital) access to the central and local governments.

This publication contains some of the selected papers from the conference. The Editors hope that the event was just the beginning of further cooperation and a deepening work on this exciting field of science.

Győr, 2019.

PRIVACY PROTECTION OF CHILDREN UNDER THE NEW EU REGULATION

KATINKA BOJNÁR[1]

Abstract

Children are facing several dangers in the virtual space due to the anonymity of the internet. Acknowledging this, Article 8 of the GDPR[2] deals with the privacy protection of the children. The explicit declaration of this right in the GDPR can be evaluated as a remarkable progress, but on the other hand a considerable gap can also be identified as the member states could not agree on the age limit of the right to informational self-determination. This rule undermines the level of protection provided for children and the legal certainty in general. Children's privacy protection needs to be our common goal what we can reach via strong regulation, efficient enforcement, and raising awareness in schools. At last, but definitely not least the supportive family background is essential.

Keywords: *privacy protection, children, General Data Protection Regulation, internet*

I. Why do we have to speak about privacy protection of the children?

Personal data relating to children is processed for many purposes by private and public sector organisations, including the provision of online and offline services, education, social care, healthcare and personal welfare, and as part of information on family circumstances. In some cases, the processing will include special categories of personal data. The children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards, and their rights in relation to the processing of personal data. These data processing activities may be regarded as high risk in some cases and require particular levels of care.

According to a survey, children use internet from the age of 8. According to the statistics more than 75% of the children in the EU use internet for different purposes, like socialising, sharing or creating virtual contents.[3] More than 59% of the age group between 9-16 have a social media profile, and more than 26 % of these profiles are public.

II. The dangers of the internet for the children

II.1. Online deviances

Despite many positive and advantageous benefits of the Internet,[4] it also poses a threat to children. Due to their age, their credulity and naivety make them vulnerable. Dangers include websites with content that are harmful to the physical, psychological, and moral development of children, or

[1] Katinka BOJNÁR, PhD student, Pázmány Péter Catholic University, Contact: katinka.bojnar@freemail.hu

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

[3] Livingstone – Haddon (2009) 47. p.

[4] Deli (2001) 91. p.

those who hate or exploit targeted children. Services that are fundamentally non-hazardous can also be a problem, including social networking, web games, and virtual games.

One of the most common threats is cyberbullying. Cyberbullying is an offensive act with "information communication tools" that repeatedly targets a specific victim that cannot protect himself.[5] During the harassment the victim is injured or the harassment causes a serious disturbance in his privacy life and is characterized by a recurring nature.[6] Cyberbullying can be therefore a rough joke, which typically affects children of the ages between 13 and 17, can appear on different platforms.[7] The keyword is disturbance, which is an annoying act, but its scale may vary. This kind of harassment is exacerbated by the fact that while physical bullying in school is over after leaving the school building, in the case of cyberbullying the child remains a victim at home, actually everywhere where he has access to the Internet. Internet harassment takes place in public, with more apparent consent from witnesses than offline harassment. The spread of smart phones limits the control and regulatory capabilities of parents and increases the number of threats to children.[8]

Internet memes is another example of online bullying. The broadcasting of digital files or links originally for advertising purposes is often the source of fake news, embarrassing videos or images, which can be either an artistic expression or a gratifying gesture, but it often extends into a rough expelling campaign. The internet memes differ from cyberbullying in that the victim is usually a stranger whom the Internet community "picks out" by some negative attribute or manifestation.[9]

According to the internet slang, the provoking comments or troll is written by a person who distributes irrelevant messages provocatively to an online community (e.g. on an internet forum, in a chat room, blog or a mailing list) or pushes forward his position violently aiming at provoking harsh reactions from other users.

Internet paedophilia has specific features where the offender uses the internet as tool to commit sexual abuse. The virtual space provides the ground to get acquainted with a child, and the abuser can build relationship and compel the child to make pornographic content without risk, and in serious cases it leads to real encounters.[10]

There are several other dangers, like online grooming. The anonymity of the Internet helps the criminal to search for potential victims. Children quite often accept the friendship of people they have never met before, only because the individual is an acquaintance of a friend or they share some common field of interest. We shall also bear in mind that a person concealing himself behind a photo and pretending to be a 14-year-old girl may be actually a 30 or 40-year-old man.[11] The Facebook made a test where they created an account under the name of Freddy posting a green frog as his profile picture. Freddy, the frog sent friend requests to 200 hundred persons. Although nobody knew who was behind the frog, half of the requests was accepted. It means that these persons opened their personal data, so their privacy to a fictitious and mysterious virtual person they have never met.

[5] Smith (2008) 376. p.
[6] Moore (2015) 129. p.
[7] Szathmáry (2012) 69. p.
[8] Sziklay (2013) 48. p.
[9] Sziklay (2013) 50. p.
[10] Sziklay (2013) 48. p.
[11] Sanderson (2004) 294. p.

II.2. Internet-connected toys

The growing popularity of "smart" Internet-connected toys poses significant privacy, security, and other risks to children. Several complaints were received by data protection authorities worldwide.[12] These toys can collect and use personal information from children in violation of the children's privacy. The toys are connected to the internet and use their build-in microphones and speech recognition technologies in order to engage in 'conversations' with children. The content of these interactions may contain personal data and sensitive information shared by the child unknowingly. So these toys are working like a telescreen installed in the family as predicted by George Orwell in 1984. The company offering these products very often reserves the right in the general terms of conditions to collect the contact lists of the device on which the app is installed. This device is usually the smart phone of the parents. These toys often lack built-in security measures common to other connected home products. That makes them easy targets for hackers looking to steal information from the toy itself or from other "smart" items connected to a home network.

Several data protection considerations were raised by data protection authorities: the companies behind these toys reserve the rights to share children's personal data with unspecified third parties; the companies fail to properly identify or restrict the purposes for which they use and distribute children's voice data; the companies may use children's data for analytical and research purposes unrelated to the toys themselves; the toys may collect children's data for advertising purposes and separate or explicit consent for this purpose is not asked; there is no clear data retention procedures.

III. The applicable European rules

The Charter of the Fundamental Rights of the European Union states that "Children shall have the right to such protection and care as is necessary for their well-being[...]"[13] and "[i]n all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration."[14]

The Directive 95/46[15] does not explicitly mention the privacy rights of minors. However, this does not mean that children do not have any right to privacy and that they fall outside the scope of the Directive as it shall apply to any "natural person", and therefore includes children. The Article 29 Working Party (WP29)[16] identified two aspects that must be taken into account when children's data are processed.[17] These are, first, the varying levels of maturity which determine when children can consent a data processing activity and, secondly, the extent to which representatives have the right to represent minors in cases where the disclosure of personal data would prejudice the best interest of the child.[18] As the Directive does not define the age limit of consent, the Member States are free to determine it. The practice of the MS is quite diverse.

---

[12] http://blogs.edweek.org/edweek/DigitalEducation/2016/12/ftc_complaint_raises_data_priv.html
[13] Article 24.1 of the Charter of Fundamental Rights of the European Union
[14] Article 24.2 of the Charter of Fundamental Rights of the European Union
[15] 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 ont he free movement of such data
[16] Established by Article 29 of the Directive 95/46/EC.
[17] Opinion 2/2009 on the protection of children's personal data (WP 160)
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp160_en.pdf
[18] For further information: https://iapp.org/news/a/will-gdpr-move-age-of-consent-to-16/

The GDPR recognises that children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data.[19] According to Article 8 of the GDPR "[...] the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years."

The Article 8 only applies where the information society service provider processes personal data of the person using the service. The Regulation foresees that consent must be given or authorised by the holder of the parental responsibility over the child. The age threshold is for the Member States to define within a range of 13 to 16 years. The main rule is 16, but the GDPR provides flexibility allowing its decrease until the age of 13, but not lower. It is a compromise and quite untypical for a directly applicable regulation to give such a flexibility. Selection of the age of digital consent, within the 13-16 threshold range, varies widely among the Member States. The age limit of digital consent are the following: in Austria 14; in Germany 16; in Czech Republic 13; in Denmark 13; in Ireland 13; in Latvia 13; in Poland 13; in Spain 13; in Sweden 13; in UK 13; in Hungary 16; in Lithuania 16; in Luxembourg 16; in Slovakia 16; and in the Netherlands 16.[20]

This compromise creates legal uncertainty and challenges the harmonised cooperation between Member States. It causes legal uncertainty as the controller providing services in the different EU Member States will face the problem of the different age limit of informational self-determination. According to the opinion of the WP29 which was endorsed by the European Data Protection Board,[21] the controller must be aware of those different national laws, by taking into account the public targeted by its services. In particular, it should be noted that a controller providing a cross-border service cannot always rely on complying with only the law of the Member State in which it has its main establishment, but may need to comply with the respective national laws of each Member State in which it offers the information society service(s).[22]

IV. The Hungarian national rules and case law

According to the Hungarian Privacy Act,[23] the age limit of consent is 16. For minors under this age an explicit permission or subsequent approval of their legal representative is required by law.

It means that the Hungarian national legislation is opt for a stricter solution, although the GDPR would allow the national legislator to lower this age limit. The Hungarian Data Protection Authority has launched several investigations to protect the children's privacy and in most of the cases, it turned out that the controller did not check whether the user was over 16 years and did not ask for the permission of the holder of parental responsibility. The Hungarian Data Protection

---

[19] Recital 138 GDPR

[20] GDPR Implementation: In Respect of Children's Data and Consent, Centre for Information Policy Leadership, issued: 6 March 2018.
https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_gdpr_implementation_in_respect_of_childrens_data_and_consent.pdf

[21] EDPB: 1/2018 Endorsement,
https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf

[22] WP29 Guidelines on consent under the Regulation 2016/679. (WP 259 rev.1.) p. 25.
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

[23] Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information

Authority investigated the age limit in the context of the data processing activities of dating sites. The Authority launched 22 investigations and in 9 cases out of the 22 imposed a fine.

The Authority highlighted that a person who is above 14 years, in accordance with civil law rules, can make minor contracts falling within the scope of the ordinary needs of everyday life according to the Civil Code. It does not include the registration on dating sites and takes into consideration not the civil law but the privacy act's age limit which is 16 years. [24] The competent Hungarian Court reviewed the Authority's above-mentioned interpretation and confirmed it. The Court clearly stated that the Hungarian Privacy Act is the *lex specialis*, it is the applicable law and not the Civil Code. The Court also stated that a data subject under 16 years can only consent a data processing activity if the holder of parental responsibility gives his permission to the data processing activity. [25]

V. Possible solutions

By Article 8 the GDPR introduces a higher threshold of protection for the processing of children's data. The new rules are necessary, but in themselves are not sufficient. How can be the right of children efficiently enforced?

V.1. Awareness raising

Children should be made aware, in particular, that they themselves must be the primary protectors of their personal data. According to this criterion, the gradual participation of children in the protection of their personal data (from consultation to decision) should be made effective. This is an area where the effectiveness of empowerment can be demonstrated. The children should be informed about dangers and online deviances [cyberbullying, internet memes, provoking comments (troll), internet paedophilia, grooming etc.]. [26]

V.2. Education and the responsibility of parents, teachers and educational institutions

These are crucial factors in the protection of children's data. To achieve a better protection of children's personal data it is important that those, who take care directly of the education of children, will have comprehensive training in data protection principles, the technology and the nature of the social media.[27]

According to an American study, children are Digital Natives. They are all "native speakers" of the digital language of computers, video games and the Internet.[28] So what does that make the rest of us? Those of us who were not born into the digital world, but have at some later point in our lives, become fascinated by the new technology are, and always will be, compared to our children, Digital Immigrants. It means that Digital Immigrants have to learn the digital language and their accent will always be detectable.[29] Those who are responsible for the education of the children, have to be well prepared to explain the different dangers of the Internet. It means also

[24] NAIH-5951-16/2012/H. számú határozat 7-8. http://naih.hu/files/5951_2012_2_hatarozat.pdf
[25] Fővárosi Közigazgatási és Munkaügyi Bíróság 27.K.31.641/2013/11. számú ítélete, 6.
[26] Opinion 2/2009. p. 20.
[27] Opinion 2/2009. p. 20.
[28] Prensky (2001) 1. p.
[29] Prensky (2001) 2. p.

that parents and teachers have to know well the different technical possibilities and developments, the world of internet and they have to keep themselves updated in this field.

V.3. Children friendly information

In the context of providing information to children or their legal representatives, special emphasis should be put on giving layered (adequate to his age) notices in a simple, concise and educational language that can be easily understood by them.[30]

The GDPR also stipulates that where children are targeted by services, there is a particular obligation to convey information in a way that is intelligible to the child. The information shall be understandable to the audience addressed by the controller, paying particular attention to the position of children.[31] In order to obtain "informed consent" from a child, the controller must explain in a clear and plain language for children, how it intends to process the data collected.[32] Besides the right to be informed, a particular emphasis needs to be given to the "right to be forgotten" in relation to personal data made available by a child.[33]

V.4. Age verification systems

Raising the age limit of consent is in itself not enough. The controllers are expected to make effective and reasonable efforts to verify that the user is over the age of digital consent. Attention shall be paid to these control mechanisms as they can also raise data protection issues if they require the collection of too much additional information. These measures should be proportionate to the nature and risks of the processing activities.

Age verification should not lead to excessive data processing. The mechanism chosen to verify the age of a data subject should involve an assessment of the risk of the proposed processing. In some low-risk situations, it may be appropriate to require a new subscriber to a service to disclose their year of birth or to fill out a form stating they are minors or not.

If the user states that he/she is below the age of digital consent then the controller can accept this statement without further checks, but will need to go on to obtain parental authorisation. If the user states that he/she is over the age of digital consent then the controller can carry out appropriate checks to verify that this statement is true. Although the need to undertake reasonable efforts to verify the age does not come explicitly from the GDPR, it is implicitly required, as invalid consent renders the processing of data unlawful.[34]

V.5. The roles of data protection authorities

According to the 2/2009 opinion of the WP29 the national authorities have different roles on how the privacy protection of children can be promoted.[35] WP29 identified four roles: First, the national data protection authorities has an exceptional role to educate and inform children and the

[30] Opinion 2/2009. p. 10.
[31] WP29 Guidelines on consent under the Regulation 2016/679. (WP 259 rev.1.) p. 24.
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051
[32] Recital 58 GDPR
[33] http://childrensrights.ie/sites/default/files/conference-proceedings/files/Data%20Protection%20and%20Children's%20EU%20Rights_Billy%20Hawkes.pdf
[34] WP29 Guidelines on consent under the Regulation 2016/679. (WP 259 rev.1.) p. 25.
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051
[35] Opinion 2/2009. p. 20.

authorities are responsible for the well-being of young people. Second, by the power to supervise all data protection related laws give the possibility to influence policy makers to make the right decisions concerning children and their privacy. Third, not only the data subjects have to be informed about their rights, but the data protection authorities have to make controllers aware of their duties. At last, but not least, in case of the infringements of the law, the authorities have to use their powers efficiently against those who have disregarded the legislation or did not adhere to codes of conduct or best practice in this area.

VI. Conclusions

Children are facing several dangers in the virtual space due to the anonymity of the internet. Cyberbullying, grooming and sexting are the main sources of dangers, but we have to keep in mind the internet connected toys as well.

Acknowledge this, Article 8 of the GDPR deals with the privacy protection of the children. Under the previous directive there was no such rule although it did not mean that children would not have had the right to data protection. The explicit declaration of this right in the GDPR can be evaluated as a remarkable progress, but on the other hand a considerable gap can also be identified as the Member States could not agreed on the age limit of the right to informational self-determination. Although the GDPR is directly applicable and determines the age limit at 16 year, it also gives the opportunity to lower this age limit until 13 year. I argue that this rule undermines the level of protection provided for children and the legal certainty in general.

The age limit in Hungary is 16 years which may cause legal problem in a cross-border case where according to the national law of the other competent authority, the age limit is lower. It would lead to the result that the same data processing activity (e.g. processing personal data of a 15-year old data subject without the parental consent) would be lawful in one member state and unlawful in the other. The Hungarian Data Protection Authority has launched several investigations to protect the children's privacy and in most of the cases it turned out that the controller did not checked whether the user is over 16 years.

Children's privacy protection needs to be our common goal what we can reach via strong regulation, efficient enforcement, and raising awareness in schools. At last but definitely not least the supportive family background is essential.

REFERENCES

Deli Gergely (2001): Internet és demokrácia a jog szemszögéből, Iskolakultúra, No.1. 90-98.

Moore, Robert (2015): Cybercrime, Investigating High-technology Computer Crime. Routledge, Taylor and Francis Group, London and New York

Livingstone, Sonia – Haddon, Leslie (2009): EU Kids Online: Final report. LSE, London: EU Kids Online.

Prensky, Marc (2001): Digital Natives, Digital Immigrants. On the Horizon - MCB University Press, Vol. 9, No. 5. 1-6.

Sanderson, Christiane (2004): The Seduction of Children, Empowering Parents and Teachers to Protect Children from Child Sexual Abuse. Jessica Kingsley Publishers, London and Philadelphia

Smith, PK. et al (2008): Cyberbullying: Its nature and impact in secondary school pupils. Journal of Child Psychology and Psychiatry, Vol. 49, No. 4. 376-385.

Szathmáry Zoltán (2012): Bűnözés az információs társadalomban, Alkotmányos büntetőjogi dilemmák az információs társadalomban, Doktori értekezés, Budapest

Sziklay Júlia (szerk.) (2013): Kulcs a net világához! Budapest, NAIH

Charter of Fundamental Rights of the European Union

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)

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

Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information

Article 29 Working Party: Opinion 2/2009 on the protection of children's personal data (WP 160), Available: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp160_en.pdf

Article 29 Working Party: Guidelines on consent under the Regulation 2016/679. (WP 259 rev.1.), Available: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

Case of the Hungarian Data Protection and Freedom of Information Authority: NAIH-5951-16/2012/H. Available: http://naih.hu/files/5951_2012_2_hatarozat.pdf

Judgement of the Hungarian Capital Adminsitrative and Labor Court: 27.K.31.641/2013/11.

GDPR Implementation: In Respect of Children's Data and Consent, Centre for Information Policy Leadership, issued: 6 March 2018. Available:

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_gdpr_implementation_in_respect_of_childrens_data_and_consent.pdf

THE IMPORTANCE OF DIGITAL PUBLIC SERVICE DEVELOPMENT FROM THE COMPANIES' POINT OF VIEW

LÁSZLÓ BUICS[1]

Abstract:

All companies are using public services thus they are all "customers" of the state. The aim of this paper is to examine governmental development approaches from the viewpoint of the companies through two systems, the Client Gate and the Company Gate. Both of them are digital public services, but while the Client Gate is offering services generally for citizens, the other was tailored especially for companies. The goal of my research is to examine the development steps which led to the creation of Company Gate and to examine it in terms of accessibility, usability and offered services to see whether it can help companies to simplify their tasks further compared to the previously used Client Gate.

Key words: *public services, digitalization, Company Gate*

I. Introduction

Digitalization and the spread of information technology inevitably transform our environment. Adaptation is indispensable, so the players of the economy cannot avoid major changes for long. Businesses have to face more and more competition. Meeting the constantly changing and expanding consumer demands is becoming more and more difficult.

The rapid development of information and communication technologies, like the industrial revolution, induced a transformation. The increase in the performance of electronic data processing, information and communication technology, digital data storage and data transfer together affected many areas.

It affects citizens' lives, the behavior of the economy (e-commerce), and the work of state organizations. This complex process has led to an informatics-based social model. The construction of an information society is no longer just an option but a condition for economic survival and the preservation of competitiveness.

The ever-changing environment and the development of information technology make the administration and the economy more transformative. As a result, public administration has undergone a major change in recent years, and has made the administration and the economy more efficient by electronically integrating its internal operation and has created the possibility for citizens and businesses to manage their administrative affairs online. The transformation of public administration into e-administration is an ongoing process ever since.

The purpose of electronic administration is to create a more convenient, efficient and more economical electronic system that reduces the administrative burden on businesses by improving the efficiency of their operations. But this can be achieved only by the expansion of the use of

[1] László BUICS, PhD student, Széchenyi István University, Győr, Hungary, buics.laszlo@sze.hu

infocommunication tools and services, the expansion of electronically manageable issues, the application of a customer-centric approach, and the e-inclusion of businesses. Taking these considerations into account, I look at businesses as clients and examine the services available to them.

The purpose of my research is to get acquainted with the administrative possibilities of domestic enterprises here in Hungary. I summarize the efforts that have led public administrations to adapt to the new digital era, thus establishing the future of e-public services. I will also examine what kind of electronic services the state provides for businesses to help managing complex business issues, highlighting the benefits of the Client Gate and Company Gate systems.

II. European Union steps and strategies of change

In order to maintain and strengthen the international competitiveness of European businesses first the Bangemann report in 1994 made concrete proposals to promote information development, thus opening a new chapter in developing an information society policy. [2]

The report suggested the active involvement of the European Council to preserve the international competitiveness of European businesses, which is needed to accelerate the process of liberalization that has already begun to maintain and ensure the unity of existing services. According to the recommendation, the information infrastructure and its functioning should primarily be based on business logic, and the indispensable regulatory framework should be based on for harmonized legislative work of the Member States and the Union institutions. [3]

The European Union information policy, which emerged in 1994, defined the tasks of the information society primarily as an economic and secondly as legal-regulatory task. The report represented a theoretical point of view that presented the economic aspects of the information society. .[4]

In March 2000, the European Council proposed the establishment of a knowledge-based economy. [5] The decision-makers of the European Union have seen not only the new technology opportunities in the use of infocommunication tools, but they have also recognized its social potential. By adopting action plans the Member States agreed to work out a common set of standards to accelerate the becoming of an information society.

Following the changes of the Lisbon meeting, the European Commission published the eEurope 2002 Action Plan in 2001. The e-government area got its own program, aimed at making public services available to the business community and citizens. The European Union's aim was to make 20 public services like corporate tax, VAT, statistical data providing, environmental licenses available electronically to business and citizens by every Member State. [6]

- 12 are G2C (government to citizen) or C2G (citizen to government)
- 8 are G2B (government to business) or B2G (business to government)

The next step is the eEurope2005 Action Plan, which aimed to develop services, applications, and content while it also deals with the development of the infrastructure and the security issues. [7]

---

[2] Bangemann Report (1994) p. 5-39.
[3] Fáber Dávid (2002)
[4] Csáki Gyula Balázs (2010) p. 20-22.
[5] Losoncz Miklos (2011) p. 148-170.
[6] Budai Balázs Benjamin (2014) p. 200.
[7]. Csáki Gyula Balázs (2009) p. 20-26.

After that the i2010 eGovernment and eGovernment 2011-2015 Action Plan both draw attention to the link between national competitiveness, strong innovation capacity and the quality of public administration, indicating that good governance is vital in world economic competition, and mentioned the acceleration and modernization of electronic government as a priority. [8] They were followed by the Europe 2020 strategy, which is an integrated strategy that seeks to address competitiveness aspects, innovation, environmental sustainability and social convergence. [9]

III. Hungarian steps and strategies of change

In Hungary, the development of e-administration is based on the domestic strategic plans which take into account the strategic documents of the European Union. They define the principles, goals to be achieved and indicators. The Computing Center Development Program (A Számítástechnikai Központ Fejlesztési Program) (1971-1985), later the Electronic Economic Development Program (Elektronizációs Gazdaságfejlesztési Program) (1985-1990), provided the IT background of the administration. [10] As a result of the program, the preparation and coordination of the IT strategy plans at the government level have started.

The next important milestone was the E-Administration 2010 strategy, which was quite similar to EU policy guidelines at several points. In Hungary, a major part of the developments in e-administration was implemented through EU co-financing. The strategic framework was included in the New Hungary Development Plan for the years 2007-2013 and in the Public Administration and Public Service Development Strategy for the years2014-2020. [11]

Due to the complexity of digitalization and peculiarities of state administration, the development is a huge challenge. At the same time, it is necessary to renew the public administration because of the changing and more concrete demands of citizenship.

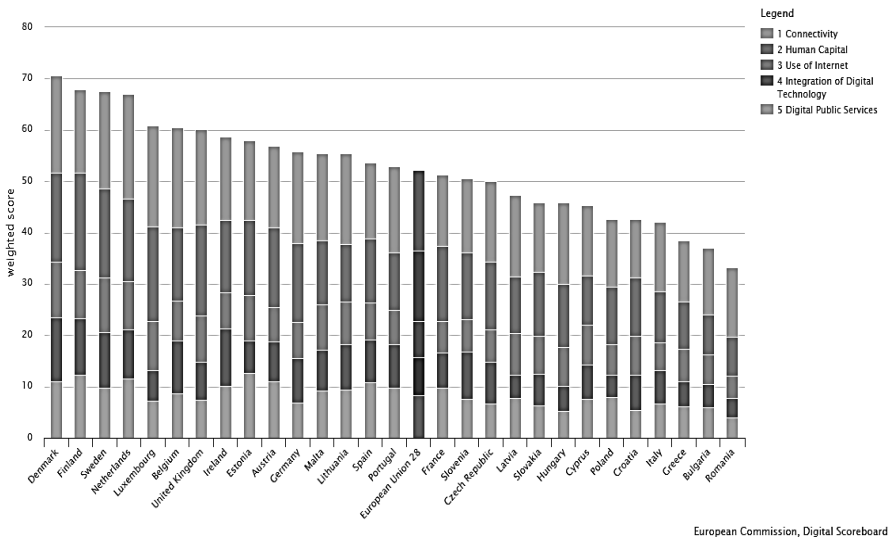
The Digital Economy and Society Index (DESI) is an online tool to measure the achievements of the EU Member States in building a digital economy and society. With DESI, EU Member States have the opportunity to identify the areas where further investment needed to achieve the main objectives of the Union. Based on data of "Digital Economy and Society Index 2017" (1. Figure), Hungary still shows a significant lag. Within the European Union, Hungary is the 22th (from 28) and the most challenging area in Hungary is still the digital public service providing. In this field, Hungary is ranked as 27th. [12]

IT tools, technologies and services are almost indispensable in today's economy and society. The use of information and communication technology tools and related technologies clearly reflects the country's economic development level, the current state of digital literacy.

