7th International Conference of
PhD Students and Young Researchers

LAW 2.0.

NEW METHODS, NEW LAWS

CONFERENCE PAPERS

Vilnius University Press
2019

INFORMATION ABOUT THE CONFERENCE:

Venue: Vilnius University, Vilnius, Lithuania

Date: 25-26 APRIL 2019

Scientific Committee of the Conference:

Prof. Dr. Tomas Davulis, Faculty of Law, Vilnius University

Dr. Donatas Murauskas, Faculty of Law. Vilnius University

Prof. Dr. Monika Namyslowska, Faculty of Law and Administration, Lodz University

Dr. Vigita Vėbraitė, Faculty of Law, Vilnius University

Conference Papers Editions composed by:

Dr. Vigita Vėbraitė, Faculty of Law, Vilnius University

Karolina Mickutė, Faculty of Law, Vilnius University

Ieva Marija Ragaišytė, Faculty of Law, Vilnius University

ISBN 978-609-07-0264-2

FOREWORD BY THE ORGANISERS

We are delighted to present you the seventh edition of international conference papers of the PhD students and young researchers. This year once again the international conference has been devoted to very live and challenging topic “Law 2.0.: new methods, new laws“.

Law is traditionally conceived of as a slow moving, incremental, and conservative sphere and profession. Today is obvious that technology is rapidly transforming both the practice and nature of law. Technology, design, and social innovation are being applied within the legal services and it is usually acknowledged that methods of law and techniques of law making are also impacted. It is obvious that there is a necessity to discuss on scientific level new legal techniques. Conference papers address the methodological transition in law implied by technological development.

Diversity of topics and countries represented in the conference shows that in 2014 established International Network of Doctoral Studies in Law by Vilnius University Faculty of Law, Frankfurt am Main J.W. Goethe University Faculty of Law, Paris Nanterre University Faculty of Law and Lodz University Faculty of Law and Administration already created an international platform to develop academic and scientific activities, to enhance quality of doctoral studies in law and to help the interchange of information and ideas among PhD students and professors.

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

Table of Contents

THE OPENING OF PUBLIC DATA IN THE EUROPEAN UNION

Vincent Annequin[1]

Abstract

Data holds an important place in our societies, it has become a basic element for many activities, such as scientific research or administrative decision. In the 21th century, accessing strategic data appeared as a necessity and became one of the main challenges for most European legal systems: free and unconditional access to these data must be guaranteed by law.

Among these important data, public data seems to be special. Indeed, being produced and / or held in the context of general interest missions, and often financed by taxes, these data seem naturally important and necessarily open. However, national laws organising the opening of public data are generally recent and are not immune to certain recurring criticisms, particularly in terms of transparency of the algorithms or in terms of protection of personal data. Also, some European-wide initiatives question the impact of the European law on the opening of public data.

Keywords: Open data, Public data, transparency, administration, re-use.

Introduction

According to the European Commission, "*data is the fuel that drives the growth of many digital products and services. Making sure that high-quality, high-value data from publicly funded services is widely and freely available is a key factor in accelerating European innovation in highly competitive fields such as artificial intelligence requiring access to vast amounts of high-quality data*".[2]

To study the opening of public data in the European Union (EU), the first step is to clarify the core of this subject: the data. Data has many definitions: it is both a piece of information[3] and the support of this information. In this way, data can take many forms: the main one is obviously the digital one, but data, taken as a piece of information, can be a

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

[2] European Commission – Press Release "Digital Single Market: EU negotiators agree on new rules for sharing of public sector data" [2019].

[3] J.-B. Auby, « Fasc. 109-30 : Données Publiques. – Définitions. Principes. Orientation » [2018] JCP A 13: Jean-Bernard Auby uses the expression "atom of information".

paper, a number, or even a fact.[4] This second dimension of data is very important when it comes to the opening of public data, because administrations can use this definition to refuse to open its data, because it is not a digital one. The current digital revolution, based partly on the development of smart grids and on the use of artificial intelligence, gives data an increasing importance: the production, the recording and the improvement of data is the first condition to have efficient smart grids and artificial intelligence. Data is the "*fuel*" of the second digital revolution. This phenomenon also explains why "*Big data*" is one of the biggest concern nowadays.[5]

Secondly, it is necessary to make a clear distinction between the Open data, and the opening of public data. In 2014, the French administration tried to build an official definition of the Open data, which has the merit to be formulated in a general way: Open data is "*a policy by which an organisation makes digital data available to all for the purpose of transparency or to enable their reuse, especially for economic purposes*".[6] The idea of Open data is to promote the spread and use of data. It implies a total and free access to data, but also that data must be made available in an open format for reutilisation. This movement goes beyond the public sphere and also concerns data produced and owned by the private sphere. Open data is part of the idea that digital and data should be a common good and must be protected.

Next to the Open data movement, the notion of public data must be individualised. Indeed, public data could be defined as "*open and raw information held or collected by a public entity and intended to be freely accessible. These data seem to be freely available to any citizen but cannot exclude possible protection as well as restrictions by intellectual property law or databases."*[7] But in the Member States, public data often comes out of a bigger notion: the administrative document. For example, in France, public data is finally an interpretation, a particular part of the administrative document access law.[8] In Spain, the right to access to information held by public administrations concerns any support (law 19/2013 of 9 December 2013, article 13)[9] and in Italia, the issue of the opening of public data is also part of the administrative document access law.[10]

In summary, Keegan McBride, Maarja Toots, Tarmo Kalvet and Robert Krimmer distinguish public data from the influence of the movement of open data on public data as

[4] A.-L. Stérin, M. Battisti, « Des données et des droits : Documentaliste-Sciences de l'information (DocSI) » [2012], vol. 49, n° 3, p. 20: "a generic term that covers very different realities: photo, number, fact, etc.".

[5] This notion also deserves a definition: according to the Commission Nationale Informatique et Libertés [French Data Protection Authority], Big Data "means not only huge amounts of miscellaneous data but also the techniques that make it possible to process them, to make them talk, to identify unexpected correlations, even to give them a predictive ability. Similarly, artificial intelligence is inseparable from the huge amount of data needed to train it and, in return, artificial intelligence processes the data" CNIL, "Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle", [2017], 18

[6] French Administration, Vocabulaire de l'informatique et du droit, JO 3 mai 2014, [2014] p. 7639.

[7] Y. Chéron "La réutilisation des données publiques : bases de données et open data" [2011] AJCT, p. 391.

[8] Indeed, even if few laws use the term of data (see the article 17 of the French Parliament Loi 2016-1321 pour une République numérique [2016] JO 0235), the public data legislation is part of the administrative document access law.

[9] Spanish Parliament, Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno

[10] G. Mancosu « L'accès aux données publiques et aux codes sources en Italie. A la recherche d'une « transparence algorithmique », à l'aube du règlement général sur la protection des données » [2018] RFAP n°167, p.575-584

follows: "*- Public data: "Public information (hereinafter information) is information which is recorded and documented in any manner and on any medium and which is obtained or created upon performance of public duties provided by law or legislation issued on the basis thereof (Riigikogu 2000); - Open government data (OGD): "Data that is collected and maintained by the government, machine-readable, human understandable, and licensed for all to use, share, and access (O'Reilly Media 2018)"*.[11] For these authors, "*in essence, all OGD is public data, but not all public data is OGD*", because open government data needs to be, for instance, easily available to the public, unlike public data.

The opening of public data has mostly increased under the presidency of Barack Obama since 2008. An important date for OGD is President Obama's memorandum on Transparency and Open Government, in January 2009: "*Government should be transparent (…). Government should be participatory (…). Government should be collaborative*".[12] Of course, the opening of public data already existed before 2008, and traditionally, Sweden is described as a pioneer: the first Swedish law on access to administrative documents dates back to 1776 (*Tryckfrihetsförordningen* or "*the fundamental law on the freedom of the Press*").[13] Furthermore, and to give more examples, the United States passed the Freedom of Information Act (FOIA) in 1977,[14] and France passed a similar law in 1978.[15] However, these first laws created a free access only to a limited amount of administrative documents, and these documents were opened only for individuals who asked for it: there was no real political will to fully open administrative documents.

Mostly since the early 2000s, Governments became aware of the advantages of opening administrative documents and, moreover, that the digital allowed the administration to share widely its information through the opening of public data. Three major benefits can be identified. Firstly, a democratic benefit, which is related to the transparency and the ability to control the Administration[16]. Secondly, a financial benefit: indeed, according to partisans of the Open data, taxpayers have already paid for the public data.[17] Finally, an important economic benefit explains why governments open public data: some data held by the Administration have a decisive role for economic operators. In a way, these important data could even be compared to essential infrastructures.[18]

The opening of public data is a European issue: indeed, many Member States of the EU have already passed laws on this subject. These laws have similarities, but also differences. It shows that the idea of an open government takes many forms in the EU. Moreover, it is interesting to study the opening of public data by comparing national

[11] K. McBride, M. Toots, T. Kalvet and R. Krimmer "Leader in E-Government, Laggard in Open data: Exploring the case of Estonia" [2018] RFAP n°167, p. 613-626

[12] President Obama, Memorandum on Transpareny and Open Government [2009] https://obamawhitehouse.archives.gov/the-press-office/transparency-and-open-government

[13] P. Jonason "Le droit d'accès à l'information en droit suédois : une épopée de 250 ans" [2016] http://ojs.imodev.org/index.php/RIDDN/article/view/137/175

[14] US Congress The Freedom of Information Act [1977]

[15] French Parliament Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal [1978]

[16] President Obama, Memorandum on Transpareny and Open Government [2009] https://obamawhitehouse.archives.gov/the-press-office/transparency-and-open-government:
"Transparency promotes accountability and provides information for citizens about what their Government is doing".

[17] M. Bourgeois Droit de la donnée [2018] Lexis Nexis, Droit & professionnels p.299: "data generated by the public sector, when financed by the tax, are common resources of the nation".

[18] Administrateur général des données, Rapp. au Premier ministre, La donnée comme infrastructure essentielle, 2017, p.41

legislations because the Members States are influenced by the same European law. One of the biggest European regulation on data is the General Data Protection Regulation of 2016,[19] but regarding the OGD, the influence of the directive on the reuse of public sector information (also known as "the PSI Directive"[20]) is important. Actually, the influence of the European legislation is growing since the first version of the PSI Directive in 2003: the PSI Directive implements a framework to all the different national legislations on the opening of public data. For example, PSI Directive's article 3 ensures that the reuse of public documents concerns commercial and non-commercial purposes.[21] However, the PSI Directive is not currently very restrictive for Member States[22] and besides, at first, the PSI Directive is not planned by the EU as an open access law for citizens: "*the PSI Directive focuses on the economic aspects of the re-use of information*".[23]

How are public data opened in the European Union? To answer this important issue, we must first analyse the gradual opening of public data in the Member States. Then, we will see how the two main rights implied by Open data are recognised in the European Union. Finally, we will study the external limits to the opening of the public data in the EU.

1. The gradual opening of public data in the European Union

Many concerns related to the opening of public data push the Member States to pass crucial regulations on this subject mainly since 2010: for example, the Spanish law on the Open data is passed in 2013,[24] the Italian[25] and the French[26] regulations in 2016. Yet, the opening of the European Commission's decisions is also part of this European movement: the European Commission opened its own data in 2011.[27] So, we must study the legal perimeter of these Open Government Data regulations. First and foremost, these rules accept limits that reduce the real impact of the OGD in the EU. These limits can be classified according two criteria: an organic criterion and a material criterion.

On one hand, Open data regulations are not the same in accordance with the administration. In principle, most of the administrations are submitted to open data legislations.[28] But for instance, in France and Spain, private operators have less obligations

[19] European Parliament and Council Regulation (EU) 2016/679 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)
[20] European Parliament and Council Directive 2013/37/EU of the of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information
[21] Ibid, article 3: "Member States shall ensure that, where the re-use of documents held by public sector bodies is allowed, these documents shall be re-usable for commercial or non-commercial purposes in accordance with the conditions set out in Chapters III and IV. Where possible, documents shall be made available through electronic means".
[22] Many PSI directive provisions accept national regulations exceptions.
[23] European legislation on the re-use of public sector information [2019] https://ec.europa.eu/digital-single-market/en/european-legislation-reuse-public-sector-information
[24] Spanish Parliament, Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno
[25] Italian Parliament, Legislative Decree n°97 of 25 May 2016 Freedom on Information Act [2016]
[26] French Parliament Loi 2016-1321 pour une République numérique [2016] JO 0235
[27] European Commission Decision of 12 December 2011 on the reuse of Commission documents [2011]
[28] French Parliament Loi 2016-1321 pour une République numérique [2016] JO 0235, article 2: "as part of their public service mission, the State, the local authorities as well as by other persons of public law or persons of private law charged with such a mission".

than other administrations, even if they are in charge of public services. In Spain, the Open data law of 2013 ignores partially these private operators: the obligation of "*active publicity*" does not apply to the data owned by these operators:[29] the Administration has to ask the data to the operator. According to Julian Valero Torrijos and Maria Belén Andreu Martinez, "*this intermediation constitutes an additional difficulty*".[30] In France, this intermediation also exists, but the public service concession holders have the obligation to give the relevant data to administrations.[31] The opening of public data held by private operators seems to be related to the ability of the Administration to centralise these data. In addition, Spanish and French legislations do not include some important private operators: in France, the data produced by a public service in competition cannot be reused.[32] In Spain, private operators "*who are in charge of specific public activities*", "*who are controlled by the administration or financed by it*" but created as firms or foundations can ignore the reuse of public data obligation.[33] The Member States' territorial organisation can also have an impact on the effectiveness of Open data legislations: in Germany, the right of access to the data covers the federal administration and the Lander.[34] Nevertheless, the "*publication by-default*" principle does not apply to the Lander's local administration.[35]