1. Figure

[8]. Csáki Gyula Balázs (2009) p. 20-26.
[9]. Csáki Gyula Balázs (2009) p. 20-26.
[10] Budai Balázs Benjamin és Tózsa István (2007) p. 33.
[11] Budai, Balázs Benjamin. (2014) p. 208.
[12] http://digital-agenda-data.eu/charts/desi-components#chart={"indicator":"DESI","breakdown group":"DESI","unit-measure":"pc_DESI","time-period":"2017"}

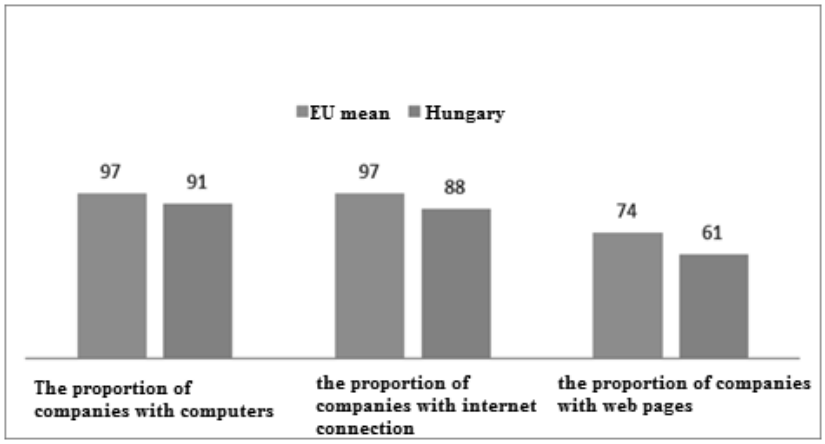
Digital Economy and Society Index, by Main Dimensions of the DESI



Source: Digital Economy and Society Index 2017[13]

2. Figure

The percentage of businesses using computers and internet in EU member states and Hungary, 2014



Source: KSH[14]

The 2. Figure shows the KSH survey about the percentage of businesses using computers and internet in EU member states and Hungary. According to this the proportion of computer using

[13] http://digital-agenda-data.eu/charts/desi-components#chart={"indicator":"DESI","breakdown group":"DESI","unit-measure":"pc_DESI","time-period":"2017"}

[14] www.ksh.hu/docs/hun/xftp/idoszaki/ikt15_1xls

enterprises in Hungary is 91%, which is not far from of the EU average. But the survey also shows that only 88% of businesses have Internet access in Hungary which is far from the EU average, which is 97%.

IV. Electronic administration in Hungary

There are basically three things needed in order to use the e-administration services:

- Basic infrastructure (internet access, computer, etc.)
- Basic knowledge about available public services via internet
- Identification of customers (citizens)

In Hungary the range of issues that can be accessed via the Internet is constantly expanding. There is a wide range of cases that can be done or at least initiated. Things that can be handled without a personal appearance can be launched online at any time and from anywhere. Issues that can be initiated begin with the submission of documents, but citizens still must be present in person at some stages during the process. But even in this case, administration is much faster than it was traditionally before.

Client Gate can be considered as the most important E-Government application in Hungary. It is the official central electronic administration web service of the country. The Client Gate service is currently available on www.magyarorszag.hu. To use the Client Gate a citizen needs to register, which can be done personally at any of the Government window.[15]

It can be used for administration and communication with the authorities, and some administrative procedures can be administered entirely online via the Client Gate (e.g. the annual tax declaration). In 2017 Client Gate reached 3 million registered users, more than two thousand forms are available for download (tax declaration, notification, account services, healthcare and social status and company registry inquiries, etc.) and it is also possible to fix an appointment for the physical Government Windows as well, and to launch the administration of many type of procedures. [16]

The fully online services of the Client Gate include: [17]

- services for employers and employees
- personal annual tax declaration and company tax declaration
- VAT declaration
- company registration (via an attorney-at-law)
- statistical data provision
- customs declaration
- e-Procurement

Company Gate is a service created for business organizations. It is similar to the Client Gate service, however, in the case of Company Gate, the business entity itself can register after the central identification. Previously in Client Gate all businesses were registered under the name of the owner citizen so one of the main intension of the creation of Company Gate was to separate citizens from business entities. Company Gate operates on a similar principle as Client Gate, but the scope of

[15] https://segitseg.magyarorszag.hu/segitseg/portal/latogatottsagi_adatok.html
[16] https://segitseg.magyarorszag.hu/segitseg/portal/latogatottsagi_adatok.html
[17] https://segitseg.magyarorszag.hu/segitseg/portal/latogatottsagi_adatok.html

services provided to citizens and businesses is being also separated. In addition from 2018 business entities are required to register at the Company Gate, because this electronic administration was made mandatory by the government. [18] Based on Act CCXXII of 2015 on the General Rules of Electronic Administration and Trust Services (E-Administration Act) business organizations, particularly companies, must communicate electronically with the state from 1 January 2018. [19]

With the help of the Company Gate, e-administration and communication, which is extensively extended to business organizations, is expected to be significantly more efficient and easier to follow. Faster, cheaper and more transparent for paper-based administration, time and cost savings for businesses. The electronically manageable groups of cases and the online forms will be expanded in this context further in the future. [20]

Basically it was created to help companies facilitate their operation. By using the Company Gate, communication with companies will completely changed, it allows all mails to arrive at a secure, trusted storage site assigned to the given business organization and they can also only be sent from there. A main difference from Client Gate is that not a person but the business organization itself will have a registration within it but in essence, we are talking about the Client Gate of the companies. The person authorized to sign up for a company can be leader of the company, but can also be someone else who is trusted with this administrative task within the company. [21]

The business portal has been introduced in other EU Member States as well before. An outstanding example is the Netherlands, where the launch of the AvB one-stop shop portal started in 2007. Users are individual businesses and business organizations that are thus given the opportunity to conduct electronic transactions beyond their customer retention time. The service has made it possible for customers to communicate more effectively with the authorities involved and to have easier access to information relevant to them. One of the main objectives of the introduction of the service is to reduce the administrative burden on businesses. The Dutch Institute for Economics and Policy Research, EIM, in a study, found that by running AvB as a single point of contact, the administrative burdens on a national level can be reduced by 65 million Euros. [22]

V. Conclusion

Governments are facing increasing expectations and greater demands from citizens about the range and quality of public services. These new expectations are driving public sector modernization, which continues to require systematic and consistent efficiency and productivity increases, especially in the larger service delivery areas of the public sector. The goal is to transform public service design and delivery provides a compelling context for greater use of digital technologies and assistive technological labor-saving solutions in the public sector. A digital government environment is largely user-driven, with users voicing their demands and needs and thereby contributing to shaping the government policy agenda.

[18] http://cegkapu.gov.hu
[19] http://cegkapu.gov.hu
[20] http://adokultura.hu/2017/08/14/kotelezo-belepni-a-cegkapun
[21] http://adokultura.hu/2017/08/14/kotelezo-belepni-a-cegkapun
[22] http://www.etudasportal.gov.hu/pages/viewpage.action?pageId=5079066#metadatas

E-government services strengthen competitiveness. The introduction of these services reduces the time spent on administrative tasks. In the time released, the business administrators can perform tasks that are more conducive to the profitable activity of the business. The use of e-government services also reduces the burden of paper-based administration, and electronically stored files can easily be retrieved.

Electronic administration is simpler and faster than traditional administration. E-administrative services indirectly strengthen the IT skills of businesses, because the use of these services also requires the existence of an IT infrastructure and the existence of the knowledge necessary to access these services.

As there are no available data yet in case of Company Gate because of its rather new nature in Hungary, it is not possible to conduct a further research in terms of administrative and financial advantages. But based on the foreign examples and the related strategies it can be expected to also reduce the burdens of the companies here in the future as well.

Acknowledgement

The paper was written with the support of the project titled "Internationalisation, initiatives to establish a new source of researchers and graduates and development of knowledge and technological transfer as instruments of intelligent specialisations at Széchenyi István University" (project number: EFOP-3.6.1-16-2016-00017).

REFERENCES

Bangemann Report (1994): Europe and the Global Information Society. Available: http://aei.pitt.edu/1199/1/info_society_bangeman_report.pdf

Budai Balázs Benjamin (2014): Az e-közigazgatás elmélete. Akadémiai Kiadó Zrt., Budapest.

Budai Balázs Benjamin, Tózsa István (2007): E-közigazgatás. Debrecen, Debreceni Egyetem,

Csáki Gyula Balázs (2009): Az elektronikus közigazgatás tartalma és gyakorlatának egyes kérdései. Doktori értekezés, Pécs.

Csáki Gyula Balázs (2010): Az elektronikus közigazgatás tartalma és egyes gyakorlati kérdései. HVGorac, Budapest.

Fáber Dávid (2002): Információs társadalom- eEurope 2005: Mindenki információs társadalma. Available: http://www.inco.hu/inco11/infotars/cikk1h.htm

Losoncz Miklos (2011): Az Európai Unió. Tri-Mester Bt., Tatabánya.

http://adokultura.hu/2017/08/14/kotelezo-belepni-a-cegkapun

http://cegkapu.gov.hu

http://www.etudasportal.gov.hu/pages/viewpage.action?pageId=5079066#metadatas

https://segitseg.magyarorszag.hu/segitseg/portal/latogatottsagi_adatok.html

www.ksh.hu/docs/hun/xftp/idoszaki/ikt15_1xls

http://digital-agenda-data.eu/charts/desi-components#chart={"indicator":"DESI","breakdown-group":"DESI","unit-measure":"pc_DESI","time-period":"2017"}

MAN VS ROBOT – VISION OF THE MODERN LUDDISM[1]

JÁCINT FERENCZ[2]

Abstract

We are facing great social and economic changes in the world: the fourth industrial revolution (Industry 4.0.) which is basically the technical integration of cyber physical systems into production and logistics and the use of the 'internet of things' and services in (industrial) processes – including the consequences for a new creation of value, business models as well. Within the next five years, it is expected that over 50 billion connected machines will exist throughout the world. The introduction of artificial intelligence in the service sector distinguishes the fourth industrial revolution from the third, completely changing the word of labor force, and as a consequence – changing every single life. Working people of the early 19th century has probably felt the same as the modern man today: technology is disfiguring the calm and safe routine of work-life balance, and demanding intensified attention from almost everybody in the labor market.
In this paper I examine how the 19th Century's luddism can be detected in today's society, and what is the reality of man and robots (which I see as the modern versions of industrial machines) working together in harmony.

Keywords: *robotics, labor law, neo-luddism*

I. Introduction

In 1982 Sar A. Levitan and Clifford M. Johnson suggested that the future of the work could belong to the robots. They were quoting data on a "study conducted at Carnegie-Mellon University asserting that the current generation of robots has the technical capability to perform nearly 7 million existing factory jobs -one-third of all manufacturing employment- and that sometime after 1990, it will become technically possible to replace all manufacturing operatives in the automotive, electrical equipment, machinery, and fabricated-metals industries."[3]

Are robots and modern technology changing the world we know today? Definitely. Is this progress threatening our everyday working routine? Sure it does. The only opened question is how we react on that change. This situation is such a complex one, that it is even hard to find a role model to adapt: while the billionaire high-tech guru Elon Musk runs his companies based on the new technology and artificial intelligence, he communicates that despite of perfectly good intentions but still companies "produce something evil by accident"—including, possibly, "a fleet of artificial intelligence-enhanced robots capable of destroying mankind."[4] In social sciences, on

[1] The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance" in the „Az állam gazdasági szerepvállalásának hatásvizsgálata egyes ágazatokban" Projekt.
[2] dr. Jácint FERENCZ PhD., associate professor, head of department, Széchenyi István University Faculty of Law and Political Sciences, Department of Trade, Agriculture and Labor Law. Email: ferencz@sze.hu
[3] Levitan, Sar A. – Clifford M. Johnson (1982): The future of work: does it belong to us or to the robots? Monthy Labor Review, September 1982, 12.p.
[4] Maureen Dowd: Elon Musk's Billion-Dollar Crusade To Stop The A.I. Apocalypse. Vanity Fair, April 2017. Available: https://www.vanityfair.com/news/2017/03/elon-musk-billion-dollar-crusade-to-stop-ai-space-x

one side some research state, that "not believing in the potential of artificial intelligence is like not believing in the potential of mathematics, physics, psychology, chemistry, engineering, etc. So not believing in the potential of artificial intelligence is like not believing in the potential of human intelligence."[5] The duplicity in this question arise also in the military field: Developing the right doctrine for using unmanned systems (and AI in them) is essential to the future of the force. If the any of the world's nations military gets it right, it will win the wars of tomorrow. If it does not, it might instead be on the way to building what one army officer called "the Maginot Line of the 21st century."[6]

In the medical sector we find perhaps the most promising approach of AI and robots by the use of robots as helpers; for example, a robot companion for the aging population with cognitive decline or limited mobility. Japanese carebots[7] are the most advanced forms of this technology. Robots are used in surgery as assistant-surgeons or even as solo performers.[8] At the same time others predict that too much perceived similarity between social robots and humans triggers concerns about the negative impact of this technology on humans, as a group, and their identity more generally because similarity blurs category boundaries, undermining human uniqueness.[9]

May sound weird, but the roots of the modern problem of AI can be found in the novels of famous science-fiction writer Isaac Asimov, who – I guess – would never believe while writing his books that his name would be quoted so many times in the near future in the academic literature.[10] But at the end, he got the point: how can we stop the robots (or something with autonomous decision-making power) to harm humans?

I would like to highlight this question from the labor law perspective: how can we find a close-to-optimal solution in the labor market to achieve the ideal quality and quantity of production parallel with the human satisfaction? In the title of this paper I suggested this process as a battle, where the party's interests are opposite, and where the robots has their own "rights and obligations" on the battlefield. But the truth is that on the side of the robots we find humans behind company's masks, who are representing mere economic interest. Several academic research has been made on the field of changing labor law both internationally and in Hungary.[11] In this paper

---

[5] Kyriakidou, Marilena (2017): Ethical concerns of surviving via and from robots: cyborgs and expiry dates. Manuscript. Available: http://www.worldscientific.com/doi/pdf/10.1142/9789813149137_0074

[6] Quoted by Singer, P.W. (2009): Wired for War? Robots and Military Doctrine. JFQ, Issue 52, 1st quarter 2009. p. 105.

[7] see in details: Larson, Jeffrey A. - Michael H.Johnson - Sam B.Bhayani (2014): Application of Surgical Safety Standards to Robotic Surgery: Five Principles of Ethics for Nonmaleficence Journal of the American College of Surgeons. Volume 218, Issue 2, February 2014, pp. 290-293.

[8] Hamet, Pavel - Johanne Tremblay (2017): Artificial intelligence in medicine. Metabolism Clinical and Experimental, Vol. 69, S36-S40.

[9] Ferrari, Francesco - Maria Paola Paladino - Jolanda Jetten (2016): Blurring Human–Machine Distinctions: Anthropomorphic Appearance in Social Robots as a Threat to Human Distinctiveness. International Journal of Social Robotics, April 2016, Volume 8, Issue 2, pp 287–302.

[10] See an analyzis of Asimov's work on regulation of robots here: Etzioni, Oren – Weld, Daniel (1994): The First Law of Robotics (a call to arms) AAAI Technical Report SS-94-03. pp. 17-23. Available: http://www.aaai.org/Papers/Symposia/Spring/1994/SS-94-03/SS94-03-003.pdf

[11] From the Hungarian literature some of the most interesting papers are: Kun Attila (2018): A digitalizáció kihívásai a munkajogban. In: Homicskó Árpád Olivér (szerk) Egyes modern technológiák etikai, jogi és szabályozási kihívásai. Acta Caroliensia Conventorum Scientiarum Iuridico-Politicarum XXII., Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, Budapest, pp. 119-137., and Gyulavári Tamás (2017): Munkajogi reformok az EU kelet-európai tagállamaiban: úton a munkavégzésre irányuló jogviszonyok új rendszere felé? MISKOLCI JOGI SZEMLE: A MISKOLCI EGYETEM ÁLLAM- ÉS JOGTUDOMÁNYI KARÁNAK FOLYÓIRATA 2: pp. 138-153., or Bankó Zoltán (2015): Elektronikus dokumentumok a munkajogviszonyban - a munkajogi jognyilatkozatokkal szemben támasztott követelmények a digitális világban. Available: http://www.kjmalapitvany.hu/sites/default/files/szakertoi-

I would like to ask the question if there is a possibility of a modern luddism movement, when we reach the time of robots taking most of the jobs of the current workers. I have no doubt that this time will come: in Germany there is already a software telling us how many percent of our job is possibly done by robots.[12] We can also find details on the possible future trends on the labor market –regarding our present job.[13]

II. Luddism and neo-luddism as social movements

There are several magnificent books and articles on modern age's similarity with the early 19th century's social movements. Here I would like to highlight Stephen A. Jones' great monography on neo-luddism[14], and Kirkpatrick Sale's book on the same subject[15], from which publications I got my starting point.

First of all, we should make it clear what the original luddites did and why, as luddism is a highly misunderstood phenomena. Despite their modern reputation, the original Luddites were neither opposed to technology nor inept at using it: many of them were highly skilled machine operators working in the textile industry. The idea of smashing machines as a form of industrial protest did not begin or end with them. [16]

The Luddite disturbances started in circumstances at least superficially similar to our own. British working families at the start of the 19th century were enduring economic upheaval and widespread unemployment. The key is in the labor-saving effects of some of the industrial innovations. The spinning jenny displaced around nine of ten warp spinners and thirteen of fourteen abb (weft) spinners. The scribbling engine displaced fifteen of sixteen scribblers. With the gig mill one man could do part of the work of a dozen shearmen, while the shearing frame made three of four shearmen redundant. Scribblers constituted around 10 percent of the preindustrial adult male work force, shearmen around 15 percent.4 Such men found their skills useless, their trade superfluous, when machinery was introduced. It is little wonder that their reaction was hostile.[17]

It is not hard to find similarities with today' robotics and their effect on labor force savings. According to the latest data of ILO from 2017, global unemployment levels and rates are expected to remain high in the short term, as the global labor force continues to grow. In particular, the global unemployment rate is expected to rise, representing 3.4 million more unemployed people globally (bringing total unemployment to just over 201 million in 2017). However, this unemployment differs in developed and developing countries: the number of unemployed people in emerging countries is expected to increase by approximately 3.6 million between 2016 and 2017,

palyazat/tanulm%C3%A1ny_banko_zoltan.pdf On the international literature we should mention the famous book of Martin Ford (2016): Rise of the Robots: Technology and the Threat of a Jobless Future. Oneworld Publications, Hungarian translation also available: Martin Ford (2017) Robotok kora - Milyen lesz a világ munkahelyek nélkül? HVG Könyvek Kiadó, Budapest.

[12] The program is available here: http://job-futuromat.iab.de

[13] Here I would recommend the following paper for further information: Dengler, Katharina - Britta Matthes (2018): Wenige Berufsbilder halten mit der Digitalisierung Schritt. IAB Kurzbericht 4/2018, Institut für Arbeitsmarkt- und Berufsforschung. Available: http://doku.iab.de/kurzber/2018/kb0418.pdf 1-12.pp.

[14] Jones, Stephen A. (2006): Against Technolog: From the Luddites to Neo-luddism. Routledge, New York-London.

[15] Sale, Kirkpatrick. Rebels Against the Future: The Luddites and Their War on the Industrial Revolution: Lessons for the Computer Age. Reading, MA.: Addison-Wesley, 1995.

[16] see the philosophy in details: Randall, Adrian J. (1986) The Philosophy of Luddism: The Case of the West of England Woolen Workers, ca. 1790-1809 Technology and Culture, 1986/1., pp. 1-17.

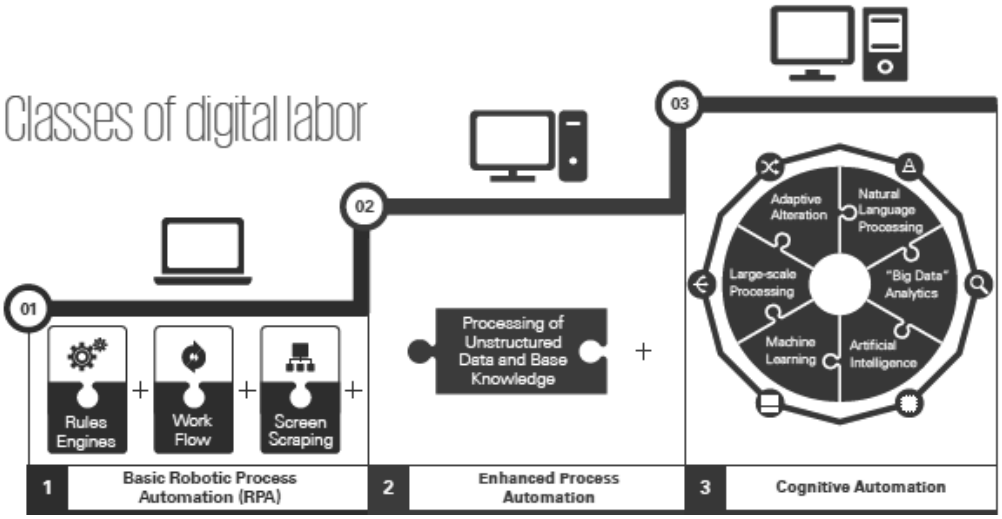
[17] ibid p. 2.

unemployment is expected to fall in 2017 in developed countries (by 670,000.)[18]. But this fall is derivable from other data, like the aging society, where less and less workforce is available on the market, so even those are getting jobs in developed countries who would be without work in a developing country.

The Luddites were neither as organized nor as dangerous as authorities believed. They set some factories on fire, but mainly they confined themselves to breaking machines. In truth, they inflicted less violence than they encountered. In one of the bloodiest incidents, in April 1812, some 2,000 protesters mobbed a mill near Manchester. The owner ordered his men to fire into the crowd, killing at least 3 and wounding 18. Soldiers killed at least 5 more the next day. Earlier that month, a crowd of about 150 protesters had exchanged gunfire with the defenders of a mill in Yorkshire, and two Luddites died. Soon, Luddites there retaliated by killing a mill owner, who in the thick of the protests had supposedly boasted that he would ride up to his britches in Luddite blood. Three Luddites were hanged for the murder; other courts, often under political pressure, sent many more to the gallows or to exile in Australia before the last such disturbance, in 1816.[19]

III. Digital labor force

The company KPMG draw a very informative picture on digital labor, as it can be seen in the next chart.



Source: KPMG 2017[20]

Under "Basic Robotic Process" the company means the following types of characteristics: repetitive in nature; well-defined explicit activities that are easily organized and sequenced; requires little to no tacit knowledge or cognitive assessment; involves multiple systems with data entry and

[18] ILO (2017): World Employment and Social Outlook: Trends 2017, International Labour Office – Geneva. p. 1.
[19] Richard Conniff: What the Luddites Really Fought Against. Smithonian Magazine, March 2011.
[20] KPMG (2017): Capitalizing on robotics. Driving savings with digital labor. Available: https://assets.kpmg.com/content/dam/kpmg/is/pdf/2017/03/capitalizing-robotics-digital-labor-savings.pdf

extraction; uses relatively structured and consistent data; and has something that can be used as an "electronic trigger" that would signal it is time to run/start the process.[21] When we examine this from the aspect of the employer who is now doing just the same we arrive to the point of this employee being easily substituted with a robot.

IV. Learning by doing: cloud robotics vs. human learning

In one of the many famous scenes in The Matrix (1999), the character Trinity learns to fly a helicopter by having a "pilot program" downloaded to her brain. For us humans, with our offline, non-upgradable brains, the possibility of acquiring new skills by connecting our heads to a computer network is science fiction. Not so for robots. Cloud robotics and so called "deep learning" are factors of innovation technology that are simply impossible to cope with for human beings. James Kuffner introduced the word "cloud robotics" in 2010[22], defining it as the phenomena when every robot learns from the experiences of all robots, which leads to rapid growth of robot competence, particularly as the number of robots growth. Cloud robotics recognizes the wide availability of networking, incorporates elements of open-source, open-access and crowdsourcing to greatly extend earlier concepts of "online robots" and "networked robots"[23]. Deep learning algorithms are a method for robots to learn and generalize their associations based on very large (and often cloud-based) "training sets" that typically include millions of examples.[24] The cloud allows robots and automation systems to "share" data from physical trials in a variety of environments, for example initial and desired conditions, associated control policies and trajectories, and importantly: data on performance and outcomes. Such data is a rich source for robot learning.[25]

Where are the human brains and learning methods against the upper mentioned techniques? Here we should have a look on the global education system. The National Academy of Science of the USA published a detailed study on the 21st century teaching. In the preface, they say that "business and political leaders are increasingly asking schools to develop skills such as problem solving, critical thinking, communication, collaboration, and self-management—often referred to as »21st century skills«."[26] In a document called the Partnership for 21st Century Skills[27] the parties argued that student success in college and careers requires four essential skills:

1. critical thinking and problem solving,
2. communication,
3. collaboration, and

---

[21] ibid p.4.

[22] quoted here: Goldberg, Ken - Ben Kehoe (2013): Cloud robotics and automation: A survey of related work. Technical Report UCB/EECS-2013-5, EECS Department, University of California, Berkeley, Jan 2013. Available: http://digitalassets.lib.berkeley.edu/techreports/ucb/text/EECS-2013-5.pdf

[23] ibid p.1.

[24] Pratt, Gill A.: Is a Cambrian Explosion Coming for Robotics? Journal of Economic Perspectives, 2015/3. p. 51.

[25] Goldberg – Kehoe (2013) p. 3.

[26] National Research Council (2012). Education for Life and Work: Developing Transferable Knowledge and Skills in the 21st Century. Committee on Defining Deeper Learning and 21st Century Skills, James W. Pellegrino and Margaret L. Hilton, Editors. Board on Testing and Assessment and Board on Science Education, Division of Behavioral and Social Sciences and Education. Washington, DC: The National Academies Press. Electronic copy available: http://www.nap.edu/catalog.php?record_id=13398

[27] P21, The Partnership for 21st Century Learning (formerly the Partnership for 21st Century Skills, joined also by the U.S. Department of Education) was founded in the United States in 2002 as a coalition bringing together the business community, education leaders, and policymakers to position 21st century readiness at the center of US K-12 education and to kick-start a national conversation on the importance of 21st century skills for all students.

4. creativity and innovation.

On the field of collaboration humans have not too much hope: while we feel sympathy, we are having "sixth sense" of somebody that influences the joint work, while we have sensible friends and family, collaboration will always be problematic for mankind. Communication, which seems to be a "mission impossible" for teenagers (and even for a large part of adults as well) does not seem even to be a problem for robots: we know that Google's company Area 120 has created a chat-automat, advertising the service like this: "*You probably get a lot of chat messages. And you want to be there for people, but also for people in the real world. What if replying were literally one tap away?*" The service is available from 20th February 2018, and during set up, the user can give Reply permission to the notifications, location, and calendar. Using these, it not only give the user quick responses to messages, but it also mutes the phone while driving, running, etc., automatically responds to tell people the user is on vacation based on the calendar appointments, unmutes your phone when an urgent text comes through, and so much more.[28] Does it sound like a secretary-robot? Definitely. But will this robot know that a new partner's call is urgent? Will this technology be discreet like a real secretary is in important matters? Here is a clear hole on the perfect robotic world!

What are the areas in which human can be better than robots at the end? Creativity and innovation is the clear answer, and in some cases the critical thinking and problem solving – when extraordinary creativity is needed to solve a problem.

[28] Source: Justin Duino: Reply, Area 120's smart quick response application, is available to download. https://9to5google.com/2018/02/20/reply-google-area-120-now-downloadable/

REFERENCES

Bankó Zoltán (2015): Elektronikus dokumentumok a munkajogviszonyban - a munkajogi jognyilatkozatokkal szemben támasztott követelmények a digitális világban. Available: http://www.kjmalapitvany.hu/sites/default/files/szakertoi-palyazat/tanulm%C3%A1ny_banko_zoltan.pdf

Dengler, Katharina - Britta Matthes (2018): Wenige Berufsbilder halten mit der Digitalisierung Schritt. IAB Kurzbericht 4/2018, Institut für Arbeitsmarkt- und Berufsforschung. 1-12.pp.

Etzioni, Oren – Weld, Daniel (1994): The First Law of Robotics (a call to arms) AAAI Technical Report SS-94-03. pp. 17-23.

Ferrari, Francesco - Maria Paola Paladino - Jolanda Jetten (2016): Blurring Human–Machine Distinctions: Anthropomorphic Appearance in Social Robots as a Threat to Human Distinctiveness. International Journal of Social Robotics, April 2016, Volume 8, Issue 2, pp 287–302.

Ford, Martin (2017): Robotok kora - Milyen lesz a világ munkahelyek nélkül? HVG Könyvek Kiadó, Budapest.

Goldberg, Ken - Ben Kehoe (2013): Cloud robotics and automation: A survey of related work. Technical Report UCB/EECS-2013-5, EECS Department, University of California, Berkeley, Jan 2013.

Gyulavári Tamás (2017): Munkajogi reformok az EU kelet-európai tagállamaiban: úton a munkavégzésre irányuló jogviszonyok új rendszere felé? Miskolci Jogi Szemle: A Miskolci Egyetem Állam és Jogtudományi Karának folyóirata 2: pp. 138-153.

ILO (2017): World Employment and Social Outlook: Trends 2017, International Labour Office, Geneva.

Kun Attila (2018): A digitalizáció kihívásai a munkajogban. In: Homicskó Árpád Olivér (szerk) Egyes modern technológiák etikai, jogi és szabályozási kihívásai. Acta Caroliensia Conventorum Scientiarum Iuridico-Politicarum XXII., Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, Budapest, pp. 119-137.

Kyriakidou, Marilena (2017): Ethical concerns of surviving via and from robots: cyborgs and expiry dates. Manuscript. Available: http://www.worldscientific.com/doi/pdf/10.1142/9789813149137_0074

Larson, Jeffrey A. - Michael H.Johnson - Sam B.Bhayani (2014): Application of Surgical Safety Standards to Robotic Surgery: Five Principles of Ethics for Nonmaleficence Journal of the American College of Surgeons. Volume 218, Issue 2, February 2014, pp. 290-293.

Levitan, Sar A. – Clifford M. Johnson (1982): The future of work: does it belong to us or to the robots? Monthy Labor Review, September 1982, pp. 10-14.

National Research Council (2012). Education for Life and Work: Developing Transferable Knowledge and Skills in the 21st Century. Committee on Defining Deeper Learning and 21st Century Skills, James W. Pellegrino and Margaret L. Hilton, Editors. Board on Testing and

Assessment and Board on Science Education, Division of Behavioral and Social Sciences and Education. Washington, DC: The National Academies Press.

Pratt, Gill A.: Is a Cambrian Explosion Coming for Robotics? Journal of Economic Perspectives, 2015/3. pp. 51-60.

Randall, Adrian J. (1986) The Philosophy of Luddism: The Case of the West of England Woolen Workers, ca. 1790-1809 Technology and Culture, 1986/1., pp. 1-17.

Singer, P.W. (2009): Wired for War? Robots and Military Doctrine. JFQ, Issue 52, 1st quarter 2009. pp. 104-110.

PRIVACY ON FACEBOOK

RASTISLAV FUNTA[1]

Abstract

Facebook is the most preferred social network. It is used by individuals privately, but also to promote a particular company or project, to win new fans or to communicate with the readers. Facebook's interface allows users to post, share and annotate texts, events and photos. But there are many open questions: How private is my Facebook profile? What am I allowed to post without violating copyrights? What is Facebook doing with my data I publish? How does Facebook follow me on the web? What are tracking cookies and how do they work? The most important goal of this article is to provide insight into how Facebook works in order to be more aware of social networks.

Keywords: *Facebook, IT Markets, Privacy*

I. Introduction

Social networks are mainly used as a contact point and for sharing content with friends and colleagues. Users upload their photos, post a press article on their profile and press the "share" button. When can this practice become a copyright issue? Many Facebook users may think, "What do I have to do with copyright infringement? I only share the content with my friends!" Users should not feel safe just because it is not so easy to keep control over the actual distribution of content on Facebook. If, for example, the visibility is set to "friends of friends", you can quickly reach ten thousand people, if one calculates that a Facebook user has an average of 100 friends. With just one click, content previously restricted to "friends" can be made accessible to everyone on the web.

II. Private frame apparently unimportant for Facebook?

It remains unclear to what extent Facebook itself makes the difference between public and private. The users are prohibited to post content that violates copyright of third parties. Facebook does not seem to assume that users upload external content (photos, music, videos) because elsewhere in the terms of use is stipulated that: "You own all the content and information that you post on Facebook." With this somewhat vague formula Facebook seems to protect against copyright hassles by the users. At the same time, Facebook is committed to respect the intellectual property of third parties. "When we receive a valid representation of the infringement of intellectual property rights, we immediately block or remove access to the allegedly infringing content," the company said. Repeat offenders can be blocked. Anyone who hopes that his postings on Facebook will

[1] Dr. Rastislav FUNTA, Ph.D.(Prague), LL.M.(Budapest), Vice-Dean at the Danubius University, Janko Jesensky Faculty of Law. rastislav.funta@vsdanubius.sk

remain private and make protected works accessible to others without permission risks that his Facebook account will be blocked.

II.1. Copyright: upload and post external content

Users should always think about how to make foreign content available on Facebook. Although it is disputed among experts, whether a private Facebook profile is legally to be seen as a home page of the user. Link to external content is usually not a problem. The user can copy the address of an Internet page (URL) into the Facebook field "status", press the "like" button and display this activity in his profile on Facebook. It remains unclear to the private user, for example, if large media houses have acquired rights[2] of use for the original photos, which also cover the display of thumbnails (preview images) by Facebook members. Also unclear is whether Facebook is jointly responsible, because the preview image is automatically preset, and the user must turn it off actively to avoid any copyright infringement. For individuals, certain serenity is recommended. If a copyright owner complains, users should turn off the preview to avoid unnecessary litigation. Videos that obviously infringe copyrights (such as Hollywood blockbusters) should generally not embed the user, even on Facebook. The same applies to recognizable criminal content, such as inciting propaganda. In the classic case of a music video on one of the big video portals such as YouTube or Vimeo, the source is certainly not "obviously unlawful" - after all, YouTube uses a filter system and many copyright holders have license agreements with the operators of the video portals.

III. Own content: to consider foreign rights

Self-created content is usually easily shared by users on Facebook. However, there are some exceptions where someone else's rights may be violated. Classic examples represent cell phone videos of concerts, theater visits or soccer matches. As a rule, the organizers prohibit the filming or at least the distribution of live recordings. On the other hand, the performers have certain rights to their performances, which allow them a legal control over recordings. In particular photographing of others in private rooms can be problematic. Who made such photos without authorization makes itself liable to prosecution (according to the Criminal Code), even if this offense is rarely reported and prosecuted. Friends regularly surprise each other with snapshots on Facebook. This is usually not a problem. Nevertheless, it is advisable to develop a sensitivity for interfering into personal rights (even of friends). Should I really share the photo with the public so everyone on the web can see it? Can the employer, the teacher or the family of the person concerned see the photo if I unlock it for "friends of friends"? For example, it should be remembered that services like Facebook have automatic face recognition software. Although it has not yet been definitively clarified whether and how Facebook is allowed to use this software legally in the EU. By law, anyone can request that its photo be taken out of Facebook, if it is placed there without permission.

[2] Svák, J. (2006).

IV. What rights does the user give to Facebook?

More than one billion members worldwide now use Facebook. Users upload 300 million photos daily. There are always rumors that the user loses the copyright of his works, which he posts on Facebook. This is wrong. The user retains his copyright until death. The question is, however, which user license the author gives to Facebook, if he uploads a copyrighted work (called "IP content" on Facebook). It is stated in the "statement of rights and Responsibilities" that "you give us a non-exclusive, transferable, sub licensable, royalty-free, worldwide license to use any IP content you post on or in connection with Facebook ("IP License")." The "Non-exclusive" means that the user with his works outside of Facebook can continue to do largely what he wants. It is a so-called simple (general) right of use, which is granted to Facebook. The user may therefore publish his photos elsewhere or sell the rights to others, but he can no longer transfer "sole" or "exclusive" rights of use to other persons as long as Facebook has the above-mentioned simple right of use. To assign exclusive rights elsewhere, the user would first need from Facebook to withdraw the simple right of use. But this can be complicated. The IP license ends, according to Facebook with the deletion of the content, but only if it was not shared with other users. In a nutshell: in extreme cases, the user would have to ask thousands of other users who shared his works (photos, videos, music, texts) to delete the shared work. This uncertainty may be a reason for professional photographers, musicians and filmmakers not to publish their works on Facebook.[3] More difficult is the question of what the words "transferable" and "sub licensable" follow. In theory, Facebook may allow third parties who use the works of a member and gain licenses. How far this may go remains unclear, since the types of use are not specifically limited. It is clear that friends can see photos that the user shares with them. But whether Facebook can allow another company to use a vacation photo of the user for an advertising campaign is difficult to day. On the one hand, the user grants the IP license via his privacy and application settings.[4] The user could therefore argue in the case of the advertising campaign, that he wanted to share the photo on Facebook only with his friends, and not with any other company. On the other hand, the user does not just share the photo with his friends, but also with Facebook, which in turn reserves itself one sub-licensing. Ultimately, courts would have to determine how far Facebook may go if it use works of its members and if the intended purpose of the contract includes, for example, the sale of rights of use to third parties. Facebook itself points out that users' trust is fundamental to its own business model: "If you do not feel that you control who can see the content you share, you use Facebook probably less often and share less content with your friends. That would neither be in the sense of Facebook nor in your sense, "it says on the Facebook corporate webpage. But Facebook could also go the other way and examine business models based on stronger commercialization of user content. As a listed company, it is always under pressure to achieve returns. In regards to free social networks in principle applies, that the user and his data are the product itself. The Facebook user should be aware of the legal framework of his "digital living room". Before content is uploaded on Facebook, everybody should briefly check the following points: Do I intervene into third-party copyright and personal rights if I make my own and third-party content available? Would I agree with an appropriate publication? What does the content say

[3] Svantesson, D. J. (2015).
[4] Rottenberg, M. - Scott, J. - Horwitz, J. (2015).

about me and could he possibly be misunderstood? And Finally: Do I want to give Facebook a simple license to use my works?

V. Privacy[5] on Facebook: Who owns my data?

The social network Facebook is polarizing. On the one hand, its benefits can hardly be denied: friends exchange views on the platform,[6] share photos, videos and texts, post and discuss network content and follow the many activities. Even with friends who live on the other side of the globe, Facebook allows uncomplicated contact. On the other hand, more and more users worry because they pay with their data for the free service. Facebook is not alone in its practices - other social networks use similar technology, collect and publish data in a similar way. Many providers have their headquarters abroad - Facebook has its EU headquarter in Ireland, where the privacy policy is less stringent than e.g. in Germany. Facebook Ireland is responsible for all users outside the US and Canada. That's why European solutions are so important because it's the only way how to meet the minimum standards. Essentially, Facebook's business model is based on being a personalized advertising platform. The better Facebook knows its members, the better it can sell ads to companies that end up on the screens of potential customers. If we follow the official statements of Facebook, then the extensive data collection serves two commercial purposes: First, the operation and improvement of the service - and thus the user retention and gaining new members - and second, the optimization of advertising.

V.1. Privacy Issues: If third parties want access

Many scenarios can be devised in which data collection by Facebook could become problematic. Law enforcement agencies sometimes work with the data they find on social networks.

Many employers also want to have access on the data in social networks. There are cases in which employees who have criticized their company or superiors on their Facebook profile have lost their jobs. But it always depends on the individual case. Data from social networks could also be used to assess the creditworthiness of certain users, and to make offers or deny them accordingly. Basically, users have to decide to what extent they trust Facebook, when they reveal their data to the company. However, it is relatively difficult to change the social network we use, if we want to keep the contents and especially the contacts. It is not easy to make an informed decision as to whether we want to share out data with Facebook because corporate policies are cumbersome or unclear - which privacy advocates routinely criticize. Another problem is that Facebook changes its privacy preferences without the users' consent. When new features are released, they are regularly pre-set so that as many users as possible see them.

[5] Funta, R. (2017).
[6] Funta, R. (2017).

VI. What data are collected by Facebook

The data that Facebook collects about the individual user can be found in different categories. First there are the registration data, i.e. the name, place of residence, birthday, gender and e-mail address. Users may voluntarily disclose other personal information, such as school they visited and where they work. In addition, there are data that users can disclose, such as likes, comments, status reports, participating in groups and events, linking and postings (photos, videos, texts), and communicating via the mail or chat function. Facebook stores the "metadata" of uploaded photos and videos. Facebook also captures the type of device (smartphone, tablet, computer, etc.), the IP address, and the location of the active user.

VII. Cookies and tracking via "like" button and Facebook ID

Our "likes" details provide a lot about us. IT researchers are able to estimate quite accurately, whether a Facebook user is female or male, homosexual or heterosexual, Christian or Muslim. But the "like" button reveals even more: When websites use so-called "social plugins" (Facebook applications such as "like" or "share" functions), visitors' data are sent to Facebook. We do not have to be logged into Facebook or to have a Facebook account, or to click on the "like" button. This happens because the buttons on a so-called iFrame of the Facebook servers are loaded. As a result, Facebook automatically know who has called up a corresponding page. The data that is transferred includes the language settings, the location of our computer, the web browser used, the screen resolution and much more. In addition, the IP address can be made visible. Facebook declares to delete or anonymize the data received within 90 days. If we have a Facebook account and are logged into it while we are online (even no Facebook window has to be open), we will be identified by so-called cookie. Registered Facebook users have Facebook identification number ("Facebook ID"). If users move to websites outside of Facebook, where "social plug-ins" are integrated, the tracking cookies send this information to Facebook. If one is logged out, this Facebook ID is removed, so that no personal tracking data is collected. Not all cookies are deleted, only those that allow us to connect the tracking data to our own Facebook account.

VIII. Data by games and applications

Users can play games and access applications via the Facebook account. Small apps are added to the Facebook profile. These applications are also called apps and have their own Facebook page, the App Center. When adding an app or game, Facebook automatically provide the publicly available user information such as name, age and gender (general profile) and the friends list to the third-party provider. However, the applications may ask for more information, and require access to messages, photos or "likes" information. Before users give their permission, they should carefully consider whether they trust the provider of the application. Which access rights one have granted to the applications can be checked in the privacy settings.. We have to agree before the installation process will be started, but many users are very careless and do not check what rights they give to the application. This may mean that providers about which we know less than about Facebook can get personal information about us. We do not have to give the application access to our entire profile. Many apps also work if they are only allowed to access restricted Facebook data.

IX. Immediate personalization and single sign-on

Two other application examples in which Facebook's personal data of the own profile are provided to other web providers, are on the one hand the "immediate personalization" and on the other the so-called "single sign-on". In the case of on-going personalization, Facebook has entered into an agreement with certain providers that allows to read user data from the public profile (name, user number, username, profile picture, gender and network, age group, language, country and friends list) so that these providers can immediately display content (e.g. advertising) that is based on the previous behavior or on the interests of the users (for example the likes or the behavior of our friends). Offers with immediate personalization include companies like Scribd, TripAdvisor, but also game providers like Zynga or EA. If we do not want this, we can always deactivate the immediate personalization (under Application Settings> Immediate Personalization). The single sign-on gives the users the opportunity not to create a separate login and user profile for each website. We can sign up for a new web service with our Facebook or Google[7] account. In this case we will be redirected to the respective page where we have to confirm that we allow Facebook to send our data to the other provider. There is a controversy about the anonymous use of Facebook. The Facebook terms of use require that the user choose his real name and not a pseudonym. Users who violate this rule may be locked out from the network.

X. Transparency: How do I know what data have been collected by Facebook?

Under EU law, every citizen has the right to know which personal data about him were stored.[8] When using Facebook a lot of data are collected: personal information, photos, likes, links, shared content, comments on our profile and on other places. Facebook provides a link in the "general account settings" that allows users to download their data stored on Facebook. There are two options: the normal and the extended archive. The extended archive, which has to be created and downloaded separately, also contains other account information such as logins, cookies, applications, chat logs, the last place we logged on Facebook, and much more. Even if we do not have a problem with Facebook's data-gathering rage, it's interesting to see how much of our life's details have been made accessible and quasi-public.

XI. Conclusion: To delete Facebook account or not?

One would think to delete his Facebook account should not be a problem. But it is not that easy. At first glance, the network offers its users only the possibility to deactivate the account. But all user data remains; they are just not seen anymore, neither by friends nor by others. But: Facebook still has the data. If we later decide to continue using Facebook, we can start from where we left the network. If we have requested the deletion of our account, it may take a while until the account

[7] More about Google and the proceedings can be found under: Funta, R. (2014): Some remarks on the Google ECJ ruling (C-131/12).
[8] Funta, R. (2011); Karas, V. - Králik, A. (2012).

is really gone.[9] Facebook delays the final deletion by about 14 days, should we change our mind. If we log in within this time on Facebook, the deletion is stopped. It takes about 90 days for all of the related data to be deleted. The exit from Facebook is not so easy - but possible, anyway for a great part. Again, this is due to the work of privacy advocates. Many of the features have been introduced by Facebook only after there were protests from users or privacy advocates complaining about it. That's why it's even more important for every user to engage with this topic - because only informed users can help shape this important area of digital life.

This article is part of the EU project of the Danubius University through which we support research activities in Slovakia [ITMS 26210120047].

[9] Funta, R. (2018).

REFERENCES

Funta, R. (2018): Facebook from competition law perspective, In. Justičná revue, No. 1.

Funta, R. (2017): Privacy protection and the transfer of personal data between EU and USA, In. Justičná revue, No. 8-9.

Funta, R. (2017): EU competition law policy and on-line platforms, In. EU Law Journal, Vol. 2. No. 1.

Funta, R. (2014): Some remarks on the Google ECJ ruling (C-131/12), In. Krytyka Prawa-Akademia Leona Kožmiňskiego, Krakow.

Funta, R. (2011): EU-USA Privacy Protection Legislation and the Swift Bank Data Transfer Regulation: A Short Look, In. Masaryk University Journal of Law and Technology, Issue 1.

Karas, V. - Králik, A. (2012): Právo Európskej únie, 1.vydanie, C.H.Beck, Bratislava.

Rottenberg, M. - Scott, J. - Horwitz, J. (2015): Privacy in the modern age: The search for solutions, The New Press, New York.

Svák, J. (2006): Ochrana ľudských práv, Poradca podnikateľa, Bratislava.

Svantesson, D. J. (2015): The (Uncertain) Future of Online Data Privacy, In. Masaryk University Journal of Law and Technology, Issue 2.

THE FUTURE OF PUBLIC PROCUREMENT: INNOVATION AND BLOCKCHAIN TECHNOLOGY

JUDIT GLAVANITS[1]

Abstract

According to the latest statistics of the OECD, the sheer size of public procurement, approximately representing 12% of GDP in OEDCD countries, makes it a key economic activity - it ranges from 5.1% in Mexico to 20.2% in the Netherlands.[2] Spending such an amount on construction, buying goods and services for education, defense and social protection and on economic affairs in general, effectiveness is crucial from the aspect of the public interest. The design and principles of governmental spending can play a role model for the business sector: if we put the focus on innovation and transparency it can make the whole supply chain more trustworthy. In the last decade governments and regional, global regulators made significant efforts towards the general application of e-procurement to make the process much cost-effective and easier for small and medium sized enterprises to join. However, it is worldwide known that the mismanagement and the corruption are still basic risks of the public procurement system, and for this reason the innovation in supply methods, such as the blockchain technology can be a solution for a better public spending in the future.

Keywords: e-procurement, blockchain, DLT, public purchase, corruption

I. Greening, e-procurement and innovation goals of the last decade

According to the European Commission's statistics, EU the Member States are spending about 14% of the GDP through public procurement contracts.[3] The percentage of GDP is even higher when taking into account state-owned companies such as utilities providing, for example, water and electricity services.[4]

Public actors and anyone under the scope of any public procurement laws are being encouraged to procure sustainably, to reduce their social and environmental footprint and also in order to stimulate sustainability in the private sector.[5] Green public procurement (GPP), i.e. public purchasing of products and services which are less environmentally damaging when taking into account their whole life cycle, is increasingly used by countries to achieve such policy objectives in the area of environmental protection.[6] Looking back to the roots of the green and innovative public procurement, in 2002 the OECD adopted the "OECD Council Recommendation on the Environmental Performance in Public Procurement", flowed by another Recommendation in 2008 and in 2012. Sustainable procurement policies have been launched in many OECD countries (USA, Japan, Canada, Australia, and South Korea) as well as in rapidly developing countries (such as

[1] dr. jur. Judit GLAVANITS PhD, associate professor, head of department, Széchenyi István University, Faculty of Law and Political Sciences, Department of Public and Private International Law. Email: gjudit@sze.hu
[2] OECD (2017) p. 172.
[3] European Commission (2017) p. 1.
[4] OECD (2012b) p. 5.
[5] Brammer, Stephen – Helen Walker (2011) 452. p.
[6] OECD (2015) 5.p.

China, Thailand, and Philippines). In 2007, an OECD survey indicated that the most common barrier to successfully implementing green procurement was a lack of know-how among procurement officials on how to achieve it. As a response, by 2010 more than three quarters of the Members have introduced practical guides on green procurement.[7]

Alongside the "greening" process we can also see the emerging importance using electronic methods in public procurement process. Generally speaking e-procurement is a catch-all term for the replacement, throughout the procurement process, of paper-based procedures with communications and processing that are based on information technology.[8] The OECD defines e-procurement the integration of digital technologies in the replacement or redesign of paper-based procedures throughout the procurement process.[9]

We can summarize the importance of e-commerce and e-procurement with the words of Jean-Claude Juncker, who said: "*Digital technologies are going into every aspect of life. All they require is access to high speed internet. We need to be connected, our economy needs it, people need it.*"[10]

A report from the United States examined the innovation aspects of the public procurement in the county in 2011 resulting that the extent of innovation achieved through public procurement varies a lot across government. Outside of the national defense/security area, innovation is not an end but a means towards achieving some social purpose such as environmental protection, energy conservation, assisting disadvantaged groups in the population, and so forth.[11] Still, the innovation was not a basic principle in the world's biggest economy's public purchase.

Speaking about the existing risks on overall public procurement system, we can generally summarize them in terms of insider-driven specifications, low visibility of procurement processes, and ample opportunities for renegotiation of terms[12]. In the next chapter I examine how e-procurement and the possible introduction of blockchain-based procurement may result in a better functioning of public purchase.

II. E-procurement at the focus

II.1. General advantages and regulation

The joint project of OECD and the EU, SIGMA research team (or SIGMA project) collected the most important advantages of e-procurement:

- reduced administrative costs of individual procurement procedures;
- streamlined procurement procedures;
- faster procurement procedures;
- increased transparency, by providing information about individual tender opportunities, but also providing a clearer picture of tenders on a wider basis;
- better monitoring of procurement;
- encouragement of cross-border competition, by reducing barriers presented by paper-based procurement processes;

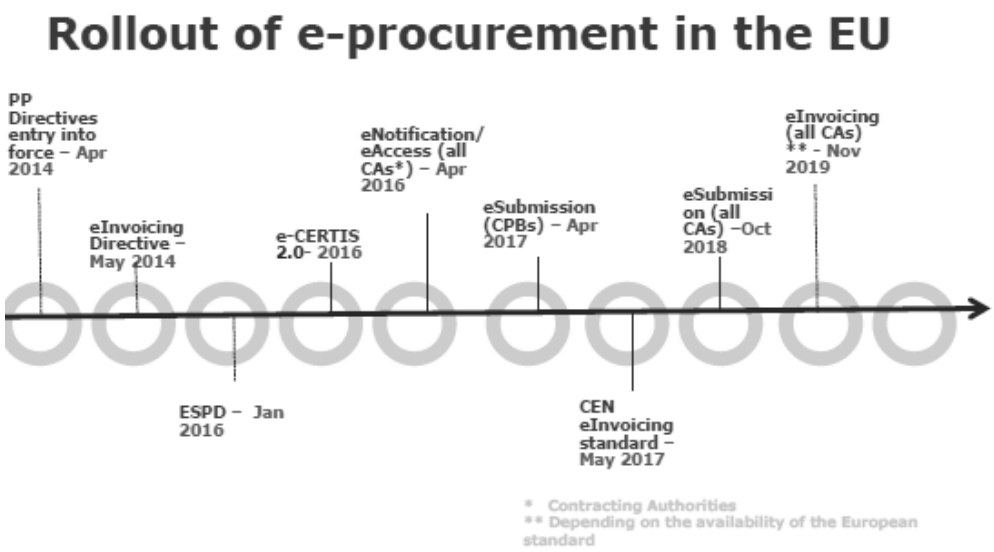
[7] OECD (2012a) 37.p.
[8] See the early motivations of introducing e-procurement here: Davila, Antonio – Mahendra Gupta – Richard Palmer (2003) pp. 11-23.
[9] OECD (2015) p.6.
[10] State of the Union Address, European Parliament, 14 September 2016
[11] Vonortas, Nicholas S – Pushmeet Bhatia – Deborah P. Mayer (2011) p. 3.
[12] See in details: Dorn, Nicholas - Michael Levi - Simone White (2008) pp. 243-260.