On the other hand, not all the public data are opened at the same level in the EU. Many exceptions exist, but some of them seem particularly interesting. First of all, the preparatory documents used and/or produced by the Administration cannot be generally opened: "*The right of communication applies only to completed documents*".[36] Then, even with completed documents, the material criterion is restricted by multiples exceptions, according to the object of the public information. Data related to the sovereignty of Member States is often excluded by Open data legislations: in France, all administrative documents that are related to the secret of the Government's deliberation, the national defence, the conduct of the foreign policy, the State security, the public security, the security of persons or the security of the information systems of administrations, the money and the public credit cannot be communicated.[37] The same logic exists in Italy when the access to some public algorithms can possibly put in danger the public security and order.[38] Of course, public documents covered by industrial property rights "*such as patents, trademarks, registered designs, logos and names*"[39] are traditionally excluded of the OGD legislations. Overall, relations between the opening of public data and the protection of personal data are complicated. Here, the influence of the EU on the Member States' regulations since the

[29] Spanish Parliament, Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, article 4
[30] J. Valero Torrijos M. B. Andreu Martinez L'encadrement juridique des données ouvertes en Espagne [2018] RFAP n°167, p.601-612
[31] French Parliament Loi 2016-1321 pour une République numérique [2016] JO 0235, article 17
[32] French Parliament Loi 2016-1321 pour une République numérique [2016] JO 0235, article 11
[33] J. Valero Torrijos M. B. Andreu Martinez L'encadrement juridique des données ouvertes en Espagne [2018] RFAP n°167, p.610
[34] German Parliament E-Government Act of 25 July2013 (Federal Law Gazette [BGBl.] Part I p. 2749
[35] Ibid, Section 12a
[36] French Code "Code des relations entre le public et l'administration", article L311-2. European Commission Decision of 12 December 2011 on the reuse of Commission documents [2011]: "to documents resulting from ongoing research projects conducted by the staff of the Commission which are not published or available in a published database".
[37] French Code "Code des relations entre le public et l'administration", article L311-5
[38] G. Mancosu « L'accès aux données publiques et aux codes sources en Italie. A la recherche d'une « transparence algorithmique », à l'aube du règlement général sur la protection des données » [2018] RFAP n°167, p.582
[39] European Commission Decision of 12 December 2011 on the reuse of Commission documents [2011] article 2

implementing of the General Data Protection Regulation in 2016 is incontestable.[40] The protection of personal data does not fit well with the opening of public data. Thus, either the personal data is an obstacle to the opening of public data containing personal information,[41] or it implies a significant work for the administration to anonymise data.[42] However, and even if the administration can anonymise the personal data, the risk of re-identification by crossing with other data still exists: this implies a re-identification risk analysis by the Administration, before opening data.[43]

This leads us to question the effectiveness of the rights shaping the opening of public data.

2. The European translation of the rights implied by the opening of public data

The opening of public data in the EU is based on two rights granted to citizens: the right of access to public information and the right of reuse public information.

The right of access to public information is historically the first which has been recognised. However, it is possible to distinguish two periods. The "*traditional one*", is quite old, as described in the introduction, even if mainly, the first European laws on this matter is nearly at the end of the 20th century (French Law in 1978,[44] Italian Law in 1990[45]) or at the early 21st century (Estonian Public Information Act in 2001, German Freedom of Information Act in 2005). This first step is limited: the access to public information only affected a citizen's request, who had to demonstrate his interest to access to such data. Nowadays, this phase seems to be complete in the EU, this right of access is a minimum: European citizens who require access to public data just have to ask the Administration. Then, more recently, European Governments have integrated Open data outcomes: more and more, European administrations forestall the right for citizens to ask access to public data and publish the data on their own initiative: it is the "*open-by-default principle*" or the "*active publication principle*".[46] From a practical point of view, this evolution of the right of access to public information is expressed by the creation of digital platforms, accessible to everyone via the Internet. This platform created by the Administration will allow each Member State (but also the European Commission[47]) to make available to citizens the data and databases held by the administrations: for instance, *portaltransparencia.gov.br* in Spain, *data.gouv.fr* in France, *govdata.de* in Germany or *opendata.riik.ee* in Estonia.

The right of reuse public information is the object of the PSI Directive and is the second right that form the effectiveness of an opening public data policy. According to the European Open data portal, "*by providing easy access to data — free of charge — we aim*

[40] Ibid
[41] French Parliament Loi 2016-1321 pour une République numérique [2016] JO 0235, article 6
[42] Spanish Parliament, Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, article 5.3
[43] J. Valero Torrijos M. B. Andreu Martinez L'encadrement juridique des données ouvertes en Espagne [2018] RFAP n°167, p.607
[44] Ibid
[45] Italian Parliament Administrative Procedure Act n°241 of 7 August 1990.
[46] For example, French Parliament Loi 2016-1321 pour une République numérique [2016] JO 0235, article 3
[47] EU Open Data Portal: data.europa.eu/euodp/data

to help you put them to innovative use and unlock their economic potential".[48] This quote raises at least two comments on the conditions to fulfil to have a real right of reuse. A right of reuse public information is relevant only if the legal framework ensures the free access to data. Increasingly, the reuse of data is free of charge, but not always. For this reason, the PSI Directive restricts the cost that an administration can ask: "*the total income from supplying and allowing re-use of documents shall not exceed the cost of collection, production, reproduction and dissemination, together with a reasonable return on investment. Charges should be cost-oriented*".[49] Despite the PSI Directive, there is still examples of administrations that limit the right of reuse by implement disproportionate costs.[50] Besides, the data must be easily readable by a machine. This condition becomes a major issue for Open data since the quick growth of artificial intelligence. So, most of the Member States have taken measures: data opened has to be in an "*open format, readable by a machine*" according to the Spanish legislation.[51] In Germany, "*the data will in principle be provided in a machine-readable format*" since the E-Government Act of 2013 (but this mandatory digitalisation only concerns federal administration).[52]

However, the right of access to public information and the right of reusing it can be limited in fact by problems that are external but not unknown to the field of data.

3. The main external limits to the opening of the public data in the European Union

These outside limits are plentiful, but it is possible to dwell on three problems: the digitalisation of the functioning of the Administration, the transparency of the algorithms and the transparency of metadata.

Indeed, a non-digital administration can be a huge obstacle to the opening of public data. As we saw in the introduction, data can be non-digital data, but the digitalisation allows a greater opening of data, and makes it easier to reuse public information. Furthermore, the European OGD legislations can exclude non-digital information. Thus, the German legislation excludes from the publication raw data that are produced by administrative action or public services provided by third parties ; when the information is initially kept on a paper format.[53] So, it would be possible for administrations to avoid Open data obligations by creating and keeping some data in paper format. Here, it is interesting to notice that the 2020's seems to be an important period for open and digital administration. Thus, for Spain and France, the horizon for a digital administration is represented by the beginning of the 2020s: 2020 for Spain, with the mandatory use of digital for the Administration (that will come fully into effect in 2020)[54] and 2022 for France, where the current Government aimed for "*the digitalisation of all administrative procedures, except for the first issue of an identity*

[48] https://data.europa.eu/euodp/about
[49] European Parliament and Council Directive 2003/98/EC on the re-use of public sector information [2003] article 6
[50] For example, about the access to the Spanish justice decisions, see J. Valero Torrijos M. B. Andreu Martinez L'encadrement juridique des données ouvertes en Espagne [2018] RFAP n°167, p.609
[51] Spanish Parliament, Ley N° 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público [2007]
[52] Ibid.
[53] German Parliament E-Government Act of 25 July2013 (Federal Law Gazette [BGBl.] Part I p. 2749, Section 12a
[54] J. Valero Torrijos M. B. Andreu Martinez L'encadrement juridique des données ouvertes en Espagne [2018] RFAP n°167, p.603

document" (but this mandatory digitalisation only concerns State administration).[55] Counter-examples exist in the EU. According to K. Bride, M. Toots, T. Kalvet and R. Krimmer,[56] Estonia is a leader in the field of e-government : 99% of Estonian public services are online, and the legislator implements digital, secure and systematised exchanges between the administration and the citizen via the so-called "*X-Road platform*" and an e-identity since 2001-2002. But Estonia seems behind concerning the opening of public data.[57] These authors show that the e-government seems to work so well that it may explain Estonia's delay in the area of OGD: the exchange of data on X-Road is sufficient for citizens. However, Estonia wants to catch up, and aims also for 2020.

Furthermore, algorithms used by the Administration have to be also transparent: indeed, why making transparent public data, while algorithms using or producing these data are not themselves transparent? Member States have understood this issue, and develop legal frameworks to avoid it. But, for the moment, algorithms, as a technical process, keep having difficulties to be well integrated in the juridical sphere. For instance, Italy and France use traditional notions of public law. In Italy, the algorithm's source code has to be publicly released because the Italian law[58] and case law[59] compare the source code to an administrative act. Therefore, the algorithm must respect the general rules of transparency of administrative acts[60]. In France, since 2016, transparency of the algorithm's source code is ensured by the general transparency rules for administrative documents.[61] Sometimes, the Administration tries not to apply this transparency obligations for public algorithms. A French law from 2018 (known as "*law ORE*"), creates an exception in transparency legislations for the placement algorithms for high school students used by the French universities.[62] Even if this legal exception has its reasons,[63] the risk lies in the potential multiplication of these exemptions from the transparency rules. An even more questionable case has occurred with the French administration, which was able to merge these two first external limits. Still in the academic field, the French Commission for Access to Administrative Documents (CADA)[64] obliged the National Education to communicate to an association of high school students the old algorithm of placement in universities

[55] French Parliament, National orientation strategy for public action Loi n° 2018-727 du 10 août 2018 pour un Etat au service d'une société de confiance [2018]
[56] K. McBride, M. Toots, T. Kalvet and R. Krimmer "Leader in E-Government, Laggard in Open data: Exploring the case of Estonia" [2018] RFAP n°167, p. 613-626
[57] Ibid., p. 615: "Why is Estonia struggling with providing and maintaining OGD when it appears to be a leader in many other aspects of digital governments?"

[58] Italian Parliament Administrative Procedure Act n°241 of 7 August 1990 [1990], article 22.1
[59] Regional Administrative Court of Lazio Roma, ect. III. Bis, March 22, 2017, n°3769
[60] G. Mancosu « L'accès aux données publiques et aux codes sources en Italie. A la recherche d'une « transparence algorithmique », à l'aube du règlement général sur la protection des données » [2018] RFAP n°167, p.580-581
[61] French Code "Code des relations entre le public et l'administration", article L300-2 : "Administrative documents ... include records, reports, studies, minutes, minutes, statistics, instructions, circulars, ministerial notes and replies, correspondence, opinions, forecasts, source codes and decisions".
[62] French Parliament, Loi n° 2018-166 du 8 mars 2018 relative à l'orientation et à la réussite des étudiants [2018]
[63] A non-final judgment of the Administrative Court of Guadeloupe asked the University of the West Indies to publish these algorithms, see, C. Stromboni "Parcoursup : la justice enjoint à une université de publier son algorithme de tri", Le Monde [2018] https://www.lemonde.fr/campus/article/2019/02/06/parcoursup-la-justice-enjoint-une-universite-a-publier-son-algorithme-de-tri_5419762_4401467.html
[64] CADA, avis n°20161989, 23 juin 2016, min. Education nationale [2016]

("*Admission Post-Bac*", or APB). Surprisingly, the Administration decided to communicate, in an incomplete format, the source code of the algorithm on paper format.[65]

Finally, the metadata transparency is the third main limit to a European relevant framework for the opening of public data. The importance of metadata was highlighted by the spying scandal on a very large scale carried out by the National Security Agency (NSA). NSA's surveillance focused mostly on these metadata.[66] Indeed, metadata give information on the data itself, as described by a French ministerial Decree from 2017: "*The administration that produces the reference data provides at least the following information (metadata): - information on the source and the date of the last update of the data; - the title of the data; - the description of the data; - the periodicity for making the data available; - the format of the data; - the geographical coverage of the data; - the re-use license applicable to the data; - the keywords of the data*".[67] Equivalent rules exist in other Member States, such as in Germany, where the opening of the metadata is also conceived at the same time as the publication of the data: public data "*are to be provided with metadata. The metadata will be included in the national metadata portal GovData*".[68]

These three limits demonstrate that the legal framework for the opening of public data in the European Union will only be fully relevant when the environment of the public data would be itself transparent and shared.

Conclusions

To conclude, the European legal framework on the Open data is not behind when we analyse the architecture of rights granted to citizens and international comparisons.[69] However, certain legal limits put in place in national legislation, notably about the scope of the OGD obligations, still restrain the access and the reuse of these data of general interest. Even if some external legal limits to the transparency of public data in Europe are worrying, it is clear that the European law and national laws are moving towards a digital administration that is more open to the society.

Bibliography

1. European Commission – Press Release "*Digital Single Market: EU negotiators agree on new rules for sharing of public sector data*" [2019]

[65] https://www.vie-publique.fr/actualite/alaune/admission-post-bac-etalab-preconise-publier-code-source-20170426.html

[66] see P. Szoldra, "Leaked NSA document says metadata collection is one of agency's 'most useful tools'" Business Insider [2016]: https://www.businessinsider.com/nsa-document-metadata-2016-12?IR=T

[67] French Administration Arrêté du 14 juin 2017 relatif aux règles techniques et d'organisation de mise à disposition des données de référence prévues à l'article L. 321-4 du code des relations entre le public et l'administration, annex.

[68] German Parliament E-Government Act of 25 July2013 (Federal Law Gazette [BGBl.] Part I p. 2749, Section 12a

[69] See for example https://index.okfn.org/place/: 15 European countries are in the top 30 countries in Open Data.

2. J.-B. Auby, « Fasc. 109-30: Données Publiques. – Définitions. Principes. Orientation » [2018] JCP A 13
3. A.-L. Stérin, M. Battisti, « Des données et des droits : Documentaliste-Sciences de l'information (DocSI) » [2012], vol. 49, n° 3, p. 20
4. Commission Nationale Informatique et Libertés [French Data Protection Authority], “Comment permettre à l’homme de garder la main ? Les enjeux éthiques des algorithmes et de l’intelligence artificielle“, [2017], 18
5. French Administration, Vocabulaire de l'informatique et du droit, JO 3 mai 2014, [2014] p. 7639.
6. Y. Chéron “La réutilisation des données publiques: bases de données et open data” [2011] AJCT, p. 391.
7. French Parliament Loi 2016-1321 pour une République numérique [2016] JO 0235
8. Spanish Parliament, Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno
9. G. Mancosu « L’accès aux données publiques et aux codes sources en Italie. A la recherche d’une « transparence algorithmique », à l’aube du règlement général sur la protection des données » [2018] RFAP n°167, p.575-584
10. K. McBride, M. Toots, T. Kalvet and R. Krimmer “Leader in E-Government, Laggard in Open data: Exploring the case of Estonia” [2018] RFAP n°167, p. 613-626
11. President Obama, Memorandum on Transpareny and Open Government [2009] https://obamawhitehouse.archives.gov/the-press-office/transparency-and-open-government
12. P. Jonason “*Le droit d’accès à l’information en droit suédois : une épopée de 250 ans*” [2016] http://ojs.imodev.org/index.php/RIDDN/article/view/137/175
13. US Congress The Freedom of Information Act [1977]
14. French Parliament Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal [1978]
15. M. Bourgeois Droit de la donnée [2018] Lexis Nexis, Droit & professionnels p.299
16. Administrateur général des données, Rapp. au Premier ministre, La donnée comme infrastructure essentielle, 2017, p.41
17. European Parliament and Council Regulation (EU) 2016/679 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)
18. European Parliament and Council Directive 2013/37/EU of the of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information
19. European legislation on the re-use of public sector information [2019] https://ec.europa.eu/digital-single-market/en/european-legislation-reuse-public-sector-information
20. Spanish Parliament, Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno
21. Italian Parliament, Legislative Decree n°97 of 25 May 2016 Freedom on Information Act [2016]
22. European Commission Decision of 12 December 2011 on the reuse of Commission documents [2011]

23. J. Valero Torrijos M. B. Andreu Martinez L'encadrement juridique des données ouvertes en Espagne [2018] RFAP n°167, p.601-612
24. German Parliament E-Government Act of 25 July2013 (Federal Law Gazette [BGBl.] Part I p. 2749
25. French Code "Code des relations entre le public et l'administration"
26. EU Open Data Portal: data.europa.eu/euodp/data
27. https://data.europa.eu/euodp/about
28. European Parliament and Council Directive 2003/98/EC on the re-use of public sector information [2003]
29. Spanish Parliament, Ley N° 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público [2007]
30. German Parliament E-Government Act of 25 July2013 (Federal Law Gazette [BGBl.] Part I p. 2749, Section 12a
31. French Parliament, National orientation strategy for public action Loi n° 2018-727 du 10 août 2018 pour un Etat au service d'une société de confiance [2018]
32. K. McBride, M. Toots, T. Kalvet and R. Krimmer "Leader in E-Government, Laggard in Open data: Exploring the case of Estonia" [2018] RFAP n°167, p. 613-626
33. Italian Parliament Administrative Procedure Act n°241 of 7 August 1990 [1990], article 22.1
34. Regional Administrative Court of Lazio Roma, ect. III. Bis, March 22, 2017, n°3769
35. French Parliament, Loi n° 2018-166 du 8 mars 2018 relative à l'orientation et à la réussite des étudiants [2018]
36. C. Stromboni "*Parcoursup : la justice enjoint à une université de publier son algorithme de tri*", Le Monde [2018] https://www.lemonde.fr/campus/article/2019/02/06/parcoursup-la-justice-enjoint-une-universite-a-publier-son-algorithme-de-tri_5419762_4401467.html
37. https://www.vie-publique.fr/actualite/alaune/admission-post-bac-etalab-preconise-publier-code-source-20170426.html
38. P. Szoldra, "*Leaked NSA document says metadata collection is one of agency's 'most useful tools'*" Business Insider [2016]: https://www.businessinsider.com/nsa-document-metadata-2016-12?IR=T
39. French Administration Arrêté du 14 juin 2017 relatif aux règles techniques et d'organisation de mise à disposition des données de référence prévues à l'article L. 321-4 du code des relations entre le public et l'administration, annex.
40. https://index.okfn.org/place/

COMPANY GROUPS REGULATION: LEGAL AND TECHNOLOGICAL CHALLENGES

Edvinas Bakanauskas[1]

Abstract

Conventionally, company law was aimed at regulating the activities of individual companies. A small number of owners who were mostly related to family or friendship relationships was characteristic of such companies. Generally, such companies would produce or sell one kind of goods and operate on the local geographic market[2]. However, favourable economic conditions and the right of the company to become a member of another company have determined the emergence of company groups. Until a company was allowed to become a shareholder of another company, neither parent companies, nor subsidiaries were known in company law.

On the other hand, despite the fact that company groups are an integral part of modern economy, only a few fragments of this institute have been established in a number of European Union (hereinafter – the EU) countries, including Lithuania. Such legal uncertainties and confusion lead to a gap between legal and economic realities. Company groups are obliged to operate according to the legal norms, which are adapted to the classical concept of a legal entity, but only partly comply with the specifics of company groups. Accordingly, the question arises whether the current legal regulation is appropriate to company groups. Besides, it is important to find out what technological challenges are encountered in the regulation of group activities and how to overcome them.

Keywords: Company groups, legal and technological challenges.

Introduction

Despite the fact that company groups are an integral part of modern economy, only a few fragments of this institute have been established in a number of European Union (hereinafter – the EU) countries, including Lithuania[3]. Such legal uncertainties and confusion

[1] PhD candidate in Vilnius University, Faculty of Law. Topic of the dissertation: Protection of Minority Shareholders' Rights in Group of Companies.

[2] J. E. Antunes, Liability of Corporate Groups. Autonomy and Control in Parent-Subsidiary Relationships in US, German and EU Law. An International and Comparative Perspective (Denventer, The Netherlands: Kluwer Law and Taxation Publishers 1994), p. 57.

[3] At the national Member States level, there are four major approaches: comprehensive regulation, partial regulation, case law recognition of the interest of the group, and lack of treatment. The first approach consists in a global and comprehensive regulation of groups of companies. This approach originates in Germany. A second approach consists in a partial or selective regulation, this is the case of Italy. The third approach is the French one. It derives from the 1985 Rozenblum decision of the French Supreme Court. Finally, some companies acts have no specific provisions on group interest. This approach is followed for instance in the Lithuania. European Model Company Act (EMCA)

lead to a gap between legal and economic realities. The lack of comprehensive regulation of company groups in Lithuania gives rise to a number of issues: more complex company group management, lack of properly ensured interests of minority shareholders and creditors of a company group.

The first part analyses issues relating to management of company group. For instance, a great deal of attention is paid to the recognition of the interest of the group. The second and third part deals with issues of protection of shareholders and creditors of a company group. The last part analyses issues relating to technological challenges in the regulation of group activities.

In the research analysis, the author also presents his position on the lack of company group regulation in Lithuania and submits proposals how to fight the legal and technological challenges.

1. Management of company group

Traditionally, it is acknowledged that the management bodies of a single company have to operate according to the company's interests. A typical aim in this case is to maximise profit, take a larger share of the market, improve product quality[4].

However, this is not entirely the case for a company group. The interests of each company in the company group make up only a certain share of the overall interests of the company group[5]. Therefore, in certain cases the management bodies of a subsidiary might have to solve a dilemma: to follow the orders of the parent company and thus fulfil the interests of the company group, or to exclusively represent the interests of the subsidiary. In fact, as per the existing Lithuanian regulation, the management body members do not have any choice but to represent the interests of the subsidiary. Article 2.87 of Civil Code of the Republic of Lithuania[6] (hereinafter – CK) establishes the main duties for the management body members of a legal person[7]. In clarifying said article, the Supreme Court of Lithuania (hereinafter – LAT) has indicated multiple times that legal person's management body members have a duty to exclusively represent the interests of the legal person (CK Article 2.87) and a failure to fulfil or inadequate fulfilment of this duty makes the management body member liable under CK Article 2.87, Paragraph 7[8]. Therefore, according to the existing regulation and LAT stance, if the management body members of a subsidiary, acting under the parent company's orders, make a decision not for the benefit of the subsidiary but for the

---

[2017], accessed 10 April 2019. Accessible via the internet at: <http://law.au.dk/fileadmin/Jura/dokumenter/forskning/projekter/EMCA/2017-03-30_EMCA_withlinks.pdf >, p. 355.

[4] J. E. Antunes, Liability of Corporate Groups. Autonomy and Control in Parent-Subsidiary Relationships in US, German and EU Law. An International and Comparative Perspective (Denventer, The Netherlands: Kluwer Law and Taxation Publishers 1994), p. 63.

[5] Ibid., p. 67.

[6] The Civil Code of the Republic of Lithuania [2000]. Valstybės žinios, 2000, nr. 74-2262.

[7] BAKANAS, A., et al. Lietuvos Respublikos civilinio kodekso komentaras. Antroji knyga. (Vilnius: Justitia 2002), p. 192.

[8] Panel of Judges of the Civil Division of the Supreme Court of Lithuania. 22 October 2008 ruling in the civil case Alaja ir ko UAB v. K. A. and V. A., No. 3K-3-509/2008, cat.: 27.1; Panel of Judges of the Civil Division of the Supreme Court of Lithuania. 12 September 2014 ruling in the civil case Mitnija UAB v. Statybų kryptis UAB, V. G., A. J., third party Nigema BUAB, No. 3K-3-389/2014, cat.: 27.7; Panel of Judges of the Civil Division of the Supreme Court of Lithuania. 11 December 2015 ruling in the civil case Creditum UAB v. G. Z., No. 3K-3-665-969/2015, cat.: 2.2.2.7.

benefit of the company group, they will be considered to have violated their duty to exclusively represent the subsidiary's interests.

On the one hand, it is agreeable that the management bodies of a single company must exclusively represent that company's interests. On the other hand, the questionable part is that the same regulation should also apply to company groups. As already mentioned, the interests of one company in the company group make up only a certain share of the overall interests of the company group. So in practice the parent company gives instructions to the management of a subsidiary, thus implementing the joint interests of the company group. It is clear that, without making it possible in certain cases for the subsidiary's management bodies to represent the interests of the entire company group instead of only those of the subsidiary, quite a few issues arise. Firstly, the application of the existing company legal regulations for company groups does not correspond to the economic reality. In certain cases the management bodies of a subsidiary represent the joint interests of the company group that are in line with the interests of the parent company but that are not in line with the interests of the subsidiary. Secondly, in implementing the company group's interests that go against the subsidiary's interests, the subsidiary's management bodies violate their duties indicated in CK Article 2.87 to exclusively represent their legal person's interests. This means that the subsidiary's management body members are not properly protected. The specific circumstances of management bodies within company groups should be taken into account.

1.1. The interests of the group and the right of a parent company to give instructions to the management of a subsidiary

As mentioned above, neither the CK nor the Republic of Lithuania Law on Companies[9] enables the possibility in certain cases for the subsidiary's management bodies to represent the interests of the entire company group instead of only those of the subsidiary. Accordingly, in case of representing the company group's interests instead of the subsidiary's interests, the subsidiary's management bodies may be considered to have violated their duty established in CK Article 2.87 – to exclusively represent their legal person's interests. Therefore, it is obvious that Article 2.87 of CK is adapted to single companies and not always can be appropriately applied with regard to the management of the companies within a company group. This issue has to be solved, but the main question is how. The Lithuanian company law is expected to establish the same right as is established in the European Model Company Act, Chapter 15, allowing a parent company to give instructions to the management of a subsidiary and acknowledging the interests of the company group. In short, the EMCA Chapter 15 Section 16 establishes the interests of a company group, making it possible for the management of a subsidiary to make a decision that goes against the interests of that subsidiary, especially upon receiving instructions from the parent company to do so. However, such a decision can be made only under certain conditions which are also set out in said section. In such a case, the management body of a subsidiary would not be considered to have violated its fiduciary duties. And the EMCA, Chapter 15, Section 9 establishes the right of a parent company to give instructions to the management of its subsidiary. Naturally, a question may arise, why exactly the EMCA's provisions should be adopted. Firstly, because the EMCA's provisions are modern[10],

[9] Republic of Lithuania Law on Companies [2000], Valstybės žinios, 2000, nr. 64-1914.

[10] The EMCA was designed to solve the relevant issues of company law. For instance, EMCA, Article 15 was designed to solve the issue of a lack of company group regulation. For more on the relevance

compatible with the applicable EU legislation and, most importantly, because the EMCA's provisions were formulated taking into account the best legal practices of the EU member states.

2. The problems of protecting the rights of minority shareholders in a company group

It is usually accepted that a share grants its owner the three rights: the right to participate in managing the company, the right to receive a share of the profits in the form of dividends, and the right to receive a share of the company's assets when the company is wound up. The other rights of the shareholder are considered additional, for instance, the right to be informed, the right to initiate the general meeting of shareholders[11]. But as soon as a company loses its independence and becomes a part of a company group, it becomes more difficult for shareholders to exercise their rights.