- support to the development of centralized procurement administration, resulting in the potential reduction of costly back-office procurement functions and the good use of economies of scale in procurement administration;
- wider administrative modernization and simplification, encouraging the integration of various administrative processes as well as the diffusion of information technology solutions within and by government and society in general.[13]

In 2014 the EU has adopted 3 new directives regulating the public procurement in the EU member states. Among these the 24/2014/EU Directive directly effects the national regulation as a whole. Preamble articles (52)-(57) are dealing with the general problem of electronic means of information and communication. As a principle, the Directive prescribes that types of e-procurement should become the standard means of communication and information exchange in procurement procedures. For that purpose, transmission of notices in electronic form, electronic availability of the procurement documents and – after a transition period of 30 months – fully electronic communication, meaning communication by electronic means at all stages of the procedure, including the transmission of requests for participation and, in particular, the transmission of the tenders (electronic submission) should be made mandatory.[14] According to Article 22, Member States shall ensure that all communication and information exchange under the Directive, in particular electronic submission, are performed using electronic means of communication in accordance with the requirements of this Article. The tools and devices to be used for communicating by electronic means, as well as their technical characteristics, shall be non-discriminatory, generally available and interoperable with the ICT products in general use and shall not restrict economic operators' access to the procurement procedure. The deadline for harmonization of the national regulation was 18th October, 2018.

Table 1.

[13] SIGMA (2016)
[14] Preamble article (52) of the Directive



E-procurement timeline of the EU member states

Source: European Commission

II.2. Regulation of e-procurement in Hungary

From some aspects of e-procurement, the Hungarian government had been too fast in harmonization: when the Act came into force on 1st November 2015, the European Single Procurement Document (ESPD) was not ready yet, it was only published on 5th January 2016 by the European Commission[15], however the Hungarian Act prescribed its mandatory use in EU-level processes with suspending this rule's effect until the Commission is publishing the ESPD.

This was not the only field of being more dedicated than prepared: the first planned date for fully electronic procurement was 1st February 2017, than modified to 31st December 2017, but in early December 2017 it became clear that the new e-procurement system is not ready yet, so another modification in the Act postponed the date to 15th April, 2018. During 1st January- 15th April 2018 there are two parallel systems operating in public procurement: the purchaser has the right to choose to start the process electronically, or paper-based.

According to the regulation in effect today, in public procurement and concession award procedures the single electronic procurement system maintained by the Miniszterelnökség (Prime Minister's Office) shall be used [Article 40 (1) of Act CXLIII of 2015). The Prime Minister's Office operates the Electronic Procurement System (EKR) since 1st January 2018, harmonizing the national law far earlier than the deadline in the Directive.

The innovation partnership, as a brand new type of procedures can be an indicator of the spreading of innovative public procurements. This new procedure allows for the combination of development and purchase elements tailored to public requirements, with specific rules in place to ensure equal treatment and transparency.[16] According the preamble Article (49) of the EU Directive

[15] Commission Implementing Regulation (EU) 2016/7 of 5 January 2016 establishing the standard form for the European Single Procurement Document
[16] European Commission (2016)

this procedure "*should allow contracting authorities to establish a long-term innovation partnership for the development and subsequent purchase of a new, innovative product, service or works provided that such innovative product or service or innovative works can be delivered to agreed performance levels and costs, without the need for a separate procurement procedure for the purchase. The innovation partnership should be based on the procedural rules that apply to the competitive procedure with negotiation and contracts should be awarded on the sole basis of the best price-quality ratio, which is most suitable for comparing tenders for innovative solutions*." The innovation partnership process takes place in three phases: *(1) the competitive phase* takes place at the very beginning of the procedure, when the most suitable partner(s) are selected on the basis of their skills and abilities. The contracts establishing the innovation partnership are awarded using the criteria of the best price-quality ratio proposed. (2) during *the development phase*, the partner(s) will develop the new solution in collaboration with the contracting authority. This research and development phase can be divided into several stages during which the number of partners may be gradually reduced, depending on whether they meet predetermined criteria. (3) Finally in *the commercial phase*, the partner(s) provide the final results. In the Hungarian regulation this means only two phase in practice: first one is the procedural phase, when the contracting party is choosing one or more partners from the applicants, and the second phase is contracting, when the deal is finished with the partnership agreement.[17]

As this is a completely new type of procurement, we might think that some time should pass to see this procedure in action after the new Regulation on public procurement is in force. However, until 31st December 2018 not a single procedure has been made under the new rules in Hungary. Examining whether the failure of the Hungarian practice is unique in the EU, we can see the UK, where the Crown Commercial Service issued a guidance on the application of innovation partnerships,[18] and since the enactment on the new regulation we can find 28 procedure on the TED database containing innovation partnership (until 31st December 2018). In case of Norway (which country is not an EU-member state…), where we can detect 8 procedures, but Germany is also very active with 28 procedures.

If we summarize that there are about 300 procedures finished or still in process until 31st December 2018, we can say that this kind of process is getting into the practice quite slowly, but certainly. However, we have to take into consideration that in some countries the EU-harmonized regulation is only in effect since two years.

III. Blockchain and public procurement: a possible future trend?

As the number of contracting public authority who are committed to sustainable and innovative public procurement grows, the practitioners will find the optimal ways to reach the GPP goals. This way the main task for regulators is to promote GPP and innovation-driven procurement, and create a regulatory background (flexible enough). Education and specialized training programs are crucial for labor force and specialists working on the field of public procurement.

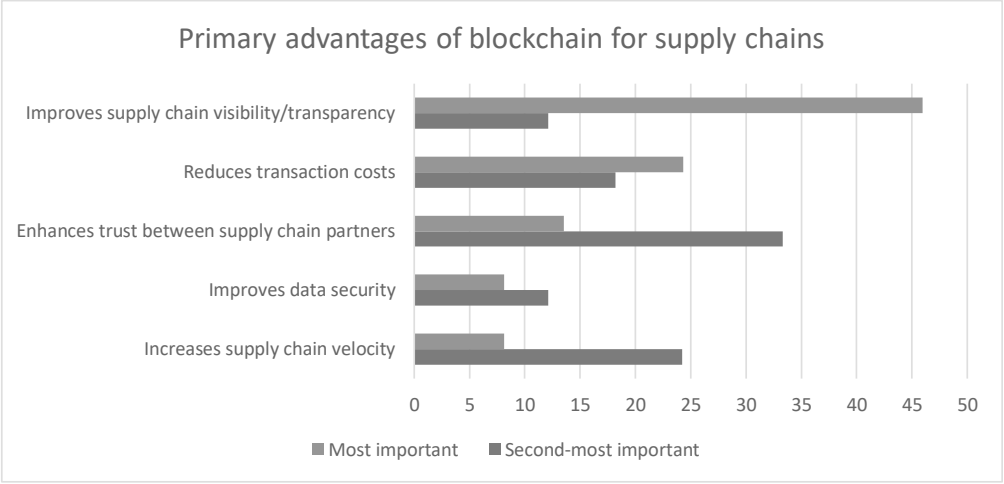
In the case of e-procurement time is obviously crucial: with the growing knowledge on the possible advantages of blockchain technology, there will be a need for even a more transparent and corruption-fighting system.

[17] Kbt. 95. § (2)
[18] See: Crown Commercial Service (2016)

III.1. Possible advantages of blockchain system on supply chains

Blockchain is a class of software technology that is composed of other technologies including data storage, distribution and synchronization, cryptography and identity.[19] It enables large and complex communities of trading and contracting partners to fulfill transactions securely in real time, this way it can have a key role to play in the future of management of global supply chains. As national and local governments and state-owned companies are one of the greatest actors on the demand-side, it is obvious to seek for positive connections between the technology and the user.

Table 2.



Source: DeConvy, 2017[20]

As an overall expectation, experts predict, that in the following years the role of blochchain technology will exponentially growing in areas like banking, medical records, elections, government services like pension disbursement or benefit disbursement, land ownership and tax payments[21]. All these areas are governed by the states, as an actor of the demand side, so the question arise: why not applying blockchain technology for public spending?

III.2. Blockchains's possible role in public procurement regulation

While blockchain technology is not typically used as a specific anticorruption tool, yet, its attributes can make it's applications more resilient to corruption because of the following specifications collected by Transparency International[22]:

1. Transparency: blockchain-based data systems record all changes to stored data. Everyone with access to a blockchain can verify the data stored in this context. Transactions can thus be made more transparent.

[19] The definition of blockchain and/or distributed ledger technology (DLT) is problematic for legal professions. See in details: Glavanits, Judit – Király Péter Bálint (2018)
[20] DeConvy, Sherree (2017) p. 6.
[21] Bashir, Imran (2018) p. 612.
[22] Kossow, Niklas – Victoria Dykes (2018) p. 9.

2. Immutability: once data is stored on the blockchain, it cannot be altered. It is thus safe from manipulation and illegitimate changes.

3. Security: as data is stored on distributed ledgers, it is secured against fraud and against attacks on a single server.

4. Inclusiveness: public blockchains are open source and accessible to everyone. DLT systems can thus be opened to all citizens, democratizing data storage.

5. Disintermediation: distributed ledger technology-based systems cut out a third party needed to verify transactions. This reduces transactions costs and makes them potentially less vulnerable to corruption.

There are self-understanding areas in which public procurement and blockchain can successfully straighten cooperate: public procurement financials and smart contracts.[23] However, the European Parliament has recently published a study, which is analyzing the possible connections between cryptocurrencies and financial crime, money laundering and tax evasion.[24] As long as these financial instruments (cryptocurrencies) will not get a legal definition and without being categorized, their official application in governmental actions within the EU Member states is questionable. Transferring "traditional" money through blockchains might be legally problematic because of the regulation on money markets which are based on the traditional banking industry actors, which blockchain system is by definition want to exclude from the transactions. Smart contracting might be easier to incorporate to the existing e-procurement platforms, while the missing piece here is the programming and developing of the IT-systems. With the possibility of automatized execution of the contracts the fulfillment of contractual obligation and possible fraud or misconduct could be transparently seen for the public. Even there could be less dispute on the remedies. However, the European Commission released a Commission notice called "Guidance on Innovation Procurement" in 2018 which is not even mentioning smart contracts or blockchain technology at all[25] – after 10 years of Bitcoin has born.

There are possible negative aspects of the technology as well of course, which sould be taken into consideration when applying a new technology in public spending. In the short history of the blockchain world, we have faced some breaches on the security. One of the most known is the "The DAO hack", where on June 17, 2016, a hacker found a loophole in the coding that allowed him to drain funds from "The DAO" (running on one of the most trusted blockchain, the Ethereum). In the first few hours of the attack, 3.6 million ETH were stolen, the equivalent of $70 million at the time. Once the hacker had done the damage he intended, he withdrew the attack.

In the last decade the users and examiners of this new technology agree on that one potentially destructive feature of blockchain is that it's possible for bad actors to control a network by sheer virtue of computing power. If more than half of the processing power on a blockchain fell into the hands of a single malicious entity[26] — which could be one person controlling a number of nodes, or a group of hackers working together, or even possible for a foreign country-driven group — it could prove very destructive for the other, well-intentioned members of the network.

[23] See also: Nicoletti, Bernardo (2018) pp. 189-230.
[24] Houben, Robby – Alexander Snyers (2018)
[25] European Commission (2018)
[26] See some technical details here: Liehuang Zhu - Yulu Wu - Keke Gai - Kim-Kwang - Raymond Choo (2019) pp. 527-535.

There are some privacy issues of the technology that still remain unregulated or unsolved so far.[27]

Overall, it is only a matter of time for public entities to start thinking about a better and more transparent purchasing system, possibly based on blockchain or distributed ledger technology. Not only could is save taxpayer's money and build more trust in public spending, but the amount spent on the innovation and development of this technology may positively affect the whole financial and retail industry.

[27] See more here: Axon, Louise - Michael Goldsmith - Sadie Creese (2018) pp. 229-278.

REFERENCES

Axon, Louise - Michael Goldsmith - Sadie Creese (2018): Privacy Requirements in Cybersecurity Applications of Blockchain, In: Pethuru Raj - Ganesh Chandra Deka (eds) Advances in Computers, Elsevier, Volume 111, pp. 229-278.

Bashir, Imran (2018): Mastering Blockchain. Second Edition, Packt Publishing, Birmingham – Mumbai.

Brammer, Stephen – Helen Walker (2011): Sustainable procurement in the public sector: an international comparative study. International Journal of Operations & Production Management Vol. 31 No. 4.

Crown Commercial Service (2016): The Public Contracts Regulations 2015 & The Utilities Contracts Regulations 2016 - Guidance on changes to procedures (Competitive procedure with negotiation, competitive dialogue & innovation partnerships) Overview, Key Points and Frequently Asked Questions. Available:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/560264/Guidance_on_Changes_to_Procedures_-_Oct_16.pdf

Davila, Antonio – Mahendra Gupta – Richard Palmer (2003): Moving Procurement Systems to the Internet: The Adoption and Use of E-Procurement Technology Models. European Management Journal, 2003/1. pp. 11-23.

Dorn, Nicholas - Michael Levi - Simone White (2008): Do European procurement rules generate or prevent crime? Journal of Financial Crime, Vol. 15 Issue: 3, pp. 243-260.

European Commission (2008): Public procurement for a better environment, COM(2008) 400 final

European Commission (2012): GPP Green Public Procurement. A collection of the best practices.

European Commission (2016): Buying green! A handbook on green public procurement, 3rd Edition. Luxembourg.

European Commission (2017): Increasing the impact of public investment through efficient and professional procurement. Press release, published on: 03/10/2017. Available: http://ec.europa.eu/growth/content/increasing-impact-public-investment-through-efficient-and-professional-procurement-0_en

European Commission (2018): Commission notice – Guidance on Innovation Procurement. Brussels, 15.5.2018, C(2018) 3051 final.

Glavanits, Judit – Király Péter Bálint (2018): A blockchain-technológia alkalmazásának jogi előkérdései: a fogalmi keretek pontosításának szükségessége. Jog-Állam-Politika, 2018/3. szám.

Houben, Robby – Alexander Snyers (2018): Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion. European Parliament, Directorate-General for Internal Policies, July 2018.

Kossow, Niklas – Victoria Dykes (2018): Blockchain, bitcoin and corruption. A review of the linkages. Transparency International Anti-Corruption Helpdesk Answer. Transparency International, 22 January, 2018.

Nicoletti, Bernardo (2018): The Future: Procurement 4.0. In: Agile Procurement. Palgrave Macmillan, Cham. pp. 189-230.

OECD (2012a): Progress Made in Implementing the OECD Recommendation on Enhancing Integrity in Public Procurement. OECD, Paris.

OECD (2012b): Public Procurement for Sustainable and Inclusive Gorwth. Available: https://www.oecd.org/gov/ethics/Public-Procurement-for%20Sustainable-and-Inclusive-Growth_Brochure.pdf

OECD (2015): Going Green: Best Practices For Sustainable Procurement. OECD, Paris

OECD (2015): Recommendation of the Council on Public Procurement, Available: https://www.oecd.org/.../OECD-Recommendation-on-Public-Procurement.pdf

OECD (2017): Government at a Glance 2017, OECD, Paris.

Parikka-Alhola, Katriina - Ari Nissinen (2012): Environmental Impacts And The Most Economically Advantageous Tender In Public Procurement. Journal of Public Procurement, Volume 12, Issue 1, pp. 43-80.

Semple, Abby (2012): Reform of the EU Procurement Directives and WTO GPA: Forward Steps for Sustainability? Available at SSRN: https://ssrn.com/abstract=2089357

SIGMA (2016): E-procurement. Brief 17, September 2016. Available: http://www.sigmaweb.org/publications/Public-Procurement-Policy-Brief-17-200117.pdf

Tilt, Carol. A. (2007). "Corporate Responsibility Accounting and Accountants". Idowu, Samuel O. - Leal Filho, Walter (Eds.), Professionals' Perspectives of Corporate Social Responsibiliry, Springer-Verlag Berlin Heidelberg 2009. pp. 11-32.

Toktaş-Palut, Peral et al (2014): The impact of barriers and benefits of e-procurement on its adoption decision: An empirical analysis. International Journal of Production Economics, Vol. 158. pp. 77-90.

Vonortas, Nicholas S – Pushmeet Bhatia – Deborah P. Mayer (2011): Public Procurement and Innovation in the United States. Final report. Center for International Science and Technology Policy, The George Washington University. p. 3.

Zhu, Liehuang - Yulu Wu - Keke Gai - Kim-Kwang - Raymond Choo (2019): Controllable and trustworthy blockchain-based cloud data management. Future Generation Computer Systems, Volume 91, pp. 527-535.

MULTIDISCIPLINARY APPROACH OF THE CONCEPT AND CHARACTERISTICS OF THE CYBERSPACE

ROLAND KELEMEN[1], RICHÁRD NÉMETH[2]

Abstract

One of the most significant challenges of the 21st century is to define cyberspace and its processes, and to provide responses to them. Determining definitions and basic characteristics is also indispensable as all segments of this area have multidisciplinary nature, so it is indispensable to formulate them for a common understanding of each discipline. In this light, this study seeks to define – at least in a schematic way – the concept and basic characteristics of cyberspace from a multidisciplinary approach.

Keywords*: cyberspace, IT, cyber geography, cyberspace sociology, cyber defense*

In the second half of the 20th century, humanity went through an explosive technical and technological development as never before. As a result, such technological innovations have emerged for the last third of the century which have now become indispensable parts of everyday functioning of people, the whole society and even the state.

Among them, the IT (information technology) sector must be highlighted, which has effectively enabled global contacts and communication between people and organizations across different parts of the Earth by various tools, programs and networks; it also facilitates and simplifies everyday tasks both in the private and the public sector.

Because of the all-embracing nature of cyberspace, it has emerged not only solely on the horizon of information science thinking, but processes of this space are also investigated in other disciplines (such as social sciences, military science, natural sciences etc.).

However, due to the complex and multidisciplinary nature of cyberspace, it is necessary to pursue common scientific discourses and thus to develop a basic attribute or basic concept that can be used to raise the activities of these individual sciences to the same level.

The purpose of this study is to provide – at least on a sketchy way – a characterization of cyberspace crossing over scientific fields that can help the future thinking of those who will work in this area.

[1] Dr. Roland KELEMEN, assistant lecturer of Széchenyi István University, Faculty of Law and Political Sciences; assistant research fellow of National University of Public Service, Faculty of Military Sciences and Officer Training. E-mail: kelemen.roland@sze.hu.

[2] Richárd NÉMETH, computer system programmer, IT hosting services, T-Systems Data Center Győr; student at Széchenyi István University, Faculty of Mechanical Engineering, Informatics and Electrical Engineering. E-mail: nemeth.richie@gmail.com

The author's research has been supported by the EFOP-3.6.1-16-2016-00017; Internationalization, initiatives to establish a new source of researchers and graduates, and development of knowledge and technological transfer as instruments of intelligent specializations at Széchenyi University project.

I. Possible IT Approaches of the Concept of the Cyberspace

The concept of cyberspace is highly complex from the point of view of information technology, which is connected to the Internet, to the online (bounded to the Internet in its functioning, and being realized through it) culture in the conventional sense. In everyday life we can say that if a webpage is uploaded to the Internet, then "it is in cyberspace", but it is actually more than that; more specifically, cyberspace means the physical and virtual reality provided by distributed or closely connected[3] computer systems connected by a network based primarily on TCP/IP protocol, however, depending on the context, it defines the place of machine to machine and human to machine connection established by these networks, as well as the data and information exchange (communication) between the participants.

The term itself came from science-fiction literature into everyday life and practical use and used in cases where computer environments are linked by network connection and thus it become a connected space of digital communication, networking, internet and data storage. Its parent is the discipline called cybernetics, derived from the ancient Greek word κυβερνητική (governance). The creator of the term, Norbert Weiner, meant this as the processing, visualization and transmission of information as well as the underlying regulatory and controlling disciplines.[4] In a scientific approach, cybernetics is aimed to explore and describe interactions between the system and the system environment, the behavior of the system created from separate set of elements and its correlation with the environment (mainly its communication with it).

The co-concept of the cyberspace is the cyber environment; in fact, in the conventional approach these two terms give the interpretation together. Space "is a reference system for describing the relative location and direction of things and events. In this sense, things and events are not part of space, but they exist or happen in space." In contrast, "environment means everything (things, circumstances, effects) that is outside of a particular thing, but has an effect on its existence and functioning."[5]

So, according to Munk's view, the infrastructure entitled to connect these computer systems (and thus the users) constitutes the so-called external cyberspace – knowing this has a significant importance in the approach of the cyberspace. Such IT environments form a system that has potentials far beyond the spectrum of services of a "single-user environment." Each element of the network is connected by transmission platforms and channels. These communication channels can be defined by several attributes; the type of the transmission medium, the possible directions of connections (simplex, half-duplex, duplex) or even by the theoretical maximum capacity of the channel.[6] Through these agents, the system goes beyond the set of separate computers of individual users and forms a relevant part of cyberspace creation.

The internal space is the space of the actors as well as the events and actions they trigger. The key of information exchange between actors is interactivity, which definitely refers to a two-sided (but not necessary two-directional) activity. This may include, but are not limited to sending,

[3] The distributed system is not the same as a simple computer network. Their common feature is that they are made up of separate computers, but the relationship between them is different. Each computer in a computer network can be clearly identified, while in a distributed system the user is unaware of this fact and sees the system as a whole unit. For more details, see: Tanenbaum, van Steen (2002).
[4] Wiener (1961) pp. 2-52. o.
[5] Munk (2018) p. 116.
[6] Terplan; Morreale (2000) pp. 3-32.

receiving, exchanging data, collaborating to achieve a common goal, sharing resources (and knowledge), working or even having fun together.

If we look at the location of a human being in cyberspace, efficiency is also an important factor, since we have to be aware that – as in almost every area of life – there is no 100% utilization in information technology. In a computer system the utilization of microprocessors executing instructions never reaches the theoretical maximum value – even in the case of parallel processing and multi-threading processes. The delay in communication is caused by the different interfaces and the operations handling conversion between different operating systems and file system layers. The above findings mainly affect the speed of contact, data access and data exchange in cyberspace.

In relation to the discussed topic, another commonly occurring concept is cognition as the theoretical background of correlation established in cyberspace; the connection between the actors of cyberspace is made possible by machines, so in this respect it is a matter of cognitive human-machine interactions. Cognitive informatics (CI) is such a new transdisciplinary research trend crossing over scientific fields which examines the inner information processing mechanisms and processes using engineering applications building on the fields of computer science, information science, cognitive sciences and human and artificial intelligence.[7] The cognitive infocommunication (CogInfoCom) examines the connection between the research areas of infocommunication and cognitive sciences, as well as the various engineering applications emerged by the synergistic combination of these sciences.[8] The cognitive infocommunication researches investigate the person and its knowledge along with the computing environment and information processing devices complemented with corresponding relations, thus visioning cybernetics as a tool of communication between the various actors; and cyberspace as the place of this.

There is no doubt that the creation of cyberspace is one of the greatest achievements of information science and at the same time one of the cornerstones of its further developments. With the Internet – which, contrary to popular belief, includes not only the World Wide Web, but also a number of other services based on network protocol (e.g. remote connection, peer-to-peer networks and file sharing, VoIP, broadcasting, cloud storages etc.) – connecting billions of users, we have created an almost inexhaustible catalog of data available to anyone; and we have created an opportunity for common work, entertainment, data exchange or video streaming without the limitation of distance. People also can keep in touch via messaging systems or social networks.

By the growth of technological development and available performance, the development of the area of different visual presentations is becoming increasingly important, which expands the information technological approach of cyberspace with further dimensions. Very interesting segments of the overall picture are the applications based on the so-called virtual reality (VR) designed to extend sensations. In these systems with the use of different display types, sound systems and sensors such a sight and sonority can be produced which are able to offer an experience to users as reality would be built up from those things they can actually see and hear.[9]

Today, the so-called 'Internet of Things' (IoT) is becoming increasingly widespread, which is a network-based connection of physical machines, home appliances and other electronic devices created by the synchronization of hardware, software, sensors and actors establishing interactivity[10] – basically, IoT uses the possibilities of cyberspace to connect the newer smart devices. The

[7] Wang; Baciu; Yao; Kinsner (2010) pp. 1-29.
[8] Baranyi; Csapó (2012) pp. 67-83.
[9] Kiss; Hámornik; Köles; Baranyi; Galambos; Persa (2015) pp. 215–216.
[10] Hsu; Lin (2016) pp. 516–527.

concept of smart homes is becoming more and more commonplace, where consumer electronic devices, small and home appliances, security systems, heating and other devices become a single, centrally controlled network, which serves the owners' comfort, monitoring their habits. IoT is the next evolutionary phase of Internet, and considering the World Wide Web's impact on education, communication, business life, science and overall on human relationships, it can be stated that the worldwide spread of the technology places information technology on a completely new basis.[11]

And as we say, it is not only the tip of the iceberg – the attention of IT researches is increasingly focusing on artificial intelligence (AI), opening up new perspectives of information technology, including communication based on human interface devices (HID). The rapid innovation of smart devices mentioned above is a good example of this. In essence, AI is nothing but an artificially created consciousness capable of learning and evaluating information, and therefore making independent decisions without human intervention[12] – and by this, indirectly a new actor, an artificial entity capable of independent decisions joins the system. Despite the fact that AI researches have almost 70 years of history (the British mathematician and code breaker Alan Turing developed the concept of the AI in the 1950s), its results started to appear in our everyday life in the last decade only.