Firstly, the right to receive distributed assets of the company[12]. It should be noted that a company group is like an *internal market* where the parent company constantly redistributes and manages the financial resources of its subsidiaries in order to maximise its return on investment. Therefore, in certain cases, even if a subsidiary is profitable, the parent company may decide not to pay dividends. In such a case, the interests of minority shareholders may be damaged[13]. Secondly, the right to participate in managing a company[14]. The decisions made during the general meeting of shareholders of a subsidiary are rather declarative because usually the real decisions had already been made by the parent company. Therefore, the voting right of the shareholders often becomes a meaningless gesture[15].

Thirdly, the right to be informed. Only when a shareholder is well informed on the company and its activities, can he/she decide whether to purchase newly issued shares or to sell the current ones[16]. Ensuring the right to be informed in a company group is much more

---

of this company-law issue see: The Reflection Group on the Future of EU Company Law [2011], accessed 11 April 2019. Accessible via the internet at: <http://ec.europa.eu/internal_market/company/docs/modern/reflectiongroup_report_en.pdf>, p. 59 – 75.

[11] L. Mikalonienė. Uždarosios akcinės bendrovės akcininko teisės ir jų gynimo būdai (Vilnius: SE Centre of Registers 2015), p. 54, 57.

[12] It should be noted that both the right to receive a share of the profit of an active company, and the right to receive a share of the company's assets when it ceases to be active are separate forms of the shareholder's right to receive distributed assets of the company. Ibid., p. 54.

[13] J. E. Antunes, Liability of Corporate Groups. Autonomy and Control in Parent-Subsidiary Relationships in US, German and EU Law. An International and Comparative Perspective (Denventer, The Netherlands: Kluwer Law and Taxation Publishers 1994), p. 89.

[14] This right can be understood both in the narrow sense and in the broad sense. In the narrow sense, the shareholder's right to participate in managing the company is related to the general meeting of shareholders. In the broad sense, the shareholder's right to participate in managing the company is not limited to the general meeting of shareholders. It also involves additional legal leverage in controlling the company's activities. L. L. Mikalonienė. Uždarosios akcinės bendrovės akcininko teisės ir jų gynimo būdai (Vilnius: SE Centre of Registers 2015), p. 55.

[15] J. E. Antunes, Liability of Corporate Groups. Autonomy and Control in Parent-Subsidiary Relationships in US, German and EU Law. An International and Comparative Perspective (Denventer, The Netherlands: Kluwer Law and Taxation Publishers 1994), p. 89.

[16] L. Mikalonienė. Uždarosios akcinės bendrovės akcininko teisės ir jų gynimo būdai (Vilnius: SE Centre of Registers 2015), p. 59.

difficult. For example, having information only about the activities of a subsidiary is insufficient for the shareholder of that subsidiary to be able to make a well-informed investment decision. The effectiveness of the subsidiary's activities depends on the entire company group, so only by knowing the situation in the entire company group can the shareholder make a well-informed decision.

3. Protection of creditors in the company group

Usually, in a company group creditors' rights could be violated in two ways. Firstly, the structure of the company group itself reduces transparency with regard to real assets – it creates an illusion that the liabilities of an individual company are backed by the assets of the entire company group. Secondly, the company group often redistributes the value of its assets[17].

It should be noted that company law presumes the limited liability of shareholders. The limited liability of shareholders means not the company's limited liability to the company's creditors but the shareholders' limited liability to the company's creditors[18]. The limited liability of shareholders is exactly what can cause in certain cases a violation of the creditors' rights.

Said rule was indicated in the *Salomon*[19] case. It was exactly this case where the *corporate veil* doctrine was formed, which is based on the principle of separation. At its core is the notion that the company and its member are separate entities having separate assets and independent liabilities according to their duties[20].

In many countries, the corporate veil doctrine is applicable to company groups as well. Therefore, a parent company can use the principle of separation and limited liability to avoid liability to the creditors of a subsidiary. The parent company is granted the freedom to found subsidiaries and decide the size of the subsidiaries and control their finances. When a subsidiary becomes insolvent, its creditors cannot demand the fulfilment of its liability by another member of the company group[21]. In other words, on the grounds of limited liability, the parent company can engage in more risky activities and avoid liability. Thus, unconditional application of the principle of separation can damage the creditors' interests, especially in company groups. Obviously, the creditors' interests should be protected. But the question is how. Should it be established that the damage incurred by creditors must be compensated jointly by entire company group? Or should there be exceptions to the principle of separation?

---

[17] G. Hertig and H. Kanda, Creditor Protection. From R. Kraakman, et al. The Anatomy of Corporate Law: a Comparative and Functional Approach. 1st ed. Oxford: Oxford University Press. From L. Mikalonienė, Asmeninio komercinio bendradarbiavimo pagrindinės teisinės formos: doctoral thesis. Social sciences, law (Vilnius: Vilnius University, 2011), p. 314.

[18] Ibid. p. 101.

[19] P. Muller, Creditor Protection in the Law of Corporate Groups – A Comparison between the U.K. and German Legal Approach (München: Akademischen Verlagsgemeinschaft München 2013) p. 8-9.

[20] V. Papijanc, Piercing the corporate veil institutas ir patronuojančios įmonės atsakomybė pagal dukterinės įmonės prievoles Lietuvos teisėje [2008], no. 10(112), p. 96.

[21] P. Lipton, The Mythology of Salomon's Case and the Law Dealing with the Tort Liabilities of Corporate Groups: An Historical Perspective [2014], accessed 11 April 2019. Monash University Law Review, 40(2). Accessible via the internet at: <http://www.austlii.edu.au/au/journals/MonashULawRw/2014/20.html>, p. 454, 482.

The answer to said questions depends on whether the company group can be considered an independent enterprise or whether each member of the company group can be considered a separate independent legal person. These are the factors that determine against whom a creditor can make claims with regard to fulfilment of a liability: against any member of the company group or against one specific legal person[22].

In the US, a theory was developed based on the concept of an integral unit (hereinafter – the identification theory). This theory is known to have influence in the EU and continental Europe as well (for example, Denmark, France, Germany). According to this theory, the separation of the companies within a company group is ignored. The group companies are regarded as a single enterprise. It means that the economic context is valued, not the legal one. A group could be understood as a single enterprise due to, for example, the its structure, joint management, mixed finances, joint business policy. It is assessed in the economic context whether the legal form of individual companies is only an artificial fragmentation of the joint business into separate sub-units[23].

However, in many countries each company within a group is considered an independent legal person. For example, in the case of *Walker v. Wimborne* the Australian Supreme Court ruled that the CEOs of subsidiaries must act on behalf of the interests of the subsidiary, not the entire company group. In another case, *Industrial v. Blackburn*, the Australian Supreme Court clarified that the profit earned by a subsidiary cannot be considered the profit of its parent company[24].

It should be noted that England also does not acknowledge a company group as a single enterprise. For example, in the case of *Adams v. Cape Industries plc.* the court ruled that there is no general principle that all the members of a company group should be considered a single entity. On the contrary, the fundamental principle is that each company of a company group is a separate legal person with respective rights and obligations[25].

In Lithuania each company within a group is also considered an independent legal person. However, the Lithuanian CK, Article 2.50, Paragraph 3 provides for an exception to the principle of separation. As explained by the LAT, this Paragraph 3 is meant exactly for the protection of creditors[26].

It should be noted that CK, Article 2.50, Paragraph 2 establishes a general rule that a legal person shall not be liable for the obligations of its member and the latter shall not be liable for the obligations of the legal person with the exception of cases provided by the law and incorporation documents of a legal person. Paragraph 3 of said article indicates that where a legal person fails to perform his obligations due to acts in bad faith of a member of the legal person, the member of a legal person shall, in a subsidiary manner, be liable for the obligations of a legal person by his property. Judging from the linguistics of CK, Article 2.50, Paragraph 3, it is clear that the member of a legal person becomes liable under certain conditions: 1) the legal person itself is unable to perform an obligation; 2) the member of the legal person is found to have acted in bad faith; 3) a causal relationship exists between the member's actions in bad faith and the damage incurred by the legal person. In those cases

[22] E. Boros and J. Duns, Corporate Law. 3rd ed. (Oxford University Press 2013), p. 49.
[23] L. Mikalonienė, Asmeninio komercinio bendradarbiavimo pagrindinės teisinės formos: doctoral thesis. Social sciences, law (Vilnius: Vilnius University, 2011), p. 314, 316.
[24] E. Boros and J. Duns, Corporate Law. 3rd ed. (Oxford University Press 2013), p. 51.
[25] B. Hannigan, Company Law. (Oxford University Press 2012), p. 55.
[26] Panel of Judges of the Civil Division of the Supreme Court of Lithuania. 9 July 2009 ruling in the civil case Alveronas BUAB v. I. S., R. P., A. P., G. M., G. B. ir D. Č., No. 3K-3-329/2009, cat.: 27.7.

where the parent company is a shareholder of the subsidiary and said 3 conditions are true, the parent company can be liable for the obligations of the subsidiary.

On the other hand, as mentioned above, CK Article 2.50, Paragraph 3 applies only when the parent company is a shareholder of (directly owns) the subsidiary, but in practice the parent company often owns its subsidiaries indirectly (e.g. through another company of the group). In such a case, said article could not apply to the parent company. Therefore, it would be useful to supplement the wording of CK, Article 2.50, Paragraph 3 by indicating that Paragraph 3 of said article can also apply when the parent company is not a shareholder of the subsidiary but owns the subsidiary indirectly.

4. Technological challenges in the company group

Recently, a lot of attention is paid throughout the EU to various initiatives related to digitalisation in company law[27]. One of the most important analyses related to digitalisation in company law was carried out in 2016. Informal Company Law Expert Group[28] (ICLEG). In this ICLEG report, the initiatives (recommendations) are divided into two main parts. 1) digitalisation issues related to the activities of national business registries (that are engaged with company law)[29], online formation of a company, acceptability of electronic documents as evidence; 2) electronic communication between company and its shareholders and other stakeholders (for example, using electronic communications to provide information or exercise rights)[30]. It is clear that the initiatives (recommendations) focus more on the activities of individual companies instead of those of company groups. On the other hand, this does not prevent said initiatives from being applied to the companies that belong to company groups because, as already mentioned, in Lithuania as well as in other EU countries a company is considered an independent entity of civil legal relationship (in the context of company law). Furthermore, the ICLEG report also notes the specifics of digitalization in the context of company groups. For example, in Chapter 15 of Part 4 of the Report, 'A company's designated homepage', the authors present their opinion that not all companies should be required to have a homepage – one of such cases would be when a company belongs to a company group[31]. Such a proposition of the authors of the report is partly agreeable because the requirement to have a single homepage for the entire company group could be implemented more easily. On the other hand, the obligation to have a homepage irrespective of whether the company belongs to a company group or not would help to protect the interests of the investors. The investors' decision to invest in a company depends on various factors (company size, financial condition, business area, etc.), including being a part of a company group. Being a part of a company group can mean

[27] Another important study related to digitalisation of company law was made in 2017 by three experts in company law. However, it mainly focused on online registration of companies and filling company's information but did not analyzed the specifics of company groups. Study on digitalisation on company law [2017] accessed 11 April 2019. Accessible via the internet at: <https://ec.europa.eu/info/sites/info/files/dg_just_digitalisation_of_company_law_final_report.pdf>.

[28] ICLEG was established by the European Commission (EC) in May 2014 to assist it with expert advice on issues of company law and it held its first meeting on 26 June 2014. ICLEG, Report on digitalization in company law [2016] accessed 11 April 2019. Accessible via the internet at: <https://webcache.googleusercontent.com/search?q=cache:H5P_0ZwfJQAJ:https://ec.europa.eu/info/sites/info/files/icleg-report-on-digitalisation-24-march-2016_en.pdf+&cd=1&hl=lt&ct=clnk&gl=lt&client=firefox-b-ab>.

[29] Ibid., p. 15.

[30] Ibid., p. 23.

[31] Ibid., p. 27.

that the aim will be to seek the joint interests of the company group instead of the interests of a particular company in that group.

Furthermore, the report indicates that the obligation for a parent company to have a homepage with information on the entire company group including its members could be difficult to implement because the company group can comprise hundreds of companies. Therefore, according to the report, a more detailed analysis is needed regarding the establishment of this obligation for parent companies. However, in the opinion of the author of this work, it would not be useful to establish such an obligation. Firstly, this would make the company group's operations more difficult, especially when the company group comprises dozens or hundreds of companies. Secondly, the structure of company groups is not necessarily vertical, it can also be horizontal, in which case it would be difficult to determine which company of the company group should be obliged to have a homepage with the information on the company group's members.

Of course, the homepage requirement is obviously not the main issue of company group regulation. However, analysing this issue highlights the difficulties that will be faced in general when digitising the company group law. Firstly, a decision will have to be made whether the new obligations (e.g. the obligation for the parent company to have a homepage with the information on the entire company group) should be applicable only to the parent company or to each company of a company group. Secondly, the issue of sharing the responsibility – who would be liable for non-fulfilment of certain obligations? It is clear that, if a certain obligation is set upon the parent company, then it would be liable for non-fulfilment of said obligation. But what if the parent company failed to fulfil its obligation because its subsidiary failed to collaborate or provide necessary information – should the parent company still be liable? It is obvious that making the parent company liable for non-fulfilment of a certain obligation without taking into account whether the non-fulfilment was due to the subsidiary would make the operations of the entire company group more difficult.

On the other hand, it should be noted that quire a few innovations related to digitalisation in company law are selective. For example, the Law on Companies Article 21, Paragraph 4 states that a company may provide for a possibility for shareholders to attend the general meeting of shareholders and to vote by means of electronic communications; the Law on Companies Article 35, Paragraph 4 states that a member of the management may express his will, that is, "for" or "against" the decision put to vote upon familiarising himself with the draft thereof, by voting by means of electronic communications, finally there is opportunity to set up a private limited liability company (UAB) electronically. Clearly, the companies within a company group are also interested in applying such innovations because they facilitate the company group's operations and management. As mentioned above, the biggest challenge will be implementing the innovations whose purpose is not to facilitate the company group operations but to ensure the interests of the creditors and minority shareholders of these groups.

Conclusions

In Lithuania the subsidiary's management body members are not properly protected. Therefore, Lithuanian company law should establish the right for a parent company to give instructions to the management of its subsidiary, acknowledging the interests of a company group.

The wording of CK, Article 2.50, Paragraph 3 should be supplemented by indicating that Paragraph 3 of said article can also apply when the parent company is not a shareholder of the subsidiary but controls the subsidiary indirectly.

Innovations in company groups can be divided into two groups: 1) those that are designed to facilitate company group operations (selective); 2) those that are designed to improve the protection of creditors and minority shareholders (mandatory). Ensuring the innovations of the second group in company law will be the biggest challenge.

Bibliography

Legislation

1. Republic of Lithuania Law on Companies [2000], Valstybės žinios, 2000, nr. 64-1914.
2. The Civil Code of the Republic of Lithuania [2000]. Valstybės žinios, 2000, nr. 74-2262.

Books and articles

1. J. E. Antunes, Liability of Corporate Groups. Autonomy and Control in Parent-Subsidiary Relationships in US, German and EU Law. An International and Comparative Perspective (Denventer, The Netherlands: Kluwer Law and Taxation Publishers 1994).
2. BAKANAS, A., et al. Lietuvos Respublikos civilinio kodekso komentaras. Antroji knyga. (Vilnius: Justitia 2002).
3. E. Boros and J. Duns, Corporate Law. 3rd ed. (Oxford University Press 2013).
4. L. Mikalonienė. Uždarosios akcinės bendrovės akcininko teisės ir jų gynimo būdai (Vilnius: SE Centre of Registers 2015).
5. L. Mikalonienė, *Asmeninio komercinio bendradarbiavimo pagrindinės teisinės formos*: doctoral thesis. Social sciences, law. (Vilnius: Vilnius University, 2011).
6. P. Muller, *Creditor Protection in the Law of Corporate Groups – A Comparison between the U.K. and German Legal Approach*. (München: Akademischen Verlagsgemeinschaft München 2013).
7. B. Hannigan, *Company Law. (*Oxford University Press 2012).
8. V. Papijanc, Piercing the corporate veil institutas ir patronuojančios įmonės atsakomybė pagal dukterinės įmonės prievoles Lietuvos teisėje [2008], no. 10(112).
9. P. Lipton, The Mythology of Salomon's Case and the Law Dealing with the Tort Liabilities of Corporate Groups: An Historical Perspective [2014], accessed 11 April 2019. *Monash University Law Review*, 40(2). Accessible via the internet at: <http://www.austlii.edu.au/au/journals/MonashULawRw/2014/20.html>.

Cases

1. Panel of Judges of the Civil Division of the Supreme Court of Lithuania. *22 October 2008 ruling in the civil case Alaja ir ko UAB v. K. A. and V. A., No. 3K-3-509/2008, cat.: 27.1.*

2. Panel of Judges of the Civil Division of the Supreme Court of Lithuania. *12 September 2014 ruling in the civil case Mitnija UAB v. Statybų kryptis UAB, V. G., A. J., third party Nigema BUAB, No. 3K-3-389/2014, cat.: 27.7.*
3. Panel of Judges of the Civil Division of the Supreme Court of Lithuania. *11 December 2015 ruling in the civil case Creditum UAB v. G. Z., No. 3K-3-665-969/2015, cat.: 2.2.2.7.*
4. Panel of Judges of the Civil Division of the Supreme Court of Lithuania. *9 July 2009 ruling in the civil case Alveronas BUAB v. I. S., R. P., A. P., G. M., G. B. ir D. Č., No. 3K-3-329/2009, cat.: 27.7.*

Other sources

1. European Model Company Act (EMCA) [2017], accessed 10 April 2019. Accessible via the internet at: <http://law.au.dk/fileadmin/Jura/dokumenter/forskning/projekter/EMCA/2017-03-30_EMCA_withlinks.pdf >.
2. ICLEG, Report on digitalization in company law [2016] accessed 11 April 2019. Accessible via the internet at: <https://webcache.googleusercontent.com/search?q=cache:H5P_0ZwfJQAJ:https://ec.europa.eu/info/sites/info/files/icleg-report-on-digitalisation-24-march-2016_en.pdf+&cd=1&hl=lt&ct=clnk&gl=lt&client=firefox-b-ab>.
3. The Reflection Group on the Future of EU Company Law [2011] accessed 11 April 2019. Accessible via the internet at: http://ec.europa.eu/internal_market/company/docs/modern/reflectiongroup_report_en.pdf.
4. Study on digitalisation on company law [2017] accessed 11 April 2019. Accessible via the internet at: <https://ec.europa.eu/info/sites/info/files/dg_just_digitalisation_of_company_law_final_report.pdf>.

COLLABORATION BETWEEN FINTECH FIRMS AND BANKS: AN OPPORTUNITY OR A CHALLENGE FOR THE EU BANK RECOVERY AND RESOLUTION LEGAL FRAMEWORK KEY OBJECTIVE?

Laurynas Balčiūnas[1]

Abstract[2]

This article discusses the trend of collaboration between FinTech firms and banks, reactions of public authorities at the global and the EU levels, and potential opportunities and challenges such collaboration could bring to banks, supervisory and resolution authorities when applying and implementing the provisions of the bank recovery and resolution legal framework and aiming to ensure one of the key resolution objectives – the continuity of bank's critical functions essential to the real economy and financial stability.

Keywords: G20; financial law; FinTech; banking supervision, recovery, resolution; critical functions.

Introduction

"By enabling technologies and managing risks,

we can help create a new financial system for a new age…

under the same sun[3]*"*

Since 2009, many legal measures in the field of banking supervision and resolution were enacted both at the global and the EU levels. The new bank recovery and resolution legal framework (e.g. EU Bank Recovery and Resolution Directive; Single Resolution Mechanism Regulation; national implementing measures transposing the provisions of the Directive such as UK Banking Act etc.) is aiming to deal with the 'too big to fail' problem by introducing legal instruments which should help to reach a paradigm-changing objective – to resolve failing bank by ensuring the continuity of bank's critical functions which are essential to the real economy and financial stability[4]. The legal framework aims to reach this objective

[1] Researcher, PhD candidate, Faculty of Law, Vilnius University. Saïd Business School, University of Oxford. Research interests include financial markets regulation, in particular, banking prudential supervision, recovery, resolution, and relevant FinTech and Brexit issues. E-mail: Laurynas.Balciunas@oba.co.uk

[2] Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the official policy or position of any institution of the European Union.

[3] CARNEY, M. The Promise of FinTech – Something New Under the Sun? Speech by the Chair of the Financial Stability Board. Deutsche Bundesbank G20 conference on "Digitising finance, financial inclusion and financial literacy". Wiesbaden, 25 January 2017. P.14. [accessed on 15 September 2018] <http://www.fsb.org/wp-content/uploads/The-Promise-of-FinTech-–-Something-New-Under-the-Sun.pdf>

[4] See more on the legal concept of critical functions: BALČIŪNAS, L. The Legal Concept of Bank's Critical Functions, Implementation Challenges and the Role in the EU Bank Recovery and Resolution Framework. In Teisės viršenybės link. Vilnius University, Faculty of Law. Vilnius, 2019.

by requiring supervisory and resolution authorities, among other things, to ensure bank's resolvability through the preparation of recovery and resolution plans were critical functions and core business lines should be mapped, checking how non-critical services could be separated from critical etc.

In recent years we have seen unprecedented growth of investment to the financial technologies (FinTech). For example, FinTech firms around the world have raised a record $39.57 billions of investment from venture capital firms in 2018, an increase of 120% from 2017[5]. Collaboration between FinTech and incumbent banks has been increasing, and a new generation FinTech banks are evolving as well. This raises the questions what kind of opportunities and challenges such collaboration could bring to the application and implementation of the bank recovery and resolution legal framework provisions and ensuring one of the key '*after crisis*' bank recovery and resolution legal framework objectives – to ensure the continuity of failing bank critical functions which are essential to the real economy and financial stability.

The paper consists of three parts. The first part discusses trends and the drivers for collaborations between FinTech firms and banks. The second part provides an overview of reactions from regulators and public authorities at the global and the EU levels. The third part discusses specific opportunities and challenges which such collaboration could bring to the continuity of bank's critical functions, and aspects which should be considered by banks, supervisory and resolution authorities to adjust to changing reality when applying the legal provisions of the bank recovery and resolution legal framework. Finally, based on the performed analysis, the conclusions are provided.

1. Drivers for collaboration between FinTech firms and banks

Since 2000 investments in FinTech have grown dramatically (see figure 1), and it is expected that such a trend will remain strong with the continuous growth of investors' interest[6]. The customer-first approach that FinTech's have, continue to facilitate and advance financial inclusion, and are re-imagining products and propositions tailored to changing needs. So, will banks disappear? No, but they will be different.

[5] Banking Tech. 4 February 2019. [accessed on 4 February 2019] <https://www.bankingtech.com/2019/02/fintech-investment-in-2018-soars-to-record-40bn/>

[6]. The pulse of FinTech – Q4 2017. KPMG, 2018. [accessed on 10 February 2019] <https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2018/02/pulse_of_fintech_q4_2017.pdf>

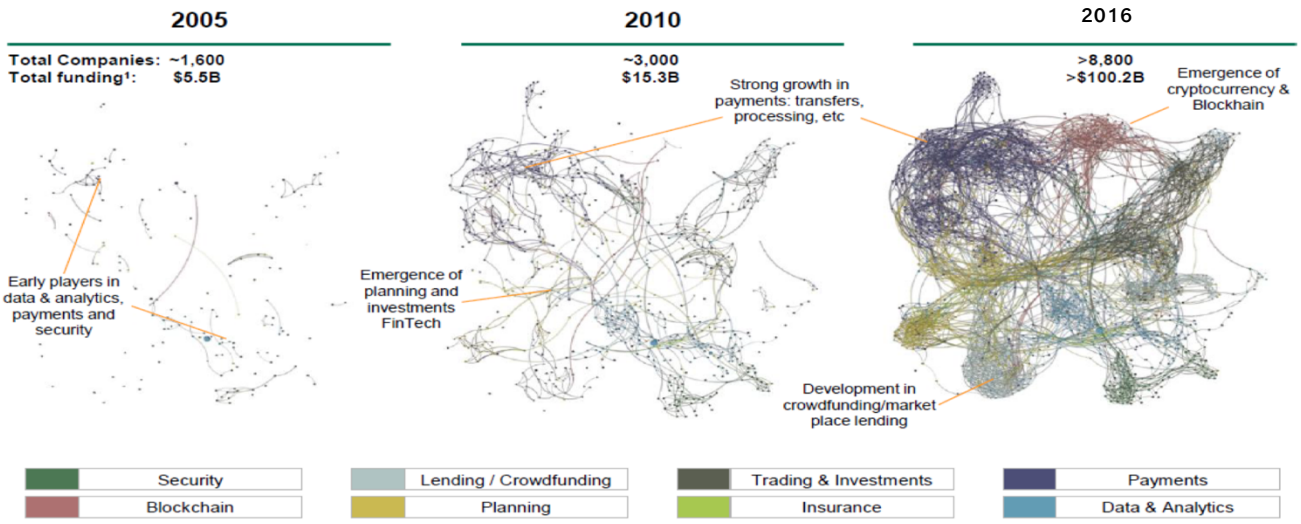


Figure 1. FinTech investment growth 2000 – 2016[7]

Customer habits and needs are changing as they get used to Google, Amazon, Apple and other user-friendly interfaces and are looking for something similar in banking. The adoption and use of internet-connected devices, computer and mobile-savvy millennials drives need for speed and convenience in financial services. However, banks' platforms are far from such experience as usually they are based on outdated, inflexible and legacy IT systems. FinTech firms aim to fill this gap. Data indicates that most investments in FinTech (usually developing products and solution based on technologies such as – data and analytics, cloud computing, artificial intelligence, and distributed ledger technology) are targeting namely retail banking[8].

According to certain empirical researches, around 75% of FinTech firms cite collaboration with incumbent banks as their primary business objective[9]. FinTech firms are aiming to collaborate with banks as this enhances their visibility by partnering with the well-know brand bank, allows to achieve economies of scale, gain customer trust, access to capital, expertise in regulations, expertise in risk management and other[10]. On the other hand, collaboration is also expected to be a priority for banks. It is increasingly expected that moving forward banks will become product and service 'aggregators', retaining the interface with clients, but combing their products and services with those of other market participants[11]. Banks are aiming to partner with FinTech firms[12] as this is reducing cost and

[7] IOSCO Research Report on Financial Technologies (FinTech). International Organisation of Securities Commission (IOSCO), February 2017. P. 5. [accessed on 10 February 2019] <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD554.pdf>

[8] As a matter of fact, McKinsey already in 2016 estimated that 52% of FinTech investments will focus on retail banking. Impact of FinTech on Retail Banking. McKinsey & Company, Brussels, 2016. Presentation slide 5. [accessed on 15 March 2018] <https://www.financialforum.be/sites/financialforum.be/files/media/1695-3-marc-niederkorn.pdf>

[9] For example, The World FinTech report 2018. P. 41. [accessed on 15 March 2018] <https://www.capgemini.com/wp-content/uploads/2018/02/world-fintech-report-wftr-2018.pdf>

[10] Ibid.