II. Other Dimensions of the Concept and Characteristics of the Cyberspace

Beyond the above-mentioned IT-based conceptual approach to cyberspace, it is necessary to examine the concepts and thinking of cyberspace in other disciplines, due to its extraordinary complexity. On the one hand, it is the only way we can get a comprehensive picture of the system surrounding the society of the 21st century and the processes take place inside it; and on the other hand, we can only give the right legal answers to these phenomena (whether they are positive or negative) in the knowledge of these approaches – or at least if we know the basic IT concepts.

The concept of the cyberspace derives from William Gibson's novel, the Neuromancer from 1984, who defined cyberspace as a certain collective hallucination or impression, a graphic representation of computer generated data.[13] Due to the accelerated development of the IT area, the world of Gibson – which was considered as fiction that time – has become physical reality; "as a result of the interactions in global computer networks, the cyberspace, the cybernetic universe came into being."[14] This cyberspace is an extremely unique and complex phenomenon, as it can be described with physical and geographical concepts, but in addition its virtual features also have extraordinary relevance in its exploration, and as a result of its extraordinary expansion, fundamental areas such as sociology, geopolitics, security policy or warfare also must be reconsidered.

The concepts of geography – especially cyber geography or virtual geography – can make a lot of connections to other areas of science, so it is worth to start the investigation with them.

First of all, it is worth noting that cyberspace itself changes the role of real (geographic) sites, modifies the concept and relationship of location and space, changes distance concepts and narrows the traditional interpretation of location and space perception.[15] However, it is also broadens it in many respects, since cyberspace is not a homogeneous space, it consists of many

[11] Evans (2011) p. 2.
[12] Cohen; Feigenbaum (1986) p. 325.
[13] Gibson (1984) p. 5.
[14] Nagy (1999) p. 173.
[15] Batty (1997) pp. 337-352.

fast growing cyber areas, each of them can make a different kind of interaction, but due to the rapid convergence of technologies, new hybrid spaces are created.[16]

Rezső Mészáros describes the cyberspace as a new geographic space "consisting of many artificially constructed spaces – these are the creations of their designers and often their users, and only assume the characteristics of the >>geographic<< (Euclidean) space when they are explicitly programmed for it. What is more, these spaces are often purely visual objects that have no weight, no mass, and even it is not sure whether they are motionless or not (spaces appear or disappear at a glance). Cyberspace has immaterial and dynamic spatial and structural forms (constructions), it is not tangible in the physical (real) sense of the word, because we can only examine it with the help of our brain, but metaphorically, it is also related to physical experiences (perception)."[17]

According to Ákos Jakobi, cyberspace is nothing more than "the unique, abstract space of the new, computerized world."[18] However, he also states immediately that it is not enough to define the term without further standardization and additional explanation. In his examination he introduces more space concepts, including conceptual and infrastructural space perception, as well as the concepts of external and internal space. From the point of view of our investigation, the latter is relevant, because on the one hand, it shows well that some areas of science cannot ignore the basic concepts of others – so the IT-conceptual separation of cyberspace has to appear in other areas – and on the other hand, these concepts give the most sense of the problems hiding in interactions of cyberspace processes.

In fact, while we can only name as external cyberspace "such spaces where the localization and the momentum of connection to terrestrial (geographic) space are predictably present..."[19], hence we name as the external space of the cyberworld the terrestrial space configuration of infrastructural accessories which can be connected to the system."[20] The term internal cyberspace "can be used when the cyberspace itself shows space characteristics, inequality and orderliness."[21]

It shall follow – and in some cases it actually does – that the classical legal, security and security policy concepts may be applicable in the scope of the resources, structures and network elements that appear in the localizable external space, since in these cases the question of the state's main power or the exercise of ownership rights can be unambiguous.

The concept of internal space can, however, relativises this. It comes from the fact that the internal cyberspace has self-created space characteristics which nullifies the traditional space concept also embodied by the concept of the external cyberspace – namely for example that the appearance of a data set on a localizable server or network does not necessary mean either the basis of legal responsibility or the actual extensibility of state main power.

However, this is based on the fact that the internal cyberspace is a localizable space with no place,[22] so the localizable segments of external cyber space cannot be clearly identified with the internal space segments.

For this reason it must be seen that the traditional conceptual thinking itself can deceive either the legislation or the establishment of security measures' mechanism. Besides, it is also evident that in many cases different mechanisms and rules are needed for external and internal

[16] Dodge; Kitchin (2001) pp. 1-33.
[17] Mészáros (2006) p. 494.
[18] Jakobi (2002) p. 1484.
[19] Jakobi (2002) p. 1487.
[20] Jakobi (2002) p. 1487.
[21] Jakobi (2002) p. 1487.
[22] Jakobi (2002) p. 1488.

space, but the real difficulty of this task is to maintain the consistency between the thinking of the two areas. However, it is also clear that the real characteristic processes – although in most cases they have external space results – are in the internal space.

Cyberspace and its processes "radically change social, cultural, political, institutional and economic life."[23] This statement is absolutely right in that today's modern state apparatus, military, social network, economic life and people in their daily lives are "managing" essential vital functions through the cyberspace, changing their country-old dynamics.

In these processes "…truly revolutionary changes began when economic, financial, social and political processes are based on cyberspace… A social economy (also called shared economy) is emerging, which is extended to cross-border infocommunication networks. Shared economy may also affect subsystems that have proved to be permanent so far, such as national monetary emission or international financial intermediary system."[24] This transformation has brought about the globalization in the financial, economic and cultural relationships.

However, it cannot be forgotten that it has a significant impact on the individual as "cyberspace can influence self-consciousness and community. Cyberspace modifies self-consciousness by providing a new opportunity to extend the limits of the body" and "cyberspace can be accessed from anywhere in the world if you have the right technical equipment and the required money is available."[25] Spanish sociologist Manuel Castells claims point-blank that belonging to the network is a measure of existence,[26] however, he has also formulated the idea of network-embedded individualism, according to which the virtual community is a self-centered or personalized community.[27]

This duality, the need for a network and individualism causes an obvious tension. This tension appears as a broader spectrum problem – as Arturo Escobar drew attention to it – in that not only cyberspace has an impact on the traditional space, but it also has a counter impact on cyberspace, because technology is basically a social construction that does not allow the processes of the traditional space to be separated from the processes of cyberspace; they are closely intertwined.[28]

Thus, the social tensions of the traditional space – whether they are political, religious, ideological or criminological – also appear in this global internal cyberspace. However, these tensions in these personalized global communities – where the prejudice, the interest, the worldview of the individual can formulate the standards and self-consciousness of the other members of the network in an exaggerated number and degree – appear with increased intensity.

The increasing social tension is also manifested by social movements, and they set their own tools; globalizing technology and culture in opposition with the networking world. Therefore, exploiting the opportunities offered by cyberspace, some terrorist organizations reinforce their transnational character and emerge a new hybrid security problem and challenge.[29]

This security problem is compounded by the fact that certain economic and financial factors, as well as the institutions of nation-state and supranational communities are connected to the global

[23] Dodge; Kitchin (2001) p. 13.
[24] Pintér (2016) p. 330.
[25] Mészáros (2006) pp. 494-495.
[26] Pintér (2007) p. 25.
[27] Bell (2007) p. 67.
[28] Escobar p. 211-231.
[29] See also: Magyar; Simon (2017) pp. 57-68.; Simon; Magyar (2017) pp. 89-101.; Simon (2015) pp. 145-162.; Tóth (2016) pp. 26-42.

cyberspace. Thus, the actors listed above who are connected to cyberspace may also become a direct target of interstate conflicts and conflicts come from social tension.

"The physical living space (the hardware) of the information society is a network of state and non-state bodies and citizens who are directly – nowadays usually electronically – connected to them… the new society's >>nervous system<< is the IT and the telecommunications infrastructure, while its immune system is the IT security and the data protection. The control and management of the processes of the society (the software) can be strategies that are capable of defending values according to the interests of the community, and capable of guaranteeing the maintenance of living space and the safe operation of the various segments of society."[30]

Taking these circumstances into account, for the protection and safety of the cyberspace – and therefore the traditional space – it is necessary that the armed defense systems of individual states[31], including their military-like bodies[32] – and researchers of this area – create their own cyberspace concepts, thereby helping the organizations to define their role and place in cyberspace processes.

The need for this narrow interpretation of cyberspace is also confirmed by the fact that "anyone can put an end to life with information… because devices connected to Internet and telecommunication networks can lead to the same result as weapons… the instrument, scale and social impact of destruction can be compared more likely to the legally-only judged consequences of wars or industrial and natural disasters." [33] Recognizing this, NATO classified cyberspace as the fourth battlefield.

"In relation to the definition of cyberspace – according to civilian interpretation – it is a commonly occurring view that it is connected to computer networks and the Internet. But the military interpretation of cyberspace extends this dimension, and understands not only the operating environment of computer networks under the term."[34]

In their work, Steve Winterfeld and Jason Andress said that in cyberspace, battlespace includes networks, computers, hardware (this includes weapon systems with embedded computer chips), software (commercial and government developed), applications (like command and control systems), protocols, mobile devices and people that run them.[35]

According to the definition by the US Department of Defense, cyberspace is "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."36 The professional cyber defense concept of the Hungarian Defense Forces also provide a concept; „cyberspace is a dynamically changing domain that can be determined by using electromagnetic spectrum, and it is

[30] Simon (2016a) p. 72.
[31] About the system of armed protection and its contemporary challenges, see: Farkas (2016); Farkas (2017a) pp. 44-58.; Farkas (2017b) pp. 5-20.
[32] For more information about the concept of military-character organs, see: Farkas (2012) pp. 3-6.
[33] Simon (2016b) pp. 41-42.
[34] Haig; Kovács; Ványa; Vass (2014) p. 23.
[35] Winterfeld; Andress (2013) p. 22.
[36] Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms, (https://fas.org/irp/doddir/dod/jp1_02.pdf), [Online] Accessed: 05/02/2018, p. 57.

entitled to handle data between interconnected networks, devices and additional physical infrastructures."[37]

III. SUMMARY

Summarizing the concepts and features above, it can be deducted that this cyberspace is an ever-expanding entity, which is easily accessible to everyone but difficult to describe with conventional geographic space concepts. It has a real impact on the self-image of the individual and the society, on social reflections and on the global economy, and in which the administrative and military-like organizations of the states appear as active players.

The meaning of cyberspace is continuously expanding with new shades from an IT point of view and it is unnecessary to make predictions about future innovations in this area – it is certain that the current trend will continue and even increase, and in line with the evolution of information technology, we will spend more and more parts of our life, entertainment and work in the cyberspace.

Through this cyberspace, millions of informational floods pass through in a single minute. "It is clearly predictable that cyberspace systems are getting bigger, faster and more complex,"[38] but their vulnerability lies exactly in this complexity. The risk of this vulnerability lies in the fact that nowadays not only private individuals and economic participants but the basic structures of the state, the social network and its armed forces are also part of the cyberspace. For this reason, the state can be attacked in cyberspace in the same way as in everyday reality. Thus, Géza Herczegh's idea is still valid today, in which he recorded that "In these circumstances, it is not only right but also necessary to review the most important rules governing the peaceful contacts and cooperation of states – not in order to change them and replace them with others, but to expand and clarify their meaning and significance from a new perspective in the rapidly changing circumstances of the world."[39]

[37] No. 60/2013. Decree of the Minister of Defense of 30th September on the publication of the Cyber Defense Concept of the Hungarian Armed Forces, Appendix 1, Paragraph 2 (8).
[38] Babos (2011) p. 42.
[39] Herczegh (1963) p. 360.

REFERENCES

Babos, Tibor (2011): Globális közös terek a NATO-ban. Nemzet és biztonság, Vol. 3. No. 3., 34–46. pp.

Baranyi, Péter; Csapó, Ádám (2012): Definition and Synergies of Cognitive Infocommunications. Acta Polytechnica Hungarica. Vol. 9. No. 1., 67–83. pp.

Batty, Michael (1997): Virtual Geography. Futures. Vol. 29. No. 4-5. 337–352. pp.

Bell, David (2007): Cyberculture Theorists – Manuel Castells and Donna Haraway. London - New York, Routledge

Cohen, Paul R.; Feigenbaum, Edward A. (1986): The Handbook of Artificial Intelligence England. California, Addison-Wesley.

Dodge, Martin; Kitchin, Rob (2001): Mapping Cyberspace. London - New York, Routledge.

Escobar, Arturo (1994): Welcome to Cyberia – Notes on the Anthropology of Cyberculture. Current Anthropology, Vol. 35. No. 3.June, 211–231. pp.

Evans, Dave (2011): The Interent of Things: How the Next Evolution of the Internet is Changing Everything. Cisco, White Paper.

Farkas, Ádám (2012): A katonai büntetőjog és igazságszolgáltatás helye, szerepe, létjogosultsága az állam és társadalom rendszereiben. Hadtudomány: A Magyar Hadtudományi Társaság Folyóirata. Online issue, 3–-6. pp.

Farkas, Ádám (2016): Tévelygések fogásában?: Tanulmányok az állam fegyveres védelmének egyes jogtani és államtani kérdéseiről, különös tekintettel Magyarország katonai védelmére. Budapest, Magyar Katonai Jogi és Hadijogi Társaság.

Farkas, Ádám (2017a): Adalékok az állam fegyveres védelmének rendszertani megközelítéséhez. Honvédségi Szemle, Vol. 145. No. 1., 44-58. pp.

Farkas, Ádám (2017b): A terrorizmus elleni harc, mint kiemelt ágazatközi fegyveres védelmi feladat. Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat tudományos-szakmai folyóirata, Vol. 15. No. 3. November, 5–20. pp.

Gibson, William (1984): Neuromancer. New York, ACE Publishing Group.

Haig, Zsolt; Kovács, László; Ványa, László; Vass, Sándor (2014): Elektronikus hadviselés. Budapest, Nemzeti Közszolgálati és Tankönyv Kiadó Zrt.

Herczegh, Géza (1963): Az erőszakkal való fenyegetésnek és az erőszak alkalmazásának tilalma a mai nemzetközi jogban. Állam és Jogtudomány. Vol. 6. No. 3., 360–380. pp.

Hsu, Chin-Lung; Lin, Judy Chuan-Chuan (2016): An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives. Computers in Human Behavior. Vol. 62. No. C., 516–527. pp.

Jakobi, Ákos (2002): A virtuális világ terei. Magyar Tudomány. Vol. 108. No. 11., 1482-1491. pp.

Kiss Laura; Hámornik, Balázs Péter; Köles, Máté; Baranyi, Péter; Galambos, Péter; Persa, György (2015): Training of Business Skills in Virtual Reality. 2015/6. IEEE International Conference on Cognitive Informatics & Cognitive Computing. Győr. 215–216. pp.

Magyar, Sándor; Simon, László (2017): A terrorizmus és indirekt hadviselés az EU kibertérben. Szakmai Szemle – A Katonai Nemzetbiztonsági Szolgálat tudományos-szakmai folyóirata. Vol. 15. No. 4., 57-68. pp.

Mészáros, Rezső (2006): A kibertér, mint új földrajzi tér. In: Kiss, Andrea; Mezősi, Gábor; Sümeghy, Zoltán (eds.): Táj, környezet és társadalom – Ünnepi tanulmányok Keveiné Bárány Ilona professzor asszony tiszteletére. Szeged, Department of Climatology and Landscape Ecology.

Munk, Sándor (2018): A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. Hadtudomány, Vol. 28. No. 1, 113–131. pp.

Nagy, Károly (1999): Titok és biztonság az információs társadalomban. Belügyi Szemle. Vol. 47. No. 4-5., 173. 172–183. pp.

Pintér, István (2016): A virtuális tér geopolitikája. In: Pintér István (ed.): A virtuális tér geopolitikája – Geopolitikai Tanács Műhelytanulmányok. Budapest, Geopolitikai Tanács Közhasznú Alapítvány.

Pintér, Róbert (2007): Úton az információs társadalom megismerése felé. In: Pintér, Róbert: Az információs társadalom – Az elmélettől a politikai gyakorlatig. Budapest, Gondolat - Új Mandátum.

Simon, László (2015): A fokozódó terrorizmus Európában és annak hatása a katonai tömegrendezvények biztosítására. Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat tudományos-szakmai folyóirata. Vol. 13. No. 2, 145-162. pp.

Simon, László (2016a): A titok speciális értelmezése az elmúlt 25 év kihívásainak, kockázatainak és fenyegetéseinek tükrében. Felderítő Szemle. Vol. 15. No. 1, 67–87. pp.

Simon, László (2016b): Az információ mint fegyver?. Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat tudományos-szakmai folyóirata. Vol. 14. No. 1, 34–60. pp.

Simon, László; Magyar, Sándor (2017): A terrorizmus és indirekt hatása a kibertérben. Nemzetbiztonsági Szemle. Vol. 5. No. 3., 89-101. pp.

Tanenbaum, Andrew; van Steen, Maarten (2002): Distributed Systems: Principles and Paradigms. New Jersey, Prentice Hall.

Terplan, Kornel; Morreale, Patricia (2000): The Telecommunications Handbook. USA, CRC Press.

Tóth, Zoltán Balázs (2016): Az Iszlám Állam online térhódítása. Nemzetbiztonsági Szemle. Vol. 4. No. 4., 26–42. pp.

Wang, Yingxu; Baciu, George; Yao, Yiyu; Kinsner, Witold (2010): Perspectives on Cognitive Informatics and Cognitive Computing. International Journal of Cognitive Informatics and Cognitive Computing, Vol. 4. No. 1. January, 1–29. pp.

Wiener, Norbert (1961): Cybernetics or Control and Communication in the Animal and the Machine. Paris, Hermann & Cie & Camb, 2nd Ed.

Winterfeld, Steve; Andress, Jason (2013): The Basics of Cyber Warfare Understanding the Fundamentals of Cyber Warfare in Theory and Practice. Waltham, Elsevier.

GAMBLING IN VIDEO GAMES

PÉTER BÁLINT KIRÁLY[1]

Abstract

Over the past two or three decades, video games have gained more and more importance. However, the world of video games has been shocked last year by the controversy sorrounding the so-called lootboxes. In my study, I would like to present the legal problems raised by them. Frist I present the most important definitionts, then discuss the problems with lootboxes, and the gambling authorities reactions to the matter. Finally I will propose some possible solutions to the lootbox problem.

Keywords: *Video games; gambling; lootboxes*

I. Intoduction

Over the past two or three decades, video games have gained more and more importance. This is proven by the fact that nowadays they can sell more than 10 million copies of a single video game,[2] video game companies hire professional scriptwriters, and composers for their games.[3] In addition they regularly organize video game competitions (so-called esports) with millions of dollars in total prize money[4] and millions of spectators.[5] Esports will be medal sport at 2022 Asian Games, and could be medal event at 2024 Olympics.[6] There is even an award for the best video games each year (similar to the Oscars Academy Award for movies), where the best games of the year are awarded in categories like Best Game Direction, Best Narrative, and Best Score/Music, etc.[7]

However, the world of video games has been shocked last year by the controversy sorrounding the so-called lootboxes. In my study, I would like to present the legal problems raised by them.

II. Definitions

In order to be able to present the problems raised by the lootboxes, I find it necessary to clarify certain definitions.

The first one of these is the online gambling service that means any service which involves wagering a stake with monetary value in games of chance, including those with an element of skill. For example lotteries and betting transactions.[8]

The second definition is skins and other cosmetic items. „Skins are items that generally can be used within a game, usually for cosmetic purposes (e.g., changing the color of a gun in Counter-

[1] Dr. Péter Bálint KIRÁLY, PhD student, Széchenyi István University, Széchenyi István Egyetem
Deák Ferenc Faculty of Law and Political Sciences, Department of Public Administrative and Fiscal Law
[2] https://steamspy.com/
[3] http://www.scriptmag.com/features/video-games-screenwriting-can-video-game-design-teach-us-screenwriting
[4] https://esport1.hu/news/2017/12/28/esport-abbiechan-top10-legmagasabb-osszdijazasu-jatek
[5] http://esports-marketing-blog.com/esports-viewership-numbers/
[6] https://www.theguardian.com/sport/2017/aug/09/esports-2024-olympics-medal-event-paris-bid-committee
[7] http://thegameawards.com/awards/
[8] 2014/478/EU: Commission Recommendation

Strike) and can range in value from a few cents to thousands of dollars." Skins can be acquired through gameplay, and/or lootboxes, and/ or microtransactions depending on the game. Important to note, that cosmetic items don't influance the gameplay, and don't provide advantage to those who own a specific cosmetic item, over those players who don't. Game developers usually don't allow skins to be exchanged for cash (only game credit), but secondary markets do allow players to convert skins to cash.[9]

The third term is power ups. In video games, power-ups are items that instantly add to the life, armor, strength or score of a player, they benefit or add extra abilities to the game character as a game mechanic.[10] (For example a new weapon, armor with better stats or power boost). You can aquire power ups the same way as skins. Contrary to cosmetic items, power ups provide advantage to players who use them, over those who don't have them.

The fourth one is in-game currency, which is a currency used in a video game. You can get in game-currency by playing a game (through leveling up your character or defeating an enemy) or by buying in game-currency with real money.[11]

The next one is microtransactions, which are a very small financial transactions conducted online (in our case in an online video game).[12] Its a business model where users can purchase virtual goods via micropayments, using real money. For instance you pay a few cents to get a new skin for your in game character, or to get a new and more powerful weapon or armor. The introduction of microtransactions were an important milestone in the history of videogames, as they allowed the appearance of free-to-play games, because video game publishers have found that „by making their game mostly available for free, gamers would flock to the popular title in such numbers that even if only a small fraction of those players ended up spending, they would generate a profit."[13] We can safely say that games would cost much more without microtransactions.[14]

The next definition is the pay-to-win games. A game is considered pay-to-win, if it lets you buy power ups with real money or allow you to improve your character faster then everyone else. This makes the game largely unbalanced, because players who purchase these gain a significant advantage over those people,[15] who have skill in the game, but opted to just play the game without paying.[16]

The last definition on the list is lootboxes. „In video games, a lootbox is a consumable virtual item which can be redeemed to receive a randomised selection of further virtual items, ranging from simple cosmetic items (like skins), to game-changing equipment such as weapons and armor."[17] You can receive lootbox by playing the game, and/or by buying them with in-game currency and/or through microtransactions. The items you get from have different rarities, and are randomised, so your chance to get something rare is minimal, and it's likely you'll be encouraged to dip in again and again. So if you want a specific skin, or you need a specific power up you are encouraged to buy lootboxes (mainly if its the only way to obtain those items).

[9] https://www.linkedin.com/pulse/how-esports-gambling-grows-30bn-wagers-2020-chris-grove?trk=prof-post
[10] https://www.techopedia.com/definition/2266/power-up-gaming
[11] http://r-stylelab.weebly.com/blog/in-game-currency-as-means-to-build-smart-mobile-game-economy
[12] https://en.oxforddictionaries.com/definition/microtransaction
[13] https://www.icy-veins.com/forums/topic/35193-on-loot-boxes-and-morality/
[14] https://whatis.techtarget.com/definition/loot-box
[15] https://www.youtube.com/watch?v=YMDGPSWWA18
[16] https://www.urbandictionary.com/define.php?term=pay-to-win
[17] https://en.wikipedia.org/wiki/Loot_box

III. What is the problem with lootboxes?

The lootbox system in general can cause addiction according to studies. By opening a lootbox our brain releases dopamine cells, that are responsible for pleasure, desire and motivation. It gives you the feeling that you did something good. So getting a reward will make you want more reward, and so on.[18]This addiction to reward is stronger if the reward is uncertain. In case of lootboxes the reward is not predictable: you either get something awesome, or something you consider bad. „This randomness taps into some of the very fundamental ways our brains work when trying to predict whether or not a good thing will happen." [19] Our brain reacts more vigorously to an uncertain reward than the same reward delivered on a predictable basis, and the more uncertain a reward is, the more dopamine cells are active. Psychologists call this effect a variable rate reinforcement.[20] Plus if you can buy lootboxes through a microtransaction system you only spend a small amount of money with each purchase and you don't really realize how much money you actually spent on a game.

Randomized items are not new in video games. Even the name lootbox comes from the game mechanic of loots. Loots (in this case it means different items and in game currency) were dropped after you defeated a boss, or any other enemy during your gameplay. These items had different rarity just like in the case of lootboxes. But even outside videogames you can find random rewards. For example in Kinder eggs, which also have random rewards.

In my opinion the problem with lootboxes is not the randomness of rewards, but the way they got implemented into some videogames (with pay-to-win mechanic, and/or only through microtransactions).

IV. The game that unleashed the lootbox controversy: Star Wars Battlefront II.

Lootboxes and other random gaming mechanisms have long been part of the video game world. From time to time, the gaming community is outraged by the pay-to-win nature of a game, or by microtransactions or by the random rewards dropped from lootboxes, but for years these voices did not reach the people outside of the gamer subculture.

This situation was changed by the videogame called Star Wars Battlefront II,[21] which was released by the publisher EA in November 2017.[22] The game contained 16 playable characters that could be obtained from the points earned during the game.[23] In addition, each hero had different power ups that could be acquired through lootboxes. Lootboxes can be obtained by playing the game and leveling up your characters.