[11] Global Financial Markets Association and Pwc. Technology and Innovation in Global Capital Markets. Current trends in technology and innovation and their impact on the Investment Bank of the Future. March 2019. P. 5. [accessed on 10 March 2019]

inefficiencies, improving client servicing, increasing revenue, maintaining business completeness and agility, meeting regulatory and compliance obligations, enhancing controls and catching up with the speed of the market[13]. Banks are also embracing new technologies to accelerate the commoditization of cost drivers[14]. Finally, considering that such collaboration brings business benefits for both sides, we could expect even greater symbiosis between FinTech firms and banks in the future. Such a trend will be stimulated by existing (e.g. Monzo, Revolut, Starling etc.) and emerging[15] FinTech banks[16] as well.

However, such collaboration brings not only new business models and opportunities for FinTech firms and banks themselves, but also raises questions how such collaboration may impact the existing prudential supervision, in particular, bank recovery and resolution legal framework, it's one of the key objectives and financial stability in general, and what are the reactions of regulators and public authorities.

2. Reactions of public authorities at the global and EU levels

At the global level, the Financial Stability Board (FSB) has a mandate to promote international financial stability; therefore, has a role to play as FinTech continues to evolve. Already in 2016, the FSB has highlighted that for regulators, it is essential to understand what FinTech developments will change the way financial markets operate[17]. In

---

<https://www.afme.eu/globalassets/downloads/publications/afme-technology-and-innovation-in-global-capital-markets.pdf>

[12] The EBA identified as well that for banks the predominant way is partnership with new entrant FinTech firms and other firms that aim to actively follow and embrace FinTech developments. See: EBA Report on the Impact of FinTech on Incumbent Credit Institutions' Business Models. European Banking Authority, London, 3 July 2018. P. 25. [accessed on 3 July 2018] <https://eba.europa.eu/documents/10180/2270909/Report+on+the+impact+of+Fintech+on+incumbent+credit+institutions%27%20business+models.pdf>

[13] Global Financial Markets Association and Pwc. Technology and Innovation in Global Capital Markets. Current trends in technology and innovation and their impact on the Investment Bank of the Future. P. 7. [accessed on 10 March 2019] <https://www.afme.eu/globalassets/downloads/publications/afme-technology-and-innovation-in-global-capital-markets.pdf>

[14] European Central Bank. Guide to assessment of fintech credit institution licence applications. Frankfurt, March 2018. [accessed on 10 August 2019] <https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.201803_guide_assessment_fintech_credit_inst_licensing.en.pdf>

[15] For example, in the UK the Bank of England has been receiving interest from a range of FinTech firms seeking authorisation in the UK as a bank. 6 firms with business models focused on providing banking services to customers digitally have already been authorised as banks since 2015. A further 16 FinTech firms are at pre-application or live application stage, compared with 26 non-FinTech firms. See: What are the business models of new FinTech firms in the UK? Bank of England, London, 29 March 2019. [accessed on 29 March 2019] <https://www.bankofengland.co.uk/bank-overground/2019/what-are-the-business-models-of-new-fintech-firms-in-the-uk?sf100451385=1>

[16] FinTech bank is a business model in which the production and delivery of banking products and services are based on technology-enabled innovation. See: Guide to assessment of FinTech credit institution licence applications. European Central Bank, Frankfurt, March 2018. P. 3. [accessed on 10 August 2018] <https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.201803_guide_assessment_fintech_credit_inst_licensing.en.pdf>

[17] ANDERSEN, S. Chatham House Banking Revolution Conference Global Regulatory Developments and their Industry Impact. Financial Stability Board, Basel, 3 November 2016. P.3. [accessed on 12 February 2019] <http://www.fsb.org/wp-content/uploads/Chatham-House-The-Banking-Revolution-Conference.pdf>

2017, M. Carney, Chair of the FSB, stated that "[b]y enabling technologies and managing risks, we can help create a new financial system for a new age… under the same sun[18]". Thought, the Chair also highlighted that as risks form FinTech emerge, "authorities can be expected to pursue a more intense focus on the regulatory perimeter, more dynamic setting of prudential requirements, a broader commitment to resolution regimes <…>".[19] The same year the FSB also issued a more specific analysis focusing on financial stability implications from FinTech and highlighting supervisory and regulatory issues that merit authorities' attention[20]. In 2019, the FSB issued the report assessing FinTech market developments in the financial system and the potential implications for financial stability[21].

The Basel Committee also has performed some work linked to FinTech and bank supervision, not to mention that the Basel Committee's Core Principles[22] are relevant for assessing innovation in banking and the interaction between banks and FinTech firms. Furthermore, in 2018, the Basel Committee issued the document summarising its main findings and conclusions on sound practices and implications of FinTech developments for banks and bank supervisors[23].

At the European Union (EU) level, in 2017 the European Commission (EC) published the Consumer Financial Services Action Plan[24] including some actions aimed at supporting the development of an innovative digital world in retail financial services[25]. Subsequently, in 2017 the European Parliament adopted the Report on FinTech[26] which among other things also highlighted that the legislation, regulation and supervision have to adapt to innovation and strike the right balance between incentives to innovative consumer and investor

[18] CARNEY, M. The Promise of FinTech – Something New Under the Sun? Speech given by the Chair of the Financial Stability Board. Deutsche Bundesbank G20 conference on "Digitising finance, financial inclusion and financial literacy". Wiesbaden, 25 January 2017. P.1. [accessed on 15 September 2018] <http://www.fsb.org/wp-content/uploads/The-Promise-of-FinTech-–-Something-New-Under-the-Sun.pdf>

[19] Ibid., P.14.

[20] Financial Stability Implications from FinTech. Supervisory and Regulatory Issues that Merit Authorities' Attention. Financial Stability Board, Basel, 27 June 2017. [accessed on 28 June 2017] < http://www.fsb.org/wp-content/uploads/R270617.pdf>

[21] FinTech and Market Structure in Financial Services: Market Developments and Potential Financial Stability Implications. Financial Stability Board, Basel, 14 February 2019. [accessed on 14 February 2019] <http://www.fsb.org/wp-content/uploads/P140219.pdf>

[22] Core principles for effective banking supervision. Basel Committee on Banking Supervision, Basel, September 2012. [accessed on 2 October 2012] <https://www.bis.org/publ/bcbs230.pdf>

[23] Sound Practices. Implications of FinTech Developments for Banks and Bank Supervisors. Basel Committee on Banking Supervision, Bank for International Settlements, Basel, February 2018. [accessed on 1 March 2018] <https://www.bis.org/bcbs/publ/d431.pdf>

[24] Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions. Consumer Financial Action Plan: Better Products, More Choice. European Commission, Brussels, 2017. [accessed on 4 April 2017] <https://eur-lex.europa.eu/resource.html?uri=cellar:055353bd-0fba-11e7-8a35-01aa75ed71a1.0003.02/DOC_1&format=PDF>

[25] See Annex to Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions. Consumer Financial Action Plan: Better Products, More Choice. European Commission, Brussels, 2017. [accessed on 4 April 2017] <https://eur-lex.europa.eu/resource.html?uri=cellar:055353bd-0fba-11e7-8a35-01aa75ed71a1.0003.02/DOC_1&format=PDF>

[26] Report on FinTech: The Influence of Technology on the Future of the Financial Sector. Committee on Economic and Monetary Affairs, European Parliament, Brussels, 2017. [accessed on 2 May 2017] <http://www.europarl.europa.eu/doceo/document/A-8-2017-0176_EN.pdf>

protection and financial stability[27]. In 2017, the European Banking Authority (EBA) published a Discussion Paper[28] on its approach to FinTech[29]. This paper also raised questions concerning the impact of FinTech on the resolution of banks[30]. In 2018, as a follow-up to this paper, the EBA's FinTech roadmap was issued providing conclusions from the consultation on the EBA's approach to FinTech[31] which, among other things noted, that although resolution requirements are not typical for FinTech firms, there is a need to consider the interaction between FinTech firms and banks[32].

The Banking Union authorities, the European Central Bank (ECB) as a supervisory authority and the Single Resolution Board (SRB) as a resolution authority, are also progressively recognising the developments in the field of FinTech banking. In 2018, the ECB issued its guide to assessments of FinTech credit institution license applications[33]. The SRB noted that the transformation and digitalisation of financial services and the influence of FinTech firms on bank resolution would need to be considered and assessed in the Banking Union[34].

As it can be seen, both at the global and the EU levels FinTech topic is progressively getting more attention from regulators and public authorities. However, even though there is some attention and work done concerning potential opportunities and challenges to financial stability stemming from FinTech, there is no or minimal specific analysis on how collaboration between FinTech firms and banks could impact the application of legal provisions and the objectives of the bank recovery and resolution legal framework. In particular, what are opportunities and challenges from such collaboration for the implementation of relevant EU bank recovery and resolution statutory framework provisions and fulfilment of one of the key resolution objectives – the continuity of bank's critical functions which are essential to the real economy and financial stability.

---

[27] Report on FinTech: the Influence of Technology on the Future of the Financial Sector. Committee on Economic and Monetary Affairs, European Parliament, Brussels, 2017. P. 5. [accessed on 2 May 2017] <http://www.europarl.europa.eu/doceo/document/A-8-2017-0176_EN.pdf>

[28] Discussion Paper on the EBA's approach to financial technology (FinTech). European Banking Authority, London, 4 August 2017. [accessed on 4 August 2017] <https://eba.europa.eu/documents/10180/1919160/EBA+Discussion+Paper+on+Fintech+%28EBA-DP-2017-02%29.pdf>

[29] Considering the EBA's statutory objective, which, among other things, requires the EBA to promoting a sound, effective and consistent level of regulation and supervision, preventing regulatory arbitrage and promoting equal competition, contribute to enhancing consumer protection, and its duty to monitor new and existing financial activities. Articles 1(5) and 2(2) of Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC. OJ L 331, 15.12.2010.

[30] Discussion Paper on the EBA's approach to financial technology (FinTech). European Banking Authority, London, 4 August 2017. P. 54 [accessed on 4 August 2017] <https://eba.europa.eu/documents/10180/1919160/EBA+Discussion+Paper+on+Fintech+%28EBA-DP-2017-02%29.pdf>

[31] The EBA's FinTech Roadmap. Conclusions from the Consultation on the EBA's Approach to Financial Technology (FinTech). European Banking Authority, London, 15 March 2018. [accessed on 15 March 2018] <https://eba.europa.eu/documents/10180/1919160/EBA+FinTech+Roadmap.pdf>.

[32] The EBA's FinTech Roadmap. Conclusions from the Consultation on the EBA's Approach to Financial Technology (FinTech). European Banking Authority, London, 15 March 2018. P. 33.

[33] Guide to Assessments of FinTech Credit Institutions License Applications. European Central Bank, Frankfurt, March 2018. [accessed on 2 April 2018] <https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.201803_guide_assessment_fintech_credit_inst_licensing.en.pdf>

[34] SRB Multi-Annual Planning and Work Programme 2018. Single Resolution Board, Brussels, 2018. P. 14. [accessed on 12 September 2018] <https://srb.europa.eu/en/content/work-programme>

3. Opportunities and challenges for the EU bank recovery and resolution legal framework and it's one of the key objectives – continuity of bank's critical functions

There are three main conditions set in the EU Bank Recovery and Resolution Directive[35] (BRRD) which have to be met by the institution that resolution authority could take resolution actions, namely: i) determination that the institution is failing or likely to fail[36]; ii) there is no reasonable prospect that any alternative private sector measures or supervisory actions would prevent the failure of the institution[37]; iii) a resolution action is necessary in the public interest[38]. While the first two conditions are more 'traditional' and were usually assessed by supervisory authorities when considering whether to put the bank under the insolvency, the third condition – public interest test – is a more specific and has introduced a new angle for the resolution paradigm[39].

The BRRD specifies that a resolution action should be treated as in the public interest if it is necessary for the achievement of and is proportionate to one or more of the resolution objectives and winding up of the institution under ordinary insolvency proceedings would not meet those resolution objectives to the same extent[40]. The continuity of critical functions is one of the key resolution objectives[41], therefore, forms an integral part of the public interest test[42]. The BRRD defines 'critical functions' as "activities, services or operations the discontinuance of which is likely in one or more Member States, to lead to the disruption of services that are essential to the real economy or to disrupt financial stability due to the size, market share, external and internal interconnectedness, complexity or cross-border activities of an institution or group, with particular regard to the substitutability of those activities, services or operation"[43].

Furthermore, it's important to note that the legal concept of critical functions is not only crucial for the public interest test and the determination of whether resolution objectives

[35] Directive 2013/36/EU Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC Text with EEA relevance. OJ L 176, 27.6.2013, p. 338–436.
[36] See Article 32 (1)(a)(4) of the BRRD.
[37] Article 32(1)(a) of the BRRD.
[38] Article 32(1)(c) of the BRRD.
[39] See more: BALČIŪNAS, L. The Legal Concept of Bank's Critical Functions, Implementation Challenges and the Role in the EU Bank Recovery and Resolution Framework. In Teisės viršenybės link. Vilnius University, Faculty of Law. Vilnius, 2019
[40] Article 32(5) of the BRRD.
[41] Article 31(2)(a) of the BRRD. Other objectives: ii) to avoid a significant adverse effect on the financial system, in particular by preventing contagion, including to market infrastructures, and by maintaining market discipline; iii) to protect public funds by minimising reliance on extraordinary public financial support; iv) to protect depositors covered by Directive 2014/49/EU and investors covered by Directive 97/9/EC; and v) to protect client funds and client assets. Article 31(2)(b)(c)(d)(e) of the BRRD.
[42] See more: BALČIŪNAS, L. The Legal Concept of Bank's Critical Functions, Implementation Challenges and the Role in the EU Bank Recovery and Resolution Framework. In Teisės viršenybės link. Vilnius University, Faculty of Law. Vilnius, 2019.
[43] Article 2(1)(35) of the BRRD. See more about the legal concept of critical functions: BBALČIŪNAS, L. The Legal Concept of Bank's Critical Functions, Implementation Challenges and the Role in the EU Bank Recovery and Resolution Framework. In Teisės viršenybės link. Vilnius University, Faculty of Law. Vilnius, 2019.

were met. This concept, in general, plays a key role in the EU bank recovery and resolution legal framework. Namely, each step, whether it was recovery planning[44], resolution planning[45], identification of resolution objectives or application of resolution tools[46] and powers[47], relates to the legal concept of critical functions and therefore the provisions of the EU bank recovery and resolution legal framework should be applied keeping in mind this concept[48].