Players calculated that they would require around 40 hours of gameplay to get a single hero.[24] In order to get all the heroes and power ups with the lootboxes, we need to play roughly 4528 hours (188 days) non-stop.[25] In addition to this, EA introduced a microtransaction system that allowed players to directly buy lootboxes. As a result, the players who bought lootboxes with real

[18] https://index.hu/tech/2017/01/01/az_iphone_ugy_hat_mint_a_drog/
[19] https://www.eurogamer.net/articles/2017-10-11-are-loot-boxes-gambling
[20] https://www.pcgamer.com/behind-the-addictive-psychology-and-seductive-art-of-loot-boxes/
[21] https://www.engadget.com/2018/02/24/loot-boxes-gambling-legislation/
[22] https://www.icy-veins.com/forums/topic/35193-on-loot-boxes-and-morality/
[23] https://www.extremetech.com/gaming/258941-take-40-hours-unlock-single-hero-star-wars-battlefront-ii
[24] https://www.extremetech.com/gaming/266264-ea-admits-defeat-unlocks-battlefront-2-heroes-removes-pay-win-mechanics
[25] https://www.extremetech.com/gaming/259163-belgium-investigates-battlefront-ii-eas-reddit-ama-bombs

money have more and stronger power ups than those who decided to acquire those only by playing the game.[26] Since this is a PvP game (which means players play against each other), this system has resulted in a pay-to-win game, as the players who invested real money into the game can easily defeat those who opted not to.

Players therefore had two choices: they play hours and hours to get every hero and power up, so they could fully enjoy the game; or they spent more money through microtransactions on lootboxes to obtain them all in a faster pace. EA went straight to the point that if the player's character died, the game would be displayed in the statistics, about which enemy character killed them, and what power ups they used. Because of this players will want to buy lootboxes, so they can have the same power ups, and the same chance of winning the game.[27]

This alone would not have been a problem at all, since other games are also have microtransactions and pay-to-win systems. These monetization systems are used mostly by free to play games. It is acceptable for a free to play game to have a pay-to-win system, as at least the game is available for free, and players can decide whether they want to spend real money on power ups, or they want to play the game entirely for free. In addition to this „it's one thing to sell skins, emotes, or cosmetic upgrades. For that matter, it's fine to sell weapons, armors, resources, and other assets in single-player games, provided those items and elements of gameplay are reasonably abundant in-game and can be earned in a reasonable amount of time."[28] But Battlefront II. is a multiplayer, PvP game, and the game itself costs $60. Players would have to spend more money on lootboxes in addition to this base cost in order not to be in a disadvantageous situation and they can fully enjoy their purchase.[29] Furthermore Battlefront II. is a Star Wars game, that not only hardcore gamers wanted to try, but also Star Wars fans who are not interested in video games anyway in the first place.

It is no wonder, however, that the system introduced by EA has triggered an outrage that has generated significant debate outside the gamer subculture. So much so that the legislature and law enforcement bodies of several states (such as Belgium, the Netherlands or Hawaii) began to deal with the legal aspects of lootboxes and other random game elements and the possibility of banning them.[30]

V. Authorities' Reactions

Gambling authorities around the world) don't classify lootboxes as gambling because, in their view, the items acquired from them cannot be exchanged for real-life money, meaning they have no real life value. The other arguement was that „though casinos and loot boxes are technically similar, there is one major difference - a casino can leave you empty handed, while you're guaranteed to get something out of lootbox. Maybe just not the thing you wanted."[31]

However the reality tells us otherwise. For example in case of the first-person shooter game, called CS:GO the virtual items you can obtain from lootboxes have real life value to them. In this

[26] https://www.icy-veins.com/forums/topic/35193-on-loot-boxes-and-morality/
[27] https://www.youtube.com/watch?v=W1hQHZedRSE
[28] https://www.extremetech.com/gaming/259163-belgium-investigates-battlefront-ii-eas-reddit-ama-bombs
[29] https://www.gamesindustry.biz/articles/2017-10-18-loot-boxes-combat-rising-development-and-marketing-costs
[30] https://www.extremetech.com/gaming/266264-ea-admits-defeat-unlocks-battlefront-2-heroes-removes-pay-win-mechanics
[31] https://www.eurogamer.net/articles/2017-10-11-are-loot-boxes-gambling

game you can get lootboxes by playing the game,[32] and they will only drop you different skins, so its not a pay-to-win system. In addition the game lets you trade your unwanted skins through the game. You can have an in-game account and you can transfer real-life money to this account, and once you did that you can buy skins with it, but you cannot transfer the money back to your bank account.[33]

This system will also be supplemented with third-party websites, where players can offer their skins for auction, and other players can bid on them. This solution is more popular than in-game skin purchases because the money that you receive this way can be transferred back to your bank account.[34] There are also websites where you can bet on the results of the CS: GO esport events,[35] but compared to real-life betting the difference is that we can bet with skins instead of real money, and if we win, we can get the losers' skins. We can even find websites where game skins can be played on an online roulette game.[36]

There were also several scandals in this regard, because these sites in order to promote themselves, contracted with well-known streamers, to broadcast on the stream-site, called Twitch as they play, for example a skin-roulette game.[37] However, it was later discovered that the owner of the skin roulette site told the streamer in advance what number will win in each round.[38] Since these streamers are mainly viewed by young people, it is particularly dangerous to promote gambling in this form, especially if we influence the outcome of the game to show that we can often win a lot of money, although in reality this is not the case.[39]

Based on the facts just described, we can safely say that the skins you get from a lootbox do have a real life value. You can trade them with real money for a price from a few cents to $10-15.000. (The most expansive skin as of today was sold for $60.000).

As a result, gambling supervisors' statement that lootboxes are not considered to be gambling, because the virtual items acquired from them do not have a real-life value, does not correspond to reality.

VI. Summary

„Internal game economies (where players can earn a virtual currency and exchange it for in-game items) have long been a popular element of a variety of video game genres. Modern video games have taken what was a static environment (players interacting exclusively with the game to earn and spend currency) and made it highly dynamic by allowing players to trade, buy, and sell virtual items among each other. To complete the loop, third-party marketplaces often emerge that allow virtual items to be exchanged for cash. The result? Complex quasi-currencies such as CS:GO skins and FIFA coins that serve purposes -- and have value -- both within the game and outside of the game."[40]

If we add that these quasi-currencies are obtainable from lootboxes – in some cases the lootbox itself can be purchased through a microtransaction – then we can say that the items

[32] https://index.hu/tech/godmode/2016/05/12/csgo_gambling/
[33] https://dotesports.com/counter-strike/news/csgo-gambling-scandal-explained-3545#list-1
[34] https://www.dexerto.com/news/csgo-weapon-sells-staggering-price-record-smashed/43275
[35] https://www.esportsbettingreport.com/valve-skin-betting-cease-desist/
[36] https://www.linkedin.com/pulse/how-esports-gambling-grows-30bn-wagers-2020-chris-grove?trk=prof-post
[37] https://index.hu/tech/godmode/2016/05/12/csgo_gambling/
[38] https://dotesports.com/counter-strike/news/csgo-gambling-scandal-explained-3545#list-2
[39] https://index.hu/tech/godmode/2016/05/12/csgo_gambling/
[40] https://www.linkedin.com/pulse/skin-gambling-crackdown-controversies-likely-shave-billions-grove

obtained from the lootboxes have a real-life value. However, from the lootboxes we definitely get some reward (as opposed to slot machines or roulette), and therefore, according to the decisions of the gambling authorities so far, it does not constitute as gambling. Here I would like to point out that gaming authorities' attitude has changed recently, for example, Belgium classified all types of lootboxes as gambling, despite the aforementioned fact.[41] In addition to this the legislation process is on its way in a lot of countries. For instance in the states of Hawaii[42] and Washington,[43] the Netherlands[44] and Germany[45] also established commissions for the legislation.

In my opinion, lootboxes may be addictive due to the variable rate reinforcement effect, and since the majority of users of video games are underaged, they need to be regulated. In my view, however, it is necessary to differentiate between different types of lootboxes during regulation. Firstly, depending on how one can acquire them, we can distinguish between games where we can only get lootboxes by playing, and where we can get them through microtransactions. Secondly, depending on whether the obtainable items from the lootboxes can only be cosmetic items, or there are power-ups among them.Thirdly, based on whether the items from lootboxes can be sold between players for real money, either inside the game or through third-party websites (including skin-gambling).

In my opinion, we should banned lootboxes in two cases:

1. On the one hand, when lootboxes contain power-ups, and these lootboxes are also purchasable through microtransactions. In this case, the game creates a pay-to-win system, in addition, it's a pay-to-win system in which luck plays a great role.

2. On the other hand, when items from lootboxes can be exchanged and / or sold between players. In this case, items from lootboxes will in all likelihood have a real-life value regardless of whether lootboxes are obtainable only through gameplay or by microtransactions, and regardless of whether they contain power-ups or not.

In my point of view, only the lootboxes of the latter two categories should be banned, because:

1. If the lootboxes are only obtainable through gameplay, and the items are not interchangeable, then it is left to the player whether they are willing to spend more time in the game in hope of getting more lootbox, or not. In this case the items have no real-life value. Therefore, this is not considered gambling. This is also true if lootboxes can contain power-ups, as this will not result in a pay-to-win system.

2. Also, if you can get a lootbox through microtransformation, but they only contain cosmetic items and they can not be exchanged, then the player is not encouraged to buy lootboxes, because they can be as successful in the game without them as those who bought lootboxes. In addition, as I mentioned, these microtransactions allowed the release of free-to-play games, and that start-up or small video game companies can stay on the market. For both video game publishers and the gamer community, it is important to maintain the microtransaction system.

---

41 https://news.unikrn.com/article/overwatch-csgo-dota-fifa-loot-box-ban-belgium?utm_source=reddit&utm_medium=news&utm_campaign=lootboxesbelgium042518&utm_term=esports+industry&utm_content=ds

42 https://www.extremetech.com/gaming/259503-battlefront-ii-loot-crates-declared-gambling-belgium-attacked-hawaii

43 http://www.casinogamespro.com/2018/01/12/washington-legislature-rolls-new-bill-aimed-loot-boxes

44 https://www.extremetech.com/extreme/267994-the-netherlands-declares-some-loot-boxes-illegal-warns-developers-to-modify-them

45 https://www.pcgamer.com/germany-may-ban-loot-boxes/

No matter how the states decide on lootboxes, it would be absolutely necessary to label the video games with a warning about: a) whether they contain lootboxes, b) whether lootboxes contain power-ups or just cosmetic items, c) whether it is a micro-transaction, d) and whether it is a pay-to-win game. This would allow players to decide whether they would be willing to buy the game under these conditions.

All in all, It can be stated that lootboxes must be regulated, and I can only hope that the legislators will take into account the interests of the gamer community and video game producers, so that gamer subculture can develop further within a safer framework.

REFERENCES

2014/478/EU Commission Recommendation

http://esports-marketing-blog.com/esports-viewership-numbers/

http://r-stylelab.weebly.com/blog/in-game-currency-as-means-to-build-smart-mobile-game-economy

http://thegameawards.com/awards/

http://www.casinogamespro.com/2018/01/12/washington-legislature-rolls-new-bill-aimed-loot-boxes

http://www.scriptmag.com/features/video-games-screenwriting-can-video-game-design-teach-us-screenwriting

https://dotesports.com/counter-strike/news/csgo-gambling-scandal-explained-3545#list-1

https://en.oxforddictionaries.com/definition/microtransaction

https://en.wikipedia.org/wiki/Loot_box

https://esport1.hu/news/2017/12/28/esport-abbiechan-top10-legmagasabb-osszdijazasu-jatek

https://index.hu/tech/2017/01/01/az_iphone_ugy_hat_mint_a_drog/

https://index.hu/tech/godmode/2016/05/12/csgo_gambling/

https://news.unikrn.com/article/overwatch-csgo-dota-fifa-loot-box-ban-belgium?utm_source=reddit&utm_medium=news&utm_campaign=lootboxesbelgium042518&utm_term=esports+industry&utm_content=ds

https://steamspy.com/

https://whatis.techtarget.com/definition/loot-box

https://www.dexerto.com/news/csgo-weapon-sells-staggering-price-record-smashed/43275

https://www.engadget.com/2018/02/24/loot-boxes-gambling-legislation/

https://www.esportsbettingreport.com/valve-skin-betting-cease-desist/

https://www.eurogamer.net/articles/2017-10-11-are-loot-boxes-gambling

https://www.extremetech.com/extreme/267994-the-netherlands-declares-some-loot-boxes-illegal-warns-developers-to-modify-them

https://www.extremetech.com/gaming/258941-take-40-hours-unlock-single-hero-star-wars-battlefront-ii

https://www.extremetech.com/gaming/259163-belgium-investigates-battlefront-ii-eas-reddit-ama-bombs

https://www.extremetech.com/gaming/259503-battlefront-ii-loot-crates-declared-gambling-belgium-attacked-hawaii

https://www.extremetech.com/gaming/266264-ea-admits-defeat-unlocks-battlefront-2-heroes-removes-pay-win-mechanics

https://www.gamesindustry.biz/articles/2017-10-18-loot-boxes-combat-rising-development-and-marketing-costs

https://www.icy-veins.com/forums/topic/35193-on-loot-boxes-and-morality/

https://www.linkedin.com/pulse/how-esports-gambling-grows-30bn-wagers-2020-chris-grove?trk=prof-post

https://www.linkedin.com/pulse/skin-gambling-crackdown-controversies-likely-shave-billions-grove

https://www.pcgamer.com/behind-the-addictive-psychology-and-seductive-art-of-loot-boxes/

https://www.pcgamer.com/germany-may-ban-loot-boxes/

https://www.techopedia.com/definition/2266/power-up-gaming

https://www.theguardian.com/sport/2017/aug/09/esports-2024-olympics-medal-event-paris-bid-committee

https://www.urbandictionary.com/define.php?term=pay-to-win

https://www.youtube.com/watch?v=W1hQHZedRSE

https://www.youtube.com/watch?v=YMDGPSWWA18

THE ARRIVAL OF THE DIGITAL ECONOMY: EVIDENCE FROM WORLD INPUT-OUTPUT TABLES[1]

KRISZTIÁN KOPPÁNY[2]

Abstract

This study investigates the most significant changes in global value chains and the industry breakdown of world output and value added assumed to be related to the arrival of the digital age. Using a series of world input-output tables (Word Input-Output Database, WIOD) from 2000 to 2014 allows us to perform a long-term analysis. To calculate multiplier effects, we use the Ghosh supply side model. Preliminary results highlight some very interesting tendencies which are in contradiction with other global statistics, and in some sense even with the title of the paper. Are they only illusory? Do they indicate the arrival of the digital economy after all?

Keywords: *digital economy, global output, global GDP, input-output analysis, world input-output tables (WIOD)*

I. Introduction

This paper analyses the sectoral structure of the global economy. World input-output tables are used to investigate how the changes of industry shares indicates the arrival of the digital economy. The hypotheses are on one hand, the growing share of digital industries, such as manufacturing of computers, smartphones and other electronic devices, related services such as computer programming, infocommunication and infotechnology service, and the supply of electricity. On the other hand, one can expect the declining share of some traditional sectors.

II. World Input-Output Database

To check whether these hypotheses are true or false, the tables of the World Input-Output Database was used. They contain 43 countries (plus the rest of the world, ROW), 56 industries and 5 final demand categories. Data are expressed in current prices and converted into US dollars using exchange rates. The latest release of the database contains table for each year of the period 2000-2014.[3]

This is an enormous amount of data. Each WIOT consists of more than 6 million cells, thus multiyear modelling is very time-consuming and resource-intensive task, not only for the researcher but the computer too. So, to be able to show some preliminary results here, data were condensed by dropping the country level. It's a plausible assumption for a global analysis without countries, country groups, regions, developed and emerging part of the world, but one must consider that every simplification is a limitation too and can cause biases. The level of aggregation affects results of input-output analysis. Using current prices and exchange rate are also the sort of things like this. Although we work with actual shares of a given year and don't make connection between years by

[1] This research was supported by „EFOP-3.6.1-16-2016-00017 Internationalisation, initiatives to establish a new source of researchers and graduates, and development of knowledge and technological transfer as instruments of intelligent specialisations at Széchenyi István University".

[2] Dr. Krisztián KOPPÁNY, PhD, associate professor, deputy dean for corporate relations, Széchenyi István University, Kautz Gyula Faculty of Business and Economics, koppanyk@sze.hu

[3] For an overview of the WIOD and its applications see Timmer et al (2015, 2016).

volume indices, for example, one must keep in mind that the price for the same product or a wage for the same work can vary between the producer countries, thus can have a significant effect on the value of sectoral output and value added.

In spite of this, the values and the trends of global output and value added fit very well to those of by other institutions like the World Bank. This, however, is not true for the sectoral shares.

III. The structure of the world economy on a large scale

According to the data of World Bank (*Figure 1*) and Statista (*Figure 2*) the share of agriculture and industry in world GDP dropped, and services have an increasing trend. These patterns aren't so clear and obvious from the WIOTs, moreover and surprisingly, they are rather the reverse. Data show a slight increase in the share of agriculture and industry, and a stagnation or rather a decrease in services (Figure 3). These are very different pictures of the structure of the world economy. And if these tendencies were strongly affected by the digitalization, they can give new perspectives to the possible outcomes of the Industry 4.0. Note that also World Bank data have a "correction" to the levels of WIOD statistics.

IV. The structure of the world economy in details

For the details, the most significant increasing and decreasing sectoral trends in the shares of output and value added, and tendencies of some digital industries are shown in *Figure 4 and 5*. Among the most increasing share trends, we have mining, food production, electricity supply, manufacture of basic metals, chemicals and so on. With a few exceptions, these all exploit and process the primary resources of the Earth, and convert it to food, energy or other basic materials. Only a few of them can be attached directly to digitalization, for example electricity supply, warehousing and supporting transportation.

Other researchers[4] also recorded a decline in trade, and some traditional industries crowded out by digitalization, for example manufacture of paper and paper products, printing and publishing, advertising and market research and so on.

For the digital industries, no clear and sharp increasing trends can be recorded. Except for some short periods of disturbances, for example the 2009 crisis, they grow at the same rate as the world.

V. Calculations with the Ghosh supply side input-output model

To show the implications of the changes of sectoral relationships and global value chains, calculations were made using the supply side input-output model by Ambica Ghosh (1958) (for the mathematical background see Miller–Blair (2009), Chapter 12).

[4] Timmer et al (2016)

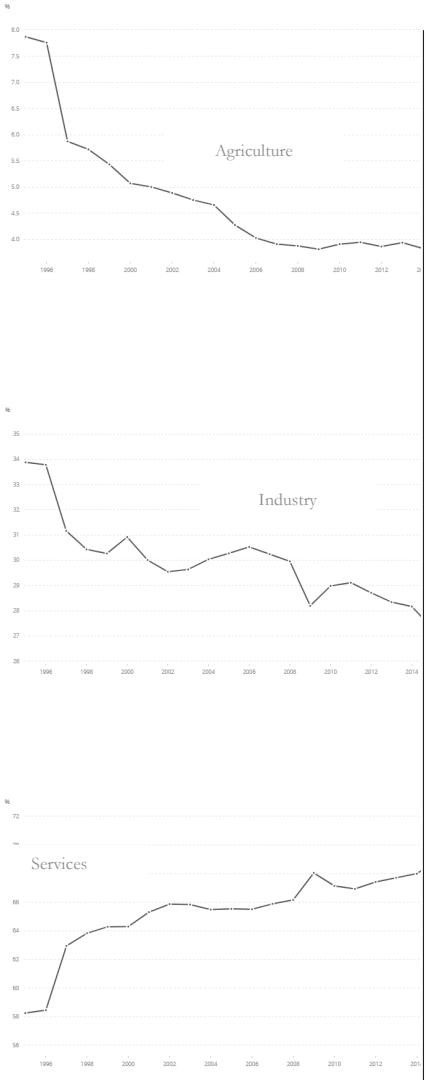


Figure 1
Global GDP by main sectors
Source: Wolrd Bank (data.wolrdbank.org)

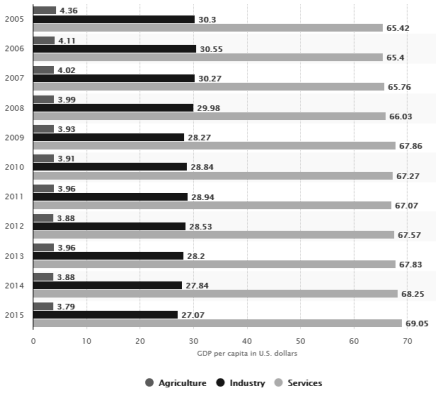


Figure 2
Global GDP by main sectors
Source: Statista (statista.com)

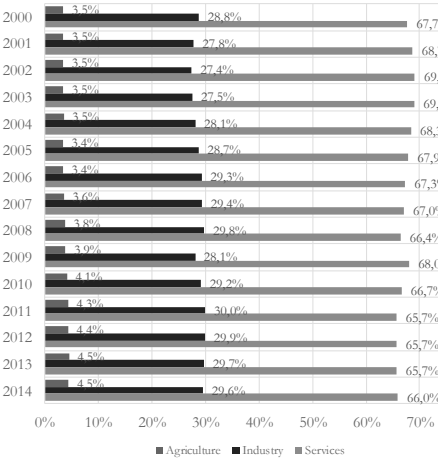


Figure 3
Global Value Added by main sectors
Source of the data: WIOD (wiod.org)

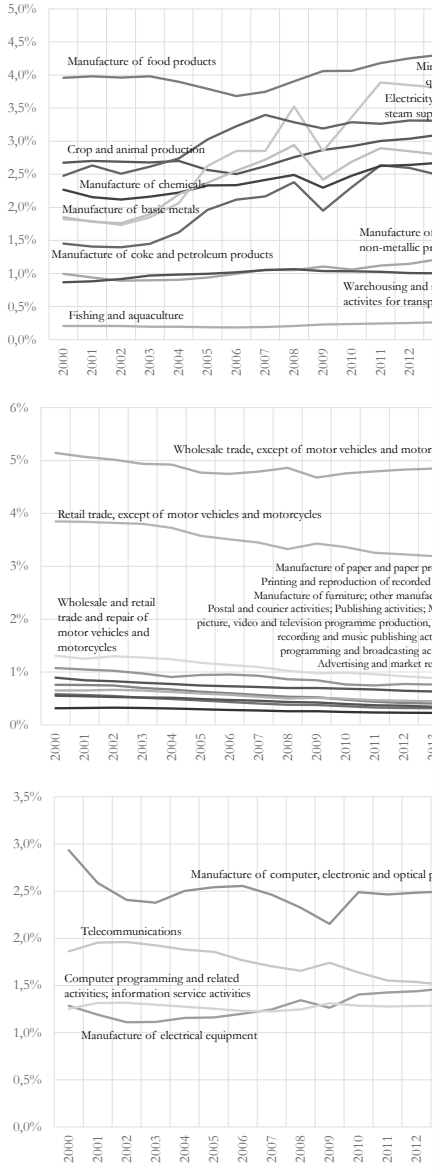


Figure 4

Industries with the fastest increasing (top) and decreasing (middle) trend in global output share, and the trends of the digital industries (bottom, share of global output)

Source of the data: WIOD

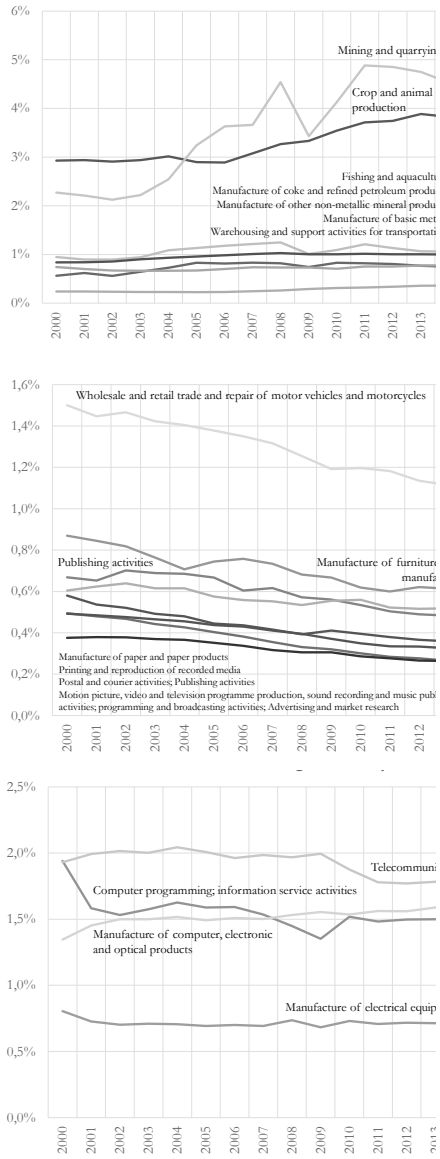


Figure 5

Industries with the fastest increasing (top) and decreasing (middle) trend in global value added share, and the trends of the digital industries (bottom, share of global value added)

Source of data: WIOD

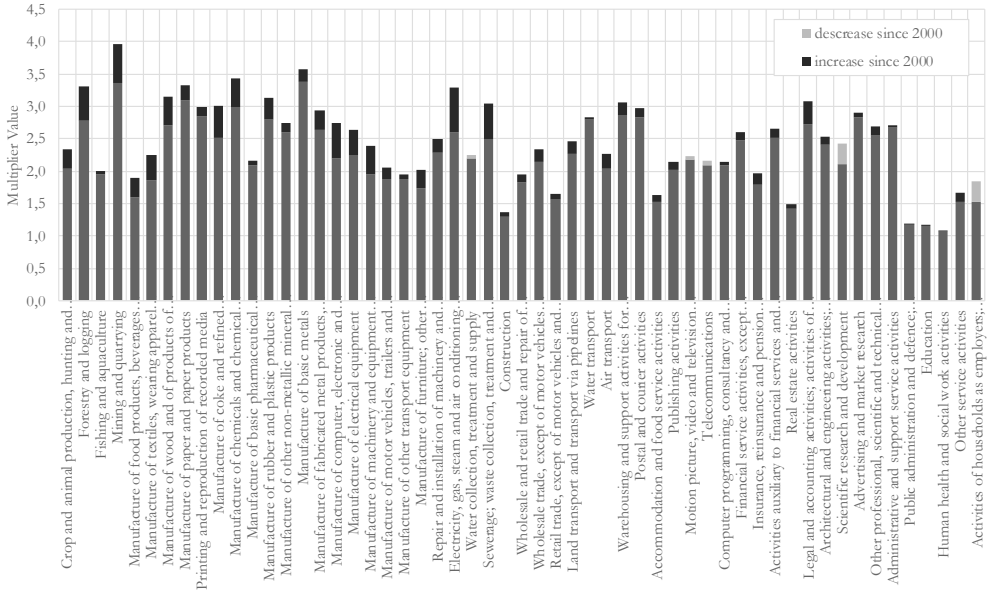


Figure 6

Output multipliers of the industries of the world

Source of the data: WIOD

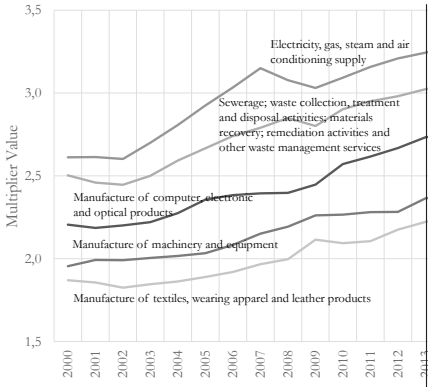


Figure 7

Five industries with the fastest incresing multiplier trend

Source of the data: WIOD

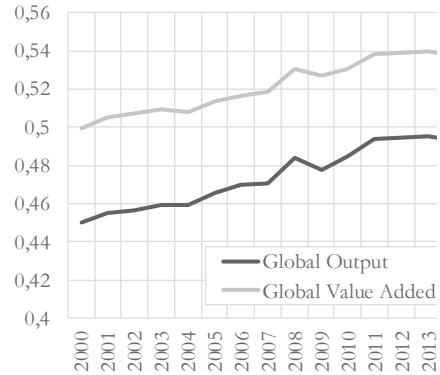


Figure 8

Gini-coefficients of global output and value added by supply chains

Source of the data: WIOD

V.1. Output multipliers

Output multipliers in *Figure 6* indicate the direct and indirect effect of one unit of primary resources used in an industry to the whole economy. Values of them for the year 2014 and the changes from 2000 are shown. The measures of agriculture and industry (they are in the first half of the chart) generally increased, but this is no so typical for services.

Among the top 5 industries with the most significant growth rate trend in their multiplier value we have the digital economy related electricity and energy supply, manufacture of computer, electronic devices and machinery (*Figure 7*).

V.2. Output and value added by supply chains

Intensities expressed by the multipliers are not enough. Intensity and volume together determine the total impact. To show these, alternative versions of *Figure 4 and 5* were produced, where diagrams would show the output and GDP shares for the industry supply chains. These charts are not published here because they haven't really changed the picture we drew before on relative sector weights and roles, and their change in *Figure 4 and 5*.

V.3. Concentration

The industrial concentration of the global economy was also investigated by Lorenz curves and Gini coefficients (*Figure 8*). They show that the concentration increased significantly: the same or a smaller number of industries give directly and indirectly a higher share of the world production and incomes. This is a key feature of our economy and with the digitalization, this process is expected to be more and more apparent and of a larger scale.

VI. Conclusions and further research

Before the conclusions, it is important to emphasize the limitations of the database and the calculations, which gave some clear and some controversial or surprising results, for example the contraction of services, or the relatively constant share of digital industries. Regarding these, note that our series of data end in 2014, but the great boom of digitalization started only after that. So, we must keep our eyes on the updates of WIOD and investigate what they say for the post 2014 years.

Of course, the analyses should be more detailed distinguishing countries and country groups, and giving results from the opposite direction, using the classical demand-pull Leontief analysis, as well

For the decrease of services, we expect that very change will come when digitalization and robots reach the high value added, labour-intensive service sector and crowd out human work. This can cause a decline in the output and GDP of service. Is this what our data and strange results show? Can't we see the forest for the woods? Has it already started? A deeper analysis with a focus on services can explore the details.

REFERENCES

Ghosh, A. (1958): Input-Output Approach to an Allocation System, *Economica*, 25, 58–64.

Miller, R. E., Blair, P. D. (2009): *Input-Output Analysis. Foundations and Extensions.* Second Edition. Cambridge University Press

Timmer, M. P., Dietzenbacher, E., Los, B., Stehrer, R. and de Vries, G. J. (2015): An Illustrated User Guide to the World Input–Output Database: the Case of Global Automotive Production, *Review of International Economics*, 23: 575–605

Timmer, M. P., Los, B., Stehrer, R. and de Vries, G. J. (2016): *An Anatomy of the Global Trade Slowdown based on the WIOD 2016 Release*, GGDC research memorandum number 162, University of Groningen

THE CONFLICT OF BLOCKCHAIN AND THE EU GENERAL DATA PROTECTION REGULATION IN THE AREA OF BUSINESS LAW

ANDREA LABANCZ[1]

Abstract

Innovation has a huge positive impact on many areas of the economy, constantly shaping economic relations and the law. Blockchain-based transactions, as results of technological innovation, may also cause structural changes in the national and EU legal systems, challenging the legislator. Taking into consideration that individuals who are subjects of blockchain-based transactions may be natural persons, it is necessary to examine the relevant data protection provisions. In this context, the question of this paper is whether the blockchain meets the data protection requirements of the GDPR, or conversely, the GDPR inhibits the business application of blockchain.

Keywords: *blockchain, GDPR, data protection*

I. Introduction

In the early 2000s, a new type of financial transaction has appeared. This innovative type of financial transactions is called the Bitcoin transaction in which Bitcoin is considered a virtual currency. Bitcoin transactions are based on a distributed ledger technology, called the blockchain.[2]

Even though, the blockchain is a technology, it may be considered a specific database from the approach of the law, in which data is collected and stored systematically and can be accessed by using IT devices.[3]

Blockchain and other distributed ledger technologies are able to change present economic relations. By using distributed ledger technology, centralized models can be replaced by decentralized models.[4]

The essence of centralized models is that the data is stored and shared centrally with the intermediation of a central market player. Given that, blockchain is a specific type of distributed ledger, where, generally, no central intermediary participates in the blockchain-based transactions.[5] Given the above, there is an opportunity for businesses to use the blockchain when entering into business relationship with natural persons.

The protection of natural persons has been identified as a priority within the European Union, due to the fact that each of the business transactions has influence on natural persons.[6]

The protection of natural persons in economic relations can be summed up through two main areas of law; consumer protection and data protection law. These areas may be distinct from each other on the basis of the nature of economic relations.

[1] dr. Andrea LABANCZ, PhD hallgató, Szegedi Tudományegyetem Állam- és Jogtudományi Doktori Iskola, Üzleti Jogi Intézet. Témavezető: Dr. habil. Gellén Klára, PhD. Elérhetőség: labancz.a@gmail.com
[2] Gates (2017) 25-28. pp.
[3] Polyák (2003) 128.p.
[4] Reed (2016) 16-17. pp.
[5] Eszteri (2012) 73. p.
[6] Benöhr–Micklitz (2010) 27-35.pp.

Natural persons should be defined as consumers in a case when the consumption characteristic is of paramount importance. In this context, the protection of natural persons is achieved by consumer protection law. Consumer protection law grants the legal basis of the enforcement of consumer rights, the education of consumers, the protection of consumer health and safety. As a matter of fact, the purpose of consumer protection law is to eliminate the economic inequality between businesses and consumers.[7] Data protection differs from consumer protection. By virtue of its nature, the purpose of data protection is providing privacy protection for natural persons. Data protection law grants the legal basis of personal data connected to natural persons.[8] Although the two areas of law have different interests, however, their interface is easy to see. It is the protection of natural persons.

Taking into account the above, in case of a blockchain-based transaction, both the consumer protection and the data protection regulation has a significant impact.

Therefore, the aim of this paper is to highlight the natural persons' protection issues in blockchain-based transactions, from a data protection point of view.

II. Blockchain in the area of business law

The scope of blockchain may be extended to a range area. It could be used in the area of public law, f. e. during elections, in procurement procedures, or substituting criminal databases, or in the area of private law, f. e. instead of using sales agreement registers or databases.[9]

As one specific area of the above mentioned potential application, blockchain may be considered an appropriate instrument for most commercial transactions, where business associations enter into a contract with natural persons and the personal data of natural persons becomes known. For example, these transactions can be performing simple payment transactions, storing order parameters, registering securities transactions, or even running smart contracts. Applying blockchain in business transactions could bring numerous benefits to business associations, f.e. shorter deadlines or lower costs.[10]

In case of business transactions, the business associations necessarily get information about the natural persons' personal data. Such data can be the name, address, financial transaction, as well as the IP address of a natural person, given that these are suitable for identifying a natural person.[11] In this case, it is important to store the natural persons' personal data in accordance with the rules and requirements of data protection.

From a business association point of view, blockchain can be used for the purpose of storing data, as set out the above. In this context, there is a need to pay special attention not only to economic benefits, but to the subjects of these business transactions i.e. to natural persons when considering the advantages of blockchain.

The protection of personal data is governed by a Community legislation, the General Data Protection Regulation (hereinafter referred to as 'GDPR'), which came into force in 25th May 2018. The purpose of the GDPR is to contribute to the accomplishment of freedom, security and justice within the internal market and to strengthen the well-being of natural persons.[12]

---

[7] Howells–Ramsay–Wilhelmsson (2010) 1-4.pp.
[8] Freidler (2009) 19-20.pp.; Jóri–Soós (2016) 15.p.
[9] Reed (2016) 16. p.; 55-69. pp.; Gates (2017) 59-69. pp.
[10] Reed (2016) 16-17. pp.
[11] Jóri–Soós (2016) 56-69. pp.
[12] GDPR Preamble (2)

III. Conflict of blockchain and the EU GDPR

Although, the GDPR has been designed to be technologically neutral, in case of blockchain technology, several considerations arise. The identity of the data controller and the scope of data controlling, as well as the question of profiling leave many aspects open to interpretation when it comes to blockchain.

Despite the fact that the above mentioned topics have significant importance when considering legal concerns related to blockchain, one specific provision of the GDPR should be taken into special consideration, which is Article 17 of the GDPR.

Article 17 of the GDPR i.e. the right to be forgotten (hereinafter referred to as 'RTBF') is a right that empowers natural persons to request the erasure of their personal data, under certain circumstances.

According to the cited provision, the data subject is entitled to request the deletion of its personal data, while the data controller is obliged to delete the relevant personal data. Such an activity, so the compliance with the requirement of RTBF, may cause legal obstacles in the practical application of blockchain.

In order to build a current picture of the conflict of blockchain and data protection provisions, it is necessary to examine the characteristics and basic function of blockchain.

In the blockchain, each data is stored in a so-called data block, which is closed by a cryptographic procedure. Such cryptographic procedures are also used to link certain data blocks. The linking procedure is being done by a specific method, so that each data block is built on one another, necessarily containing the cryptographic code (hash) of the previous block. Consequently, the data stored therein is retrospectively inalterable. One specific attribute of blockchain is this non-editable characteristic.[13]

This characteristic means that blockchain should be considered immutable and inalterable. It is almost impossible to change or delete data stored in the blockchain. In the light of present state-of-the-art, transactions in the blockchain may be considered irreversible.[14]

In that sense, the examination of the RTBF has an especially emphasized meaning. If the RTBF is exercised, one would therefore expect to act against the basic principle of inalterability of the blockchain.

To perform such a request, each of the blocks must be erased or corrected, until the requested data is reached.[15]

Taking into account that the RTBF is a legal requirement, failing which the practical use of blockchain is not acceptable, this right could hinder the use of blockchain to store personal data. Consequently, blockchain could not be used in business transactions.

IV. Potential and alternative solutions

Taking account of possible solutions, storing personal data outside the blockchain would seem to be the least difficult solution. Therefore, it would mean a restriction of technological development, so seeking appropriate alternative solutions is especially important.

[13] Gates (2017) 11-19. pp.; Reed (2016) 24-25. pp.
[14] Gates (2017) 14. p.
[15] Reed (2016) 24-25. pp.

In order to solve the conflict of the blockchain and the GDPR, two alternative solutions may be considered feasible, one of which is technological and the other is legislative.

The technological solution would be to create a new editable blockchain system that allows the data controller users to rewrite or delete data and data blocks, if the RTBF is exercised by any of the data subject users.[16] But as long as this is not the case, it is necessary to construe a legal environment that allows the benefits of blockchain to be exploited. In order not to make benefits arising from blockchain impossible, the EU legislation should interpret the RTBF in view of certain technical restrictions.

In light of that, it would be advisable to provide legal solutions for the conflict. In order to introduce such potential legal solutions, it is necessary to describe the scope of the RTBF.

It is thought that the RTBF has evolved from the Google Spain Case. In this case, the Court has ruled that citizens may request from operators of search engines the removal of content from the search index, if it contains information about the person and makes the natural person almost identifiable. According to the Court, processing personal data may affect the fundamental right to privacy and the protection of personal data. In the absence of such data processing, the natural person could not be interconnected with certain data or could be interconnected only with significant difficulty. Taking into account the above mentioned, this situation could not be justified merely by the economic interest. A balance should be reached between the legitimate interest of accessing information and the fundamental rights of the data subject.[17]

The Court has given an interpretation to the processing personal data in connection with business associations, in the Camera di Commercio Case. According to the judgment of the Court, data processing shall be based on the consent of the person or some other basis laid down by law, and shall be processed fairly, for specific purposes. The Court has ruled that, the person has the right to request the erasure or blocking of the processed data, but in order to grant these rights, it is necessary to examine the purpose. However, there may be some specific cases in which processing data may be necessary later the in future, *inter alia*, for the purpose of examining the legality of an act, or in order to enable third parties to exercise their right of bringing an action. The questions that may require this information to be provided may even be postponed for a few years after a particular act.[18]

Among that judgment of the Court, Article 17 Section 3 of the GDPR provides for exceptions to the RTBF. Indeed, the protection of personal data is not an absolute right, i.e. certain restriction on that right should be acceptable under the law, as it stated in the GDPR.[19] According to the cited provision, personal data cannot be deleted, if data processing is necessary for exercising the freedom of expression and information, protecting and performing public interest, or protecting legitimate interest.[20]

In case of providing alternative solutions to the conflict between blockchain and the GDPR, protecting public interest and protecting legal interest can be considered relevant, based on the cited judgment and the exceptions stated in Article 17.

---

[16] Cermeno (2016) 14-15. pp.

[17] Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González [ECLI:EU:C:2014:317]

[18] Case C-398/15 Camera di Commercio, Industria, Artigianato e Agricoltura di Leccev Salvatore Manni [ECLI:EU:C:2017:197]

[19] GDPR Preamble (4)

[20] See in details the GDPR Article 17 (3); Linder (2016) 36. p.

However, in order to be certain of the scope of public interest under the GDPR, it would be advisable to provide an indicative list, at the very least. Aside from this, it should also be noted that possible areas of blockchain application are being examined by a Community Institution, the Blockchain Observatory and Forum.[21] Taking into account that the competence of the institution is to highlight key developments of blockchain and to encourage governments, industries and citizens to benefit from its opportunities, so that its primary purpose is related to public interest, it would be acceptable to interpret blockchain in light of that, i.e. under the scope of public interest.[22]

In the event of blockchain being excluded from the scope of public interest, it would be worth considering interpreting blockchain in the scope of legitimate interest, given that the user's ownership may be based on or originates from data stored in the blockchain. Due to data blocks in the blockchain being only valid in conjunction with the previous data block, deleting parts of the previous data block containing personal data would inevitably generate uncertainty for the legal basis of future transactions. In this case, the legal basis of data processing should be based on the legal protection of another data subject, and data processing should be necessary.

V. Summary

It is a general rule, that changes in economy due to innovation and the novelties of technique, as well as the development of technology will always precede legislation. All of this means that legislation should regulate and, if it is necessary, repair detriments that have already occurred. For this reason, the law should be suitable for carrying out these tasks and not hinder technological development.

It is very difficult to establish an appropriate regulatory conduct. On one hand, there is a need for early regulatory action to grant legal protection for economic players and the market, but on the other hand too fast regulation can prevent innovation from gaining ground.

As one example of the above, practical application of the blockchain, an innovative solution in the 21th century, may be undermined due to the conflict of innovation and regulation. Even though the benefits of blockchain have already become obvious, its' potential applications are just being examined by the European Commission. In this context, there is a need to reflect the conflict of blockchain and the EU GDPR. This conflict is embodied in the so-called RTBF, i.e. the right to erasure of personal data.

Despite the fact that blockchain meets the requirements of data security, i.e. the blockchain system provides the possibility for natural person users to keep their personal data completely confidential, there is no fully developed opportunity of editing blockchain, on the basis of present state-of-the-art technology. Consequently, the law should play an active role in resolving the issue by creating an appropriate legal environment.

In this context, it is necessary to find the right balance between the protection of certain economic interests and the protection of natural persons.

It is the task of future legislature and application of law to find this balance.

[21] European Commission on Blockchain Observatory and Forum (2018)
[22] Linder (2016) 36. p.

REFERENCES

Benöhr, Iris – Micklitz, Hans W. (2010): Consumer protection and human rights. In: Howells, Geraint – Ramsay, Iain – Wilhelmsson, Thomas – Kraft, David: Handbook of Research on International Consumer Law. Edward Elgar Publishing Limited.

Cermeno, Javier Sebastian (2016): Blockchain in financial services: Regulatory landscape and future challenges for its commercial application. BBVA Research, No. 16/20. Available: https://www.bbvaresearch.com/wp-content/uploads/2016/12/WP_16-20.pdf

Eszteri, Dániel (2012): Bitcoin: az anarchisták pénze vagy a jövő fizetőeszköze? Infokommunikáció és Jog. Vol. 9. No. 49.(April)73.p.

European Commissionon Blockchain Observatory and Forum (2018) Available: http://europa.eu/rapid/press-release_IP-18-521_en.htm

Freidler, Gábor (2009): Az adatvédelem alapjai. In: Dósa Imre (lekt.): Az informatikai jog nagy kézikönyve. Complex, Wolters Kluwer Kiadó Jogi és Üzleti Tartalomszolgáltató.

Gates, Mark (2017): Blockchain, Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money. s. l. CreateSpace Independent Publishing Platform.

Howells, Geraint – Ramsay, Iain – Wilhelmsson, Thomas (2010): Consumer law in its international dimension. In: Howells, Geraint – Ramsay, Iain – Wilhelmsson, Thomas – Kraft, David: Handbook of Research on International Consumer Law. Edward Elgar Publishing Limited.

Jóri, András – Soós, Andrea Klára (2016): A személyes adat. In: Jóri András – Soós Andrea Klára (szerk.): Adatavédelmi jog, Magyar és európai szabályozás. HVGOrac Lap- és Könyvkiadó Kft.

Jóri, András – Soós, Andrea Klára (2016): Bevezetés – az adatvédelem helyzete napjainkban. In: JóriAndrás – Soós Andrea Klára (szerk.): Adatvédelmi jog, Magyar és európai szabályozás. HVG Orac Lap- és Könyvkiadó Kft.

Linder, Andreas (2016): European Data Protection Law, General Data Protection Regulation 2016. s. l. CreateSpace Independent Publishing Platform.

Polyák, Gábor (2003): Az információs társadalom szerzői joga. In: Dósa Imre – Polyák Gábor (szerk.): Informatikai jogi kézikönyv. KJK-KERSZÖV Jogi és Üzleti Kiadó Kft.

Reed, Jeff (2016): Blockchain. s. l. Create Space Independent Publishing Platform.

LEGAL ASPECTS OF OUR ONLINE DATA AFTER DEATH

SZABOLCS NÉMETH[1]

Abstract

What happens to our Facebook profile, e-mail account or personal blog after we deceased? This question is no more a theoretical one, but a very current issue. In the recent years this topic emerged more and more frequently so after the service providers, the legislation had to find answers (or at least to start to think about it). The topic of the online (personal) data after death is something between laws: data protection and civil law also have connection but they keep the distance. In the study, I will introduce the main questions and difficulties of the topic, the history of the regulation of online data after death and the current legislative results with the different approaches on different levels of legislation.

Keywords: *social media; online data; law of succession; data protection law; comparative law*

I. Introduction

It is unquestionable that the Internet has gradually become a decisive part of our lives since its release, and in the last few years the related processes have accelerated so dramatically that it is difficult to keep up with them for the older generations than the "Y" generation.

Here are some surprising information to highlight these phenomena, and to highlight how urgent it is for the legislators of modern legal systems to start making transparent and logical rules regarding such 21st century legal issues like posthumous online data. If we only look at the one but perhaps the most significant segment of the services available on the Internet, the social networking sites: there are currently around 1.4 billion active Facebook users, so nearly 18.4% of the world's population already use the most popular social site on a daily basis! This telling information is linked to the fact stated by an author of an article in the summer of 2017: 10,273 users of Facebook die a day.

When discussing this topic, the first question is why is it important at all to settle the legal fate of such online data after death? Different types of online data can activate different motivations, whether it is a purely emotional or even real economical interest.

In general, we can imagine two basic situations: in the first case, the aim of the deceased person and his relatives is to have access to or even have rights to use online data after the death of the late. In this case it may be necessary for the deceased to make actions for secure the access for his relatives to such data in his life and to inform his heirs of the types and location of these information. In the other case, the de facto situation is more complicated because the deceased person leaves data that he has kept in secret from his relatives during his lifetime, while after his death - even knowing the existence of these data or even just trying to access the whole set of data left over – the relatives violate the deceased persons' right to protect private secrets and personal data which he had in his life.

[1] Dr. Szabolcs NÉMETH, PhD student of Károli Gáspár University of the Reformed Church Faculty of Law Doctoral School

Legal disputes can come up in both cases. In the first type of the situation we can find on the opposing sides the service providers and the relatives requires access to the data in question. In the second type, the three-sided line-up contains the left-behind relatives, the service providers and the law enforcement agencies. After we considered these complex legal cases it seems like the challenge of the legislation of the very near future to invent solutions for the questions of posthumous online data.

In the interest of the deceased, it may also be that his relatives have access to his online data, whether emotional or artistic, such as letters, photographs, digitized works of art, and may manage the inheritance and make it to be the part of the family inheritance as similar physical objects (family jewels, old postcards, photographs, manuscript novels).

In addition there may be a reasonable need from the later deceased person to provide access for the heirs to his online data with significant economic value and be able to realize incomes with them (for example a website developed for years with hard work or musical artworks accessible on the Internet for a fixed fee).

On the other hand, the relatives can claim their access on the significant emotional value, even if it is a well known set of data created by the deceased in his life on the Internet or something they do not know especially, but they become aware of its existence after the death of their creator. It is not a special case when we can find the last expressed thoughts or manifestations of a person on the Internet. An illustrative example for these type of data can be a last shared photo of the deceased which can have huge emotional value for the mourning family members. The same emotional aspects appear in connection with the last sent online messages. Economical interests can also come up in these cases (for example if a last sent business e-mail contains important information which is not accessible on other digital platforms.) In our view, all of these demands are already well-grounded at first reading, which necessitates legal regulation, but in any case, substantive consideration and discussion.

II. Basic issues, possible approaches

The most important issue of our subject is that during the legislation and the legal judgement of the legal questions of the online data after death which right or claim do we prefer and protect? The right to protect the deceaseds' privacy and personal data which he enjoyed in his life and the rights after deaths which protect his memory (the root of these rights are the deceased person's fundamental rights)? Or the rights of his relatives to remember, rights for the inheritance, as well as the reasonable need for access to the online memories with serious emotional value? The latter claims are worthy of equity but have not been legally supported yet.

The next question is if we have the preferred interests, what legislative technique do we want to provide and protect them.

From the point of view of legislation, even though it seems that this issue can be connected by many legal and legislative areas (data protection law, civil law, but also criminal and procedural law), but it is difficult to clearly identify the regulatory structure that can be applied without justification the problem of the post-mortem status of online data.

From the point of view of privacy law, personal data can only be linked to a natural person, with the same standard of data protection law, so the legal status of these data becomes uncertain for a deceased person.

In our opinion this is can result an erroneous legal interpretation because based on its logic these data get into a legal vacuum by the death of the person who they are connected to. Did they practically lose their legal relevance and drift only as an IT unit in the sea of web 2.0? Scarcely despite of the approaches of effective laws and law enforcement agencies (data protection authorities on the first place). In our point of view, it is still more important in terms of the legal nature of these data that they were connected to a natural person at the time of their creation and could have a lot of relevance even after the death of that person. The General Data Protection Regulation directs the regulatory issues of online data of deceased persons into competence of the Member States. Thus the newest version of the Hungarian Data Protection Act contains provisions on these posthumous data management issues.

From the aspect of civil law, one possible way is to extend the legal concept of personal property and apply it beyond the physical objects to the data of the digital space. This would be the application of the analogy of the rights of rem to the online information, as some acts do it on the level of member states in the USA.

In many cases, consumers pay a fee for content that become available for them on the Internet after the payment, so in such cases such access can be surely categorized as a form of a pecuniary rights. These are the parts of the legacy by the rules of inheritance law, so it maybe sounds like a scene from a science-fiction movie, but it can happen very soon that on the inheritance trial the parties are arguing about the deceased's Spotify, Netflix or digital Financial Times subscription.

The situation is much more complicated, when it is not about digital forms of peculiar rights but about information which has only emotional value for the left-behind relatives. It is possible, that they do not know the exact content of these information – for example a private e-mail account – so we can not be sure if we are opening Pandora's box by disclosing these information to them or just help them to pull through the desperate times of mourning. The emotional motivations behind these requests for access can create a precarious situation for the legislation and the stabilization does not look like something what can be done easily with the techniques of law.

It is not surprising that, to the best of our knowledge, the legal system of the United States of America was the first which has paid attention to the subject of the legal aspects of the citizens' data after their death. The reason for this is that the largest service providers (Amazon, Google, Facebook, Twitter, Instagram, Yahoo, etc.) are all based in North America and, therefore, the "online existence" has become the most significant part of mass culture here.

Legislative settlement of online data is not yet a priority for all states in the US, with only eight of the fifty Member States of the United States of America adopting relevant legal provisions. Seven of these eight regulations at Member State level mention our topic only in a few sentences, or refer to online data after death in certain parts of regulating sentences. Apart from these eight states (Connecticut, Delaware, Idaho, Indiana, Nevada, Oklahoma, Rhode Island and Virginia), of course, several laws have been introduced to legislate on the posthumous issues of some forms of online data within the provisions of the member state level of inheritance right. In the case of other Member States, it is not expected that more specific laws in the Member States will be enacted due to the Uniform Fiduciary Access to Digital Assets Act enacted in the autumn of 2014.