Increasing collaboration between FinTech firms and banks could provide direct as well as indirect opportunities and benefits linked to the EU bank recovery and resolution framework one of the key objectives – the continuity of bank's critical functions. For example, decentralisation and diversification across critical services and functions providers may dampen the effects of financial shocks in some circumstances as the failure of a single bank may be less likely to shut down a market as there would be other providers of critical services and critical functions.

Furthermore, technological solutions provided by FinTech firms may increase efficiency in bank's operations, improve bank's ability to manage risk and in this way support the stable business model of the bank which subsequently would contribute to overall efficiency gains in the financial system and the real economy. FinTech firms could also help to improve bank's ability to extract and aggregate specific information, as well as monitoring and reporting processes and systems what would, as a result, help to deal with the operational continuity issues. Smart management information systems could ensure that the resolution authorities are able to gather precise and complete information about the bank's core business lines, critical services, operations supporting critical functions what would facilitate to make informed and rapid decisions. Ability to instantly extract accurate information on financial contracts[49], or the assets (their place and eligibility as collateral) and liabilities of the bank could speed-up, for example, valuation exercise or decision to provide liquidity support.

However, such collaboration brings not only opportunities for the application and implementation of bank recovery and resolution framework legal norms and objectives, it also brings direct and indirect challenges. Increasing collaboration between FinTech firms and banks may result in an increased number of critical services[50] which will be provided by

[44] Title II, Chapter I, Section 2 of the BRRD.
[45] Title II, Chapter I, Section 3 of the BRRD.
[46] Title IV, Chapter IV of the BRRD.
[47] Title IV, Chapter VI of the BRRD.
[48] See more: BALČIŪNAS, L. The Legal Concept of Bank's Critical Functions, Implementation Challenges and the Role in the EU Bank Recovery and Resolution Framework. In Teisės viršenybės link. Vilnius University, Faculty of Law. Vilnius, 2019.
[49] Art. 2(1)(100), Art. 71(7)(8) of the BRRD.
[50] Critical services - the underlying operations, activities, services performed for one (dedicated services) or more business units or legal entities (shared services) within the group which are needed to provide one or more critical functions. BALČIŪNAS, L; et all. Technical advice on the delegated acts on critical functions and core business lines. European Banking Authority, London, 6 March 2015. P. 4. [accessed on 6 March 2015] <https://www.eba.europa.eu/documents/10180/983359/EBA-Op-2015-05+Technical+Advice+on+critical+functions+and+core+business++++.pdf>; Recital 8 of Commission Delegated Regulation (EU) 2016/778 of 2 February 2016, supplementing Directive 2014/59/EU of the European Parliament and of the Council with regard to the circumstances and conditions under which the payment of extraordinary ex post contributions may be partially or entirely deferred, and on the criteria for the determination of the activities, services and operations with regard to critical functions, and for the determination of the business lines and associated services with regard to core business lines. OJ L 131, 20.5.2016, P. 41-47. *For more details on the concept of critical services see: BALČIŪNAS*, L. The Legal Concept of Bank's Critical Functions, Implementation

FinTech firms to banks and which are needed to provide one or more critical functions which are essential to the real economy and financial stability. This brings to the question whether the resolution authorities will be able to use their resolution powers ((e.g. stay power) and tools effectively, as the role of third parties providing essential specialised services to banks will increase. On the other hand, banks reliance of third-party service providers raises questions whether they will be able to ensure business and operation continuity once faced with the difficulties as technological solutions (e.g. based on distributed ledger technology[51]) may not be in their control. This will require to continuously discuss and think how legal provisions set expectations for the way banks should engage third parties, to mitigate operational continuity issues which could be stemming from the increased interconnectedness and/or technological complexity of banks.

Furthermore, in order to avoid legal arbitrage and 'grey' zone, not only relevant bank recovery and resolution legal framework provisions aiming at ensuring operational continuity and continuity of bank's critical functions, but also more general bank supervision legal framework provisions, for example, dealing with the outsourcing risk management, will need to be considered in order to have a common and up to date approach on expectations how banks should engage third parties.

Moreover, increased digitalisation and technological solutions in the field of payments, FinTech banking, mobile banking solutions and instant access to the bank account, progressively allow clients to move funds across accounts easier and speedier. This could enable depositors to speed-up outflows of deposits from the bank which faces difficulties and could create additional complications for authorities to stabilise the financial situation of the bank or to determine when the bank meets resolution conditions[52] (e.g. is failing or likely to fail[53]).

Finally, such collaboration could increase overall complexity of bank's corporate structure what would as a result make it more complicated to resolve it or to segregate critical functions, core business lines, critical services from each other or the legal entity, what ultimately would complicate and/or make it impossible to achieve the continuity of those critical functions.

As it can be seen the collaboration between the FinTech firms and banks could bring not only opportunities but also challenges when implementing and applying the EU bank recovery and resolution legal framework and aiming to ensure one of its key objectives – the continuity of bank's critical functions which are essential for the real economy and financial stability. It is expected that such collaboration will continuously grow. Therefore, this aspect will require increased attention from banks, supervisory and resolution authorities in future. This will also require to carefully consider such relationship when applying legal norms linked to recovery planning, resolution planning and assessment of resolvability to ensure that the continuity of banks' critical functions and to avoid banks to become 'too technologically complex and interconnected' to be resolved.

Challenges and the Role in the EU Bank Recovery and Resolution Framework. In Teisės viršenybės link. Vilnius University, Faculty of Law. Vilnius, 2019.

[51] See more on the DLT: Technological Innovation. Distributed Ledger Technology: Challenges and Opportunities for Financial Market Infrastructures. European Central Bank, Frankfurt, 2016. [accessed on 7 May 2017] <https://www.ecb.europa.eu/pub/annual/special-features/2016/html/index.en.html>.

[52] Art. 32 of the BRRD.

[53] Art. 32(1)(a) of the BRRD.

Conclusions

1. In recent years, the speed and scale of investments to FinTech has increased rapidly. Collaboration between FinTech firms and banks is growing as both parties benefit from it. On the one hand, such collaboration brings new opportunities for customers and new business models for FinTech firms and banks themselves, on the other hand, it also impacts the application of existing bank prudential supervision, recovery and resolution legal framework and fulfilment of its objectives.

2. Both at the global and the EU levels FinTech topic is progressively getting more attention from regulators and public authorities. However, even though there is some attention and work done with regard to potential opportunities and challenges to supervision and financial stability stemming from FinTech, there is no or very limited specific analysis on how collaboration between FinTech firms and banks could impact the application of legal provisions and the objectives of the bank recovery and resolution legal framework.

3. The analysis shows that collaboration between FinTech firms and banks could create opportunities (e.g. improved data and risk management etc.) and challenges (e.g. bank's critical functions dependence on critical services supplied by FinTech firms etc.) in ensuring the continuity of bank's critical functions. Therefore, more attention from banks, supervisory (competent) and resolution authorities will be needed in order to balance those opportunities and challenges when applying and implementing the provisions of the EU bank recovery and resolution legal framework and ensuring that banks would not become 'too technologically interconnected and complex' to be resolved.

4. When preparing recovery plans, banks will need to consider their critical functions dependence from critical services supplied by FinTech firms, while supervisors, when reviewing those plans, will need progressively to draw more attention whether this aspect is adequately captured. When preparing the resolution plans, resolution authorities will need gradually to draw more attention to this aspect as well, as such collaboration could not only bring opportunities which could help to improve bank's resolvability, but also could bring challenges and potential impediments for bank's resolvability. Finally, if not adequately balanced, such collaboration may ultimately complicate the fulfilment of one of the key resolution objectives – the continuity of bank's critical functions which are essential to the real economy and financial stability.

Bibliography

1. ANDERSEN, S. Chatham House Banking Revolution Conference Global Regulatory Developments and their Industry Impact. Financial Stability Board, Basel, 3 November 2016. P.3. [accessed on 12 February 2019] <http://www.fsb.org/wp-content/uploads/Chatham-House-The-Banking-Revolution-Conference.pdf>

2. Annex to Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions. Consumer Financial Action Plan: Better Products, More Choice. European Commission, Brussels, 2017.

[accessed on 4 April 2017] <https://eur-lex.europa.eu/resource.html?uri=cellar:055353bd-0fba-11e7-8a35-01aa75ed71a1.0003.02/DOC_1&format=PDF>

3. BALČIŪNAS, L; et all. Technical advice on the delegated acts on critical functions and core business lines. European Banking Authority, London, 6 March 2015. [accessed on 6 March 2015]<https://www.eba.europa.eu/documents/10180/983359/EBA-Op-2015-05+Technical+Advice+on+critical+functions+and+core+business++++.pdf>

4. BALČIŪNAS, L. The Legal Concept of Bank's Critical Functions, Implementation Challenges and the Role in the EU Bank Recovery and Resolution Framework. In Teisės viršenybės link. Vilnius University, Faculty of Law. Vilnius, 2019.

5. CARNEY, M. The Promise of FinTech – Something New Under the Sun? Speech given by the Chair of the Financial Stability Board. Deutsche Bundesbank G20 conference on "Digitising finance, financial inclusion and financial literacy". Wiesbaden, 25 January 2017. [accessed on 15 September 2018] <http://www.fsb.org/wp-content/uploads/The-Promise-of-FinTech-–-Something-New-Under-the-Sun.pdf>

6. Commission Delegated Regulation (EU) 2016/778 of 2 February 2016, supplementing Directive 2014/59/EU of the European Parliament and of the Council with regard to the circumstances and conditions under which the payment of extraordinary *ex-post* contributions may be partially or entirely deferred, and on the criteria for the determination of the activities, services and operations with regard to critical functions, and for the determination of the business lines and associated services with regard to core business lines. *OJ L 131, 20.5.2016, p. 41–47.*

7. Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions. Consumer Financial Action Plan: Better Products, More Choice. European Commission, Brussels, 2017. [accessed on 4 April 2017] <https://eur-lex.europa.eu/resource.html?uri=cellar:055353bd-0fba-11e7-8a35-01aa75ed71a1.0003.02/DOC_1&format=PDF>

8. Considering the EBA's statutory objective, which, among other things, requires the EBA to promoting a sound, effective and consistent level of regulation and supervision, preventing regulatory arbitrage and promoting equal competition, contribute to enhancing consumer protection, and its duty to monitor new and existing financial activities. Articles 1(5) and 2(2) of Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC. OJ L 331, 15.12.2010.

9. Core principles for effective banking supervision. Basel Committee on Banking Supervision, Basel, September 2012. [accessed on 2 October 2012] <https://www.bis.org/publ/bcbs230.pdf>

10. Directive 2013/36/EU Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC Text with EEA relevance. OJ L 176, 27.6.2013, p. 338–436.

11. Discussion Paper on the EBA's approach to financial technology (FinTech). European Banking Authority, London, 4 August 2017. [accessed on 4

August 2017] <https://eba.europa.eu/documents/10180/1919160/EBA+Discussion+Paper+on+Fintech+%28EBA-DP-2017-02%29.pdf>

12. European Central Bank. Guide to assessment of fintech credit institution licence applications. Frankfurt, March 2018. [accessed on 10 August 2019] <https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.201803_guide_assessment_fintech_credit_inst_licensing.en.pdf>

13. Financial Stability Implications from FinTech. Supervisory and Regulatory Issues that Merit Authorities' Attention. Financial Stability Board, Basel, 27 June 2017. [accessed on 28 June 2017] <http://www.fsb.org/wp-content/uploads/R270617.pdf>

14. FinTech and Market Structure in Financial Services: Market Developments and Potential Financial Stability Implications. Financial Stability Board, Basel, 14 February 2019. [accessed on 14 February 2019] <http://www.fsb.org/wp-content/uploads/P140219.pdf>

15. FinTech investment in 2018 soars to record $ 40bn. In Banking Tech. 4 February 2019. [accessed on 4 February 2019] <https://www.bankingtech.com/2019/02/fintech-investment-in-2018-soars-to-record-40bn/>

16. Global Financial Markets Association and PwC. Technology and Innovation in Global Capital Markets. Current trends in technology and innovation and their impact on the Investment Bank of the Future. March 2019. [accessed on 10 March 2019] <https://www.afme.eu/globalassets/downloads/publications/afme-technology-and-innovation-in-global-capital-markets.pdf>

17. Global Financial Markets Association and PwC. Technology and Innovation in Global Capital Markets. Current trends in technology and innovation and their impact on the Investment Bank of the Future. [accessed on 10 March 2019] <https://www.afme.eu/globalassets/downloads/publications/afme-technology-and-innovation-in-global-capital-markets.pdf>

18. Guide to assessment of fintech credit institution licence applications. European Central Bank, Frankfurt, March 2018. [accessed on 10 August 2018] <https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.201803_guide_assessment_fintech_credit_inst_licensing.en.pdf>

19. Guide to Assessments of FinTech Credit Institutions License Applications. European Central Bank, Frankfurt, March 2018. [accessed on 2 April 2018]<https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.201803_guide_assessment_fintech_credit_inst_licensing.en.pdf>

20. Impact of FinTech on Retail Banking. McKinsey & Company, Brussels, 2016. [accessed on 15 March 2018] <https://www.financialforum.be/sites/financialforum.be/files/media/1695-3-marc-niederkorn.pdf>

21. IOSCO Research Report on Financial Technologies (FinTech). International Organisation of Securities Commission (IOSCO), February 2017. P. 5. [accessed on 10 February 2019] https://www.iosco.org/library/pubdocs/pdf/IOSCOPD554.pdf

22. Report on FinTech: The Influence of Technology on the Future of the Financial Sector. Committee on Economic and Monetary Affairs, European Parliament, Brussels, 2017. [accessed on 2 May 2017] <http://www.europarl.europa.eu/doceo/document/A-8-2017-0176_EN.pdf>

23. Report on FinTech: the Influence of Technology on the Future of the Financial Sector. Committee on Economic and Monetary Affairs, European Parliament, Brussels, 2017. P. 5. [accessed on 2 May 2017] <http://www.europarl.europa.eu/doceo/document/A-8-2017-0176_EN.pdf>

24. Sound Practices. Implications of FinTech Developments for Banks and Bank Supervisors. Basel Committee on Banking Supervision, Bank for International Settlements, Basel, February 2018. [accessed on 1 March 2018] <https://www.bis.org/bcbs/publ/d431.pdf>

25. SRB Multi-Annual Planning and Work Programme 2018. Single Resolution Board, Brussels, 2018. P. 14. [accessed on 12 September 2018] <https://srb.europa.eu/en/content/work-programme>

26. Technological Innovation. Distributed Ledger Technology: Challenges and Opportunities for Financial Market Infrastructures. European Central Bank, Frankfurt, 2016. [accessed on 7 May 2017] <https://www.ecb.europa.eu/pub/annual/special-features/2016/html/index.en.html>

27. EBA Report on the Impact of FinTech on Incumbent Credit Institutions' Business Models. European Banking Authority, London, 3 July 2018. [accessed on 3 July 2018] <https://eba.europa.eu/documents/10180/2270909/Report+on+the+impact+of+Fintech+on+incumbent+credit+institutions%27%20business+models.pdf>

28. The EBA's FinTech Roadmap. Conclusions from the Consultation on the EBA's Approach to Financial Technology (FinTech). European Banking Authority, London, 15 March 2018. [accessed on 15 March 2018] <https://eba.europa.eu/documents/10180/1919160/EBA+FinTech+Roadmap.pdf>.

29. The EBA's FinTech Roadmap. Conclusions from the Consultation on the EBA's Approach to Financial Technology (FinTech). European Banking Authority, London, 15 March 2018. P. 33.

30. The pulse of FinTech – Q4 2017. KPMG, 2018. [accessed on 10 February 2019] <https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2018/02/pulse_of_fintech_q4_2017.pdf>

31. The World FinTech report 2018. [accessed on 15 March 2018] <https://www.capgemini.com/wp-content/uploads/2018/02/world-fintech-report-wftr-2018.pdf>

32. What are the business models of new FinTech firms in the UK? Bank of England, London, 29 March 2019. [accessed on 29 March 2019] <https://www.bankofengland.co.uk/bank-overground/2019/what-are-the-business-models-of-new-fintech-firms-in-the-uk?sf100451385=1>

COMPARATIVE PERSPECTIVES ON DATA PROTECTION: INFORMATION SHARING IN LAW ENFORCEMENT

Kelly Blount[1]

Abstract

This paper will examine the ability of a multi-level enforcement system to maintain the goals of data protection in the face of increasingly shared personal data. The paper will examine this issue in the law enforcement context using a comparative analysis between two multi-level enforcement systems; the European Union (EU) and the United States (US).

In 2018, the EU implemented the General Data Protection Regulation (GDPR) to protect the right of individuals to maintain the privacy of personal data, and a Directive intended to protect personal data in the realm of public safety and police matters. Around the same time the Commission agreed on a Framework Decision that advances the interoperability of data for use by law enforcement. Correctly striking a balance between security and privacy is an important and difficult feat, however in the case of a multi-level enforcement system, there are additional layers of complexity. As another form of multi-level enforcement system, the US offers a unique comparison for two reasons. The first reason is the nuanced, yet significant, difference in how data protection and privacy are legally constructed in the US. The second reason this is a meaningful comparison is the difference between multi-level enforcement in the EU and in the US. These multi-level systems each provide separate results in the cases of both vertical and horizontal information sharing.

The paper will begin by comparing notions of data protection in the EU and the US, and discussing the way in which these seemingly subtle differences have large effects on individual rights. It will then illustrate how interoperability is applied in practice and the differing results on data protection in each respective system. In conclusion the paper will posit that based on the comparisons made, the obstacles confronting a seamless combination of interoperability and data protection come less from the multi-level enforcement system, but more from the way in which each system functions according to its notions of data protection.

Keywords: data protection, privacy, information sharing, law enforcement, transatlantic perspectives

Introduction

[1] Kelly Blount is a Doctoral Researcher at the University of Luxembourg, as a member of the Doctoral Training Unit on Multi-Level Enforcement, supported by Luxembourg National Research Fund (FNR) – 10965388. Her dissertation focuses on the use of personal data in criminal investigations. Kelly is an American licensed attorney and has a Master's Degree in Middle East Studies.

Through a comparative analysis, this paper will examine the ability of a multi-level enforcement system to maintain the goals of data protection in an interoperable world. First the paper will introduce the issue at hand; namely, the legal constructs of data protection and privacy from both the EU and US perspectives. In so doing it will compare and contrast the EU standards for privacy and data protection (Articles 7 and 8 of the EU Charter of Fundamental Rights) with the US understanding of privacy (Amendment Four to the Constitution). Second, it will examine the interoperability of databases as currently used in either system and the likely usage of proposed systems. In the example of both the EU and the US, this section will provide hypothetical scenarios that illustrate the application and consequences of interoperability in practice, both vertically and horizontally. Finally the paper will conclude that the general right to data protection affords individuals different rights based on the legal formation of privacy, rather than differing forms in the enforcement system.

1. Transatlantic perspectives on privacy and data protection

Both the EU and the US have experienced a push toward making information more available to law enforcement and security agencies in the post-9/11 world. The enormous amount of data that is collected through myriad policing methods provides great advantage to law enforcement and carries with it great responsibility. The 1948 Universal Declaration of Human Rights declares privacy to be a human right.[2] However the approaches taken on either side of the Atlantic vary when it comes to defining the right. In practice, the distinction invokes divergent results in the reoccurring tension between security and human rights. In the EU, personal data was initially conceived of as information related to the private life, which after a short use should be forgotten, and the facts of life which it reflected will again be private.[3] In the US, generally once that information is obtained by a third party it ceases to be private henceforth. This section will continue on to describe the different approaches to data protection which will serve as the basis for later discussion on how this applies in practice.

In the EU privacy is a fundamental right, separate and apart from the fundamental right to the protection of one's personal data. These rights are set forth in the EU Charter of Fundamental Rights, Articles 7 and 8, respectively. Article 8 describes the right to "the protection of personal data concerning him or her."[4] In 1995 the EU passed its first data protection legislation, the Data Protection Directive (DPD), which was worded specifically to ensure the rights of individuals' privacy in regard to the processing of personal data.[5] The Directive states that persons have "the right to privacy *with respect to* the processing of personal data."[6] [Emphasis added] The purposeful wording of the Directive seems to make clear the distinction between privacy and data protection. The Directive stated that personal

[2] United National General Assembly resolution 217 A. Declaration of Human Rights. 10 December 1948, Paris. This paper adopts the general extension of correspondence to include digital correspondence of various formats.
[3] Gonzalez Fuster, Gloria. The Emergence of Personal Data Protection as a Fundamental Right of the EU. Pg 97.
[4] EU Charter of Fundamental Rights. Article 8(1). Official Journal of the European Union C 303/17 - 14.12.2007.
[5] Gonzalez Fuster, at 128-129.
[6] Directive 95/46/EC of the European Parliament and of the Council. "on the protection of individuals with regard to the processing of personal data and on the free movement of such data**."** October 24, 1995.

data be collected for "specified, explicit and legitimate purposes and not be further processed in a manner that is incompatible with these purposes."[7] The Directive was intended to harmonize the state rules on data protection while ensuring the free flowing movement of information, building on the European Convention on Human Rights and the even earlier OECD Guidelines.[8] When the DPD was repealed and replaced in May, 2018 it made directly applicable on the Member States a mélange of pre-existing and new rules. Article 5 (1)(b) of the GDPR as well as Article 4(1)(b) of the Law Enforcement Directive maintain the principles of 'specified, explicit and legitimate' as a requirement for proper data protection.[9] This clause embodies the principle of purpose limitation, which prohibits ongoing processing of personal data. It also honors a general principle of the GDPR, that a person should have some choice and control over "how information about them is used."[10] Generally the initial reason for collecting the data remains the only valid reason (outside stated public interest needs) for retaining or using the data for future purposes.[11] Even processing based on legal, proportionate grounds will not comply with purpose limitation if beyond the scope of the initial purpose.[12] Therefore the data retains its intrinsic value, which is its relation to private life, and the interference to privacy is finite. As will be discussed in the following section, a push toward interoperable databases for law enforcement may not be compatible with this principle.

Unlike in the EU, American jurisprudence approaches the protection of personal data as a constituent part of the right to privacy. The Fourth Amendment to the US Constitution ensures "The right of the people to be secure in their persons, houses, papers, and effects…" and is generally extended to include data.[13] In the 1970's the issue of privacy began to gain attention with the advent of computers.[14] Privacy in the US was already considered to include the right of individuals "to determine for themselves when, how and to what extent information about them is communicated to others."[15] Unlike in the EU where data protection is separate from notions of privacy, US data protection falls under privacy law, and is based on a reasonable expectation test. However this right is protected mainly by the courts, rather than legislation. In a landmark 1967 judgement by the Supreme Court, Justice Harlan wrote that the expectation of privacy must be one that "society is prepared to recognize as 'reasonable.' Thus, a person has a legitimate expectation privacy if…a reasonable person in the same or similar circumstances would believe [it] … to be private as well."[16] Therefore, once an individual's information is available to a third party entity, the individual may no longer reasonably expect that data is private unto them. And so the strongest tenant of purpose limitation, that future uses of data beyond the initial purpose are illegitimate, is precluded from the notion of US privacy. Similarly to the EU concept of primacy in which competencies left to the member states remain as such, US states are left to craft individual legislation where the federal government has not. In the case of data

[7] Forgo, Nikolaus, Stefanie Hanold and Benjamin Schutze. "The Principle of Purpose Limitation and Big Data." New Technologies, Big Data and the Law. 2017, Spring. Referring to Recital 8 Directive 95/46/EC Article 6(1)(b).
[8] Tzanou, Maria. "Is Data Protection the Same as Privacy? An Analysis of Telecommunications' Metadata Retention Measures." Journal of Internet Law. September 2013. Pg. 25.
[9] General Data Protection Regulation. Regulation (EU) 2016/679. Article 5(1)(b). Official Journal of the European Union Law Enforcement Directive. Article 4(1)(b). Official Journal of the European Union L 119/108 – 4.5.2016.
[10] The Economist, "The power of privacy." March 23, 2019.
[11] Article 29 Data Protection Working Party (2013) Opinion 03/2013. 3.
[12] Forgo et. al,
[13] United States Constitution. Amendment IV.
[14] Packard, Vince. The Naked Society. 1964.
[15] Id.
[16] Katz v. United States, 389 U.S. 347 (1967).

protection in law enforcement, there is no generally sweeping federal regulation. Therefore the protection of personal data varies widely between states. However despite this, interoperability of personal data between federal and state entities flows in both directions and is available to law enforcement at all levels, the subject of the following section.

2. Interoperability in practice

A general, and widely accepted definition of interoperability defines it as "allow[ing] applications executing on separate hardware platforms, or in multi-processing environments … to share data and cooperate in processing it…"[17] Interoperability in a multi-level system begs questions of both horizontal and vertical data sharing. In the EU and especially within the Area of Freedom, Security and Justice, there are Union level institutions and agencies which play an important role apart from, but in coordination with, national governments. In the US, federal law enforcement agencies umbrella over state agencies. This section will attempt to illustrate how the different conceptions of data protection discussed above result in varying applications of interoperability. Law enforcement's use of personal data will provide the framework for the case studies.

On March 23, 2017, the European Commission passed the European Interoperability Framework, which includes 47 recommendations on interoperability. These recommendations suggested the creation of a single search portal that will allow multiple agencies to access the data of numerous EU security and migration databases at once.[18] The information in these databases are submitted via state authorities, law enforcement agencies and border control agents, each acting in their separate capacities of authority. The information includes biometric, familial and migration information, amongst others.[19] Therefore the question now being raised by scholars and practitioners is whether the principle of purpose limitation must minimize the Commission's plans to make this type of data sharing possible.[20] In an example to illustrate vertical information sharing, a citizen of State A applies to obtain a visa to the EU and is registered into the Visa Information System (VIS), and her information is stored in that database.[21] The current system requires that to access that data, law enforcement must act through the proper channels of police cooperation as set out in the Treaty of Lisbon and EU secondary law.[22] Under the VIS in particular, law enforcement must show a clear necessity for the information.[23] Under the proposed changes, that information would now be searchable all through one platform.[24] If that initial data was collected based on her application for a visa into the EU, i.e. collected

[17] Bureau of Public Safety and Homeland Security, Federal Communications Commission. "Interoperability." Factsheet. <https://www.fcc.gov/general/interoperability>.
[18] European Commission. "New European Interoperability Framework, Promoting seamless services and data flows for European public administrations." 2017.
[19] Id.
[20] See Quintel, Teresa. "Connecting personal data of Third Country Nationals, Interoperability of EU databases in the light of the CJEU's case law on data retention." Law Working Paper Series, Paper number 2018-002. University