III. Legislation of the USA

III.1 Level of Member States

On the level of Member States, the first was Connecticut where a regulation has been enacted about the rules of a procedure in which the service providers have to disclose the content of a deceased persons' e-mail account to his relatives. Later six Member States created its own legal rules, but these were about only a specific aspect of the topic, so its relevance is not significant already.

At last the State of Delaware has enacted provisions on the legal status of online posthumous data. In their case, however, we can talk about comprehensive regulation, which is not surprising: the codification was based on the original text of federal legislation which was finally enacted in the autumn of 2014 and which is still the most important legal source for our subject since it is broad, detailed and transparent. At the same time this act has designated a possible path ahead of the codification of the future.

III.2 Federal law

The most prominent federal law is the Uniform Fiduciary Access to Digital Assets Act (UFADAA), which was adopted in the autumn of 2014 and has since been amended several times.

The lobbying activities of large service providers (Facebook, Google, etc.) have also supported the adoption of this federal law, as it will also provide a much simpler situation for them if they have to comply with uniform rules in all Member States. To date, a total of 39 additional Member States have implemented the law at Member State level, so this legislation has become the indicator of substantive legislation throughout the United States.

The law, following highly detailed interpretative provisions, defines the obligations and rights of each person entitled to act in relation to the access of the deceased (or incapacitated) person's online data. So there are special regulations about the a fiduciary acting under a will or power of attorney, a personal representative acting for a decedent who died before, the trustee and a custodian in perspective of the access to the deceased persons' online data.

The person authorized to act, whether any of the foregoing, is considered to be a new contractor of a service contract between the former user and the data controller (service provider), and shall be entitled to such rights as the former user used to be. Thus, taking the provisions of applicable data protection laws into account at the same time, these people may request the data controller to make the user's electronic communication content accessible to them.

In addition to the federal law expounded above, two previously adopted laws are worth mentioning, although they were limitedly able to be applied to the problem of post-mortem online data, but before UFADAA the disclosure of these data was refused mostly on the reasons grounded by them.

The Computer Fraud and Abuse Act (CFAA) was adopted in 1986 as a complement to the Comprehensive Crime Control Act, which has existed for 2 years before. This federal law has primarily a criminal law nature and originally directed against cybercrime, against the creators and distributors of viruses and hackers that are becoming more and more problematic at the time of the adoption. It is intended to protect state computer systems and state secrets, so much of it is irrelevant for our subject. However, we must mention that since 1994, civil lawsuits can be initiated against the violation of this law, providing a reference basis for service providers. According to the

CFAA, that person commits a crime and therefore has a criminal responsibility who deliberately accesses a computer for that he does not have the permission and thus receives information from a protected computer if its conduct concerns communication between the states (ie, between the US Member States) or outside states. In 1986, under the concept of a protected computer, only the specially protected ones was understood which were owned by state authorities (and their employees), but since 1994 the legal definition of the concept has changed. Since then, all computers are considered to be protected by CFAA which are used for communication with interstate or external states, and civil lawsuits may also be initiated against those who demonstrate that conduct against such machines. The act names seven types of perpetration behavior, one of them is a topic to which service providers may rely and may refuse to release any data of the deceased. This is the breach of privacy.

The above-mentioned provisions of federal law offer a great opportunity for service providers to refuse to disclose the deceased's online data to their personal representatives by referring to the law. Practically, in states where there is no relevant provision in the level of Member States, this federal law is a barrier to any claim to know about online data posthumous. A part of the Electronic Communications Privacy Act, called The Stored Communications Act may also be a limit to access to the deceased's online data to the personal representative of the estate. It expressly states that it is forbidden for the service provider to release any data relating to the electronic communication it provides. However, in particular cases, the law exempts this ban.

IV. The current situation in Hungary

Looking at the subject of our research in the Hungarian legal environment, it is not as easy as it is in the US. The issue is hardly mentioned at the legislative level. As we mentioned above, the Hungarian Data Protection Act contains connecting regulations but in our opinion these are too rough-and-ready and has no practice yet. This does not mean, of course, that there has not been a case in Hungary that drew the attention of the authorities to the topic's actuality.

As part of the study of the Hungarian aspect, it is worth mentioning the legal case that came to the National Data Protection Authority (NAIH) in the fall of 2015. Following the case, a recommendation was issued on the subject of online legal death, and the president of NAIH, later turned to the Ministry of Justice calling the attention of the ministry and the legislative backlogs on the subject.

V. Summary

So far, we have presented the aspects and circumstances that make it timely in 2019 that legislation should address the issue of post-mortem online data. The solution to the United States has been described, where it has been on the agenda for several years, first on national and then federal level. When analyzing the situation in Hungary, we found that the regulator still felt that the issue was not timely enough, but there is more and more evidence of law enforcement and practice that this situation can not permanently persist.

If we look at the question through the lens of inheritance law, our plausible question may sound like this: how is it possible to shape the rules of testament so as they help the testator to ensure the legal fate of his online data or to help the heirs to get access to them? The problem is that although the notion of inheritance encompasses all the rights and obligations of a given legal entity, it will involve a narrower circle than the property itself, since it does not form part of the

personal rights and obligations (such as the right to vote). With this in mind - as mentioned above - assets with emotional value (such as domain names, subscriptions to media content) can be included in our will in the current legal framework and can be transferred to the heirs as part of the legacy. (Another question is how often this option is used by testators in real life.)

The introduction of the state's legislative mechanism would justify the fact that another group of online data is more likely to have the characteristics of personal rights. No surprise that the majority of services providers determine in the Terms & Conditions that their transfer is not possible).

For testators, the current legal environment also ensures, at a certain level, that online data which can not be interpreted as part of the legacy can be accessed after his death. Obviously, the most profane solution to have the necessary data for the access (typically a username and password) documented to certain non-transferable accounts is to deposit them in a document certified and deposited by a lawyer or notary, or by using less formal and secure forms, simply handing them over to their heirs on a piece of paper. However, it is only possible to provide access to the most important, most frequently used data. It seems unlikely that someone will include all of the usernames and passwords it in this document. If access has been provided by the testator, you can either designate a heir by order to appoint an explicit task to delete your online data from death (either manually or by your service provider). While in most of the legal systems we know it could be quite out of the line, in our opinion it would be best to settle this legal issue if, like US regulation, the concept of a representative can be introduced. After the death of the deceased this representative can take care of all of the legal relationships that the will or the inheritance cannot cover, like the non-material rights and obligations and the rights attached to the person (personal rights e.g.).

In our view, first of all, the "opening up" of the rules of inheritance law should legitimize the general requirements for online legal after death as the American acts do on the level of member states and federal also.[2]

[2] This study is the actualized and extracted version of the publication see in the biography.

REFERENCES

Németh Szabolcs (2016): Online adataink jogi sorsa a halál után. In: Tóth András (szerk.) Technológia jog: Új globális technológiák jogi kihívásai. Budapest: Károli Gáspár Református Egyetem, Állam- és Jogtudományi Kar, pp. 261-275. (Hungarian)

REGULATION AND AI IN THE FIELD OF ALGORITHMIC COPYRIGHT ENFORCEMENT

ANDREA KATALIN TÓTH[1]

Abstract

Copyright has been a major field of application for algorithmic enforcement technologies, which have been extensively criticized for their shortcomings, such as the lack of transparency and accountability. Self-learning machines and semi-autonomous AI have the potential to offer more sophisticated and balanced enforcement by code, however, they could also aggravate the aforementioned issues. This paper aims to identify the main issues and potential long-term consequences of rendering the use of „content identification technologies" essentially compulsory (as envisioned by the EU copyright reform) and thus leaving the public function of copyright enforcement to private tech companies and their constantly evolving technologies.

Keywords: *copyrigh law, AI, legislation, technology, EU law*

I. Introduction: copyright, exceptions and technology

Traditionally, the purpose and aim of copyright law has been to promote the advancement of learning and culture by providing certain exclusive rights to authors and creators in order to stimulate the production and dissemination of intellectual works. From an economic aspect, these exclusive rights (such as, inter alia: the right of reproduction, distribution or pubic performance) incentivize and reward the intellectual labour of copyright holders, as their right to exploit their works is ensured. However, for the sake of long-term development, and in order to make knowledge accessible, some forms of uses are excepted from the reach of exlcusive rights. Exceptions and limitations are carved out of copyright protection due to their de minimis impact on right holders' rights (e.g. private copying) or their socially benefitial purpose or nature (e.g. teaching illustration, criticism).[2] They also serve as a tool to create a balance between the economic and personal interests of copyright holders and the other fundamental rights (most importantly the freedom of expression and information) of users.

The other important point about copyright law for the purposes of this paper is that its development and the advancement of technology have been closely intertwined from the start: the appearance of the movable type and its contribution to the technology of dissemination of information resulted in the need for an exclusive right for publishers in order to secure their business and led to the appearance of copyright as a distinct field of law.[3] Throughout its history, technology and new technological inventions proved to have had the most relevant impact on copyright's evolution: new inventions not only accomodated new ways for uses, but also tended to

[1] Andrea Katalin TÓTH, LL.M. legal officer at the Department of International Copyright Law, Hungarian Intellectual Property Office, Ph.D. candidate at the Department of Civil Law of Eötvös Loránd University Faculty of Law and Political Science. Contact: andreakatalin.toth@gmail.com

[2] Gyenge (2010) p. 72.

[3] Joyce (2013) p. 16.

upset the above-mentioned balance between the interests of right holders and users.[4] The most dramatic change and challenge for copyright law so far proved to be the digitalization and the emergence of the Internet, as mass production and mass distribution also fosters mass infringement.[5] In this environment, the proper enforcement of exclusive rights became exponentially more difficult, as the actual digital uses are virtually impossible to track. Many commentators sought to find a solution to this „crisis" situation, with or without legislative means.[6]

II. Algorithmic copyright enforcement and its development

The so-called algorithmic enforcement of copyright appeared in light of the problem triggered by digitalization and the Internet. As it became clear that the traditional ways of enforcement became inefficient, the idea of using technology itself to solve the issues brought about by technology appeared,[7] in order to be able to control digital uses by digital means.

In copyright, the first generation of algorithmic enforcement tools comprised of the so-called technological protection measures (TPM) and digital rights management (DRM) technologies, which operated as digital locks: right holders could technically prevent unauthorized access to the digital formats of their works, by way of encryption.[8]

Later on, with the spread of social media and user-generated content (through the emergence of websites such as Facebook, YouTube, or Instagram), the second generation of these technologies appeared that targeted the online availability of copyright protected content.[9] The best example to illustrate the functioning of such systems is through the example of YouTube's ContentID. Through this mechanism, right holders provide information and data about their works to YouTube, based on which a digital fingerprint for that specific piece of content is generated. In the event of a newly uploaded video matching this fingerprint, it becomes flagged as potentially infringing content. As a consequence, the right holder has a choice: he can block the video, claim the ad-revenues generated by it, or simply follow the viewership statistics.[10]

The apparent benefit of the second generation systems is that contary to the first generation of enforcement technologies, they enable an ex post facto licensing mechanism through the possibility of claiming ad-revenues.[11] This way, the collection of revenues takes place after the actual use has already happened, instead of seeking preliminary authorization. Although it does not fit perfectly into the traditional copyright framework of prior licensing, this scheme accomodates freedom of expression and information better, as the default option is not to make the potentially infringing content unavailable for the public, but to keep it accessible in order to generate revenue

---

[4] Latman (1986) vii.
[5] Joyce (2013) pp. 45-47.
[6] For more on this, see: Mary L. Mills: New Tehcnology and the Limitations of Copyright Law: An Argument for Finding Alternatives to Copyright Legislation in an era of Rapid Technological Change, (Chicago-Kent Law Review. Volume 65, Issue 1, Symposium on Post-Chicago Law and Economics, 1989 April); Paul Edward Geller: Beyond the Copyright Crisis: Principles for Change (Journal of the Copyright Society of the USA. Vol. 55, 2008); Jessica Litman: Revising Copyright Law for the Information Age (In: Adam Thierer and Wayne Crews [eds.]: Copy Fights: The Future of Intellectual Property in the Information Age, 2002).
[7] About the idea that „code is law" and the role of technology as a means for indirect regulation, see: Lawrence Lessig: Code v. 2.0 (New York, Basic Books, 2006; available at: http://codev2.cc/download+remix/Lessig-Codev2.pdf
[8] Perel, Elkin-Koren (2016) p. 484.
[9] Perel, Elkin-Koren (2016) pp. 478–481.
[10] https://support.google.com/youtube/answer/2797370?hl=en&ref_topic=2778544
[11] Perel, Elkin-Koren (2016) pp. 512–513.

for the right holder. At first glance, this mechanism seems to be a near to ideal solution to the digital copyright law crisis: works are still accessible for the passive, consumer public, while enforcement is ensured and right holders receive income off of the use of their works. However, as it will be demonstrated below, one crucial group in this system of those active users that actually create the user-generated content, might actually be disfavored by this scheme.

III. The potential issues of algorithmic copyright enforcement

Even though the technologies introduced in the previous chapter cater for an effective and seemingly well-functioning enforcement of digital copyright, their potential drawbacks and the issues caused by them need to be considered as well.

First of all, the codes and algorithms used as the basis of these technologies are mostly treated as trade secrets and are kept hidden from the public. The resulting non-transparency can lead to overprotection and an abuse of power through a lack of accountability.[12] As a consequence, users are unable to adjust their behavior to be compliant due to their unawareness of the rules regarding the type of content that actually triggers the algorithm and qualifies as infringing use.

Secondly, right holders can effectively disable copyright exceptions by exercising excessively strict control over their content. The problem with the current content identification technologies (including YouTube's Content ID) is that although they are capable of filtering out matching content, they are unable to distinguish infringing use from uses that are excused as exceptions (e.g. when a work is used for commentary or criticism, in case of a review video made about a recently released movie).[13] Thus, even excepted uses could be flagged and blocked from public availability. Either inside or outside of the realm of copyright exceptions, disproportionality may present another issue. The terms of the after-the-fact „complusory licence" embodied in the demonetization and ad-revenue claims could be highly unfair and disproportionate to the actual use of the protected content.[14] For instance, the use of a few seconds of a song as background music in a vlog or a gaming stream could essentially „hijack" the advertising revenue of videos of substantial length and views. In jurisdictions where „de minimis" use falls outside of the scope of copyright protection, this issue relates back to the limitations of copyright.

Finally, whenever legal provisions are translated into code, private and potentially biased actors analyze and interpret the law. As these entities determine the metes and bounds of specific rules, they have a substantial potential in building bias that would favor their interests into the code.[15] Given that the interpretation of law is traditionally a public function of the judiciary, in instances when it is outsourced to private companies, the public scrutiny that courts and judges are otherwise subject to can be easily evaded.[16]

[12] Id, p. 483.
[13] Bartholomew (2015), p. 70.
[14] Id. p. 66.
[15] Friedman, Nissenbaum (1996) p. 333.
[16] Citron (2008), p. 1298.

IV. A new generation in algorithmic enforcement?

As artificial intelligence and machine learning is gradually taking over the world, algorithmic copyright enforcement seems to be an obvious field of application. The supply of infinite amount of user-generated content[17] provides an invaluable pool of diverse and unfiltered training data for autonomous and semi-autonomous systems, in a digital and mostly online environment.

Considering the issues of algorithmic enforcement discussed above, AI's and machine learning's main contribution towards algorithmic copyright enforcement could be their potential to spot and differentiate clearly infringing use from fair use.[18] In order to make these algorithmic systems more balanced in their functioning, the checks of the exclusive rights embodied in the exceptions and fair use should be part of their design.[19] Through an adequate flagging and training system,[20] the algorithm could be taught to identify cases of fair use or instances of copyright exceptions. Even though the different legal systems and jurisdictions regulate copyright exceptions differently,[21] the problem translated into code is rather uniform. There are some uses that necessitate the evaluation of the creator's intent and purpose: whether the work was used in relation to criticism or comment, a parody or for teaching illustration. AI is already getting better at understanding intent of the writer or speaker and the context of the specific text through natural language processing.[22] Additionally, it is known that YouTube actually uses machine learning in order to distinguish and eliminate extremist content from its platform, and, according to the company, the algorithm works quite well.[23] Based on these assertions, it is not irrational to imagine that the different AI and machine learning applications could be combined together to deal with more complex expressions and more complex issues, such as audiovisual content and copyright exceptions.

Nevertheless, even though the issue relating to fair use and exceptions could be potentially addressed, the problems already mentioned in relation to algorithmic copyright enforcement have the chance to be magnified in the context of AI and machine learning. Transparency would essentially disappear: some forms of autonomous systems generate their own code, while deep learning applications and neural networks function effectively as „black boxes" due to their immense complexity.[24] It would be close to impossible to tell if the machine made justified decisions and used the right criteria for assessing fair use. Similarly, accountability could present a new challenge: the question of how AI could explain its decisions also touches on the issue of legal

[17] According to some sources, there are 400 hours worth of videos uploaded to YouTube every minute and approximately 95 million pictures shared on Instagram daily. Sources: https://expandedramblings.com/index.php/youtube-statistics/ and https://www.omnicoreagency.com/instagram-statistics/.

[18] Elkin-Koren (2017), p. 1097.

[19] Elkin-Koren (2017), p. 1085.

[20] Lester, Pachamanova (2017), p.69.

[21] Although there is no opportunity to explore the topic in detail in this paper, regarding the subject of regulation of copyright limitations the distinction between the Anglo-American style of fair use/fair dealing system and the exhaustive list of exceptions found in continental European droit d'auteur regimes should be mentioned. While the former, more flexible scheme relies on the judicial interpretation of certain standards, the latter accomodates clearly and narrowly defined exceptions implemented by way of legislation.

[22] There has been recent developments both regarding sentiment analysis and sarcasm detection through deep learning. See: Sarikaya, Hinton and Deoras (2014) and Zhang, Zhand and Fu (2016) pp. 2457–2458.

[23] Source: https://youtube.googleblog.com/2017/10/an-update-on-our-commitment-to-fight.html

[24] For further information on this issue, see: https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/

personality of artificial intelligence.[25] Finally, the algorithm-driven pre-adjudication process could lead to biased decision making: even though the formal and public court proceedings would still be available for aggrieved parties, the trust put in algorithmic enforcement and automation bias[26] would discourage people from turning to the traditional judiciary when they feel that their rights as users have been violated by the application of automated enforcement measures.

V. Proposal for a directive on copyright in the Digital Single Market, Article 13.

These concerns have become even more relevant recently, as one provision proposed as part of the EU's current copyright reform, Article 13 of the proposal for a directive on copyright in the digital single market[27] (DSM Directive) would essentially make the employment of content identification technologies and algorithmic enforcement systems obligatory for certain platforms. It is due to the fact that one of the proposal's aims is to declare online content sharing platforms that store and handle a significant amount of copyright protected works to be primary users of the content uploaded by their actual end users[28] – this provision would thus mainly concern social media and content sharing sites, such as YouTube, Facebook or Instagram. As primary users of copyright protected works, it would be necessary for these platforms to obtain licenses, pay licensing fees and if they fail at fulfilling these obligations, they would have to face primary liability for copyright infringement. Based on the latest versions of the text, the platforms could potentially avoid liability if they performed certain measures and made their best efforts in order to prevent the availability of unauthorized content on their sites.[29] The earlier versions of the proposal even made an explicit reference to content ID technologies.[30]

Even though such technologies are currently used by some online platforms voluntarily, as these sites could still qualify as intermediaries, they could also benefit from the Ecommerce Directive's safe harbor provisions shielding them from secondary liability.[31] However, if we are to regard these platforms as primary users, the utilization of content ID technologies would essentially become obligatory for them to avoid liability. This creates a strong incentive for these platforms to overfilter and block any suspicious and possibly infringing content and also to strictly enforce the agreements concluded with rightholders: as large corporate copyright holders possess a more substantial negotiating power, this would possibly happen according to their terms.

Overall, the result of these provisions could be an environment where copyright exceptions and through them, the freedom of expression would be controlled by certain private actors. This

[25] For the extensive literature on the issue of legal personality implications of artificial intelligence see for example: Lawrence B. Solum (1991): Legal Personhood for Artificial Intelligences, North Carolina Law Review, Vol. 70. No. 4, 1231–1287. pp.; Paulius Čerka, Jurgita Grigienė, Gintarė Sirbikytė (2017): Is it possible to grant legal personality to artificial intelligence systems? Computer Law & Security Review, Vol. 33. Issue 5, October, 685–699. pp.; Ben Allgrove: Legal Personality for Artificial Intellects: Pragmantic Solution or Science Fiction? (June 2004) Available at: https://ssrn.com/abstract=926015;

[26] Bamberger (2010) p. 676.

[27] Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market, Brussels, 14.9.2016, COM(2016) 593 final.

[28] Article 13 paragraph (1), ST 8145/18 INIT (the latest version of the text as of 12.05.2018).

[29] Article 13 paragraph (4), ST 8145/18 INIT.

[30] Article 13 paragraph (1), COM(2016) 593 final.

[31] The proposal even makes explicit reference to the inapplicability of the Ecommerce Directive's safe harbor rules to online content sharing platforms that perform a communication to the public in Article 13 paragraph (3), ST 8145/18 INIT.

sort of privatization of enforcement fosters censorship. Additionally, we have seen the drawbacks of the currently working algorithmic enforcement systems and also the potential future issues of technology operated by artificial intelligence. If the legislator is about to make these systems essentially obligatory, then extra attention and care should be paid to the possible direction of technological develpoment. Unfortunately, based on the state of the current negotiations, these issues did not surface during the directive's preparatory work, as neither the impact assessment,[32] nor any documents released through the course of the Council-level negotiations considered or examined these aspects of the proposed provisions.

VI. Possible solutions

In light of the discussion above, the following question can be formulated: what measures in terms of regulation should be taken and what approach would be the best in order to address the issues presented above and to create a balanced system which could accomodate machine learning-based solutions in algorithmic copyright enforcement?

One possible device in creating a balanced technological ecosystem could be to create more detailed rules on both transparency and accountability: platforms would have to explain and justify their systems in general as well as their individual decisions in particular. One way, this could be achieved by setting certain standards of disclosure regarding statistics about disabled or demonetized content, which could provide some level of insight into the workings of these mechanisms.[33]

A useful and key device from a different aspect could be to design an effective and balanced complaint and redress mechanism, which would ensure that users would have an effective recourse within the system, when they feel that their rights were violated by the algorithmic preventive measures.[34] These rules should be detailed, specific and highly harmonized while ensuring that none of the interested parties (neither the right holders nor the platforms) have the discretion and power to arrive to a final decision about the justification of the users' appeals against the platforms' measures. It should be the task of independent, unbiased entities to decide whether such appeals are justified, as this could also provide the necessary amount of human review in a world largely run by algorithms.

Concerning the current negotiations on the new DSM Directive, these considerations have not become key issues for the legislator. Currently, the negotiations run in a reactive fashion where only the existing problems are addressedd with little to no consideration to the future direction of technological development and its possible implications. This manner of legislation has the potential to result in an already obsolete and defunct directive at the time of its entering into effect, which, in turn could generate even more reactive legislative activity. This way, the potential benefits of AI and machine learning to copyright law could prospectively be overshadowed by their disadvantages.

---

[32] Commission Staff Working Document Impact Assessment on the modernisation of EU copyright rules, Brussels, 14.9.2016, SWD(2016) 301 final.

[33] Lester, Pachamanova (2017), p.70. and Perel, Elkin-Koren (2016) pp. 529–530.

[34] The proposal already has certain provisions on a complaint and redress mechanism (Article 13 paragraph (7) ST 8145/18 INIT), however, these rules are broad and general and leave a significant margin of discretion to the Member States regarding their implementation. This particular issue has been the subject of extensive debate and discussions during the Council-level negotiations, as it is reflected in the different draft versions of the proposal.

REFERENCES

Bamberger, Kenneth A. (2010): Technologies of Compliance: Risk and Regulation in a Digital Age. Texas Law Review. Vol. 88. No. 4. March, 669–739 pp.

Bartholomew, Taylor B. (2015): The Death of Fair Use in Cyberspace: YouTube and the Problem with Content ID. Duke Law & Technology Review, Vol. 13. No. 1, March, 66–88. pp.

Citron, Danielle Keats (2008): Technological Due Process. Washington University Law Review, Vol. 85. Issue 6, 1249–1313 pp.

Elkin-Koren, Niva (2017): Fair Use by Design. UCLA Law Review, Vol. 64. Issue 5, August, 1082–1100. pp.

Friedman, Batya – Nissembaum, Helen (1996): Bias in Computer Systems. ACM Transactions on Information Systems, Vol. 14. No. 3. July, 330–347 pp.

Gyenge, Anikó (2010): A kivételek és korlátozások céljai a szerzői monopoljogban. Verseny és szabályozás. Vol. 4. No. 1, 72–119 pp.

Joyce, Craig (ed.) (2013): Copyright Law. New Providence, NJ, LexisNexis.

Latman, Alan (1986): Latman's the Copyright Law. Washington, D.C., Bureau of National Affairs.

Lester, Toni–Pachamanova, Dessislava (2017): The Dilemma of False Positives: Making Content ID Algorithms more Conducive to Fostering Innovative Fair Use in Music Creation. UCLA Entertainment Law Review, Vol. 24. Issue 1, 51–73. pp.

Perel, Maayan–Elkin-Koren, Niva (2016): Accountability in Algorithmic Copyright Enforcement. Stanford Technology Law Review, Vol. 19. Issue 3, February, 473–533 pp.

Sarikaya, Ruhi–Hinton, Geoffrey E.–Deoras, Anoop (2014): Application of Deep Belief Networks for Natural Language Understanding. IEEE TRansactions on Audio, Speech and Language Processing, Volume 22. Issue 4, April, 778–784. pp.

Zhang, Meishan–Zhang, Yue–Fu, Guohong (2016): Tweet Sarcasm Detection Using Deep Neural Network. Proceedings of COLING 2016, the 26th International Conference on Computational Linguistics: Technical Papers, December, 2449–2460. pp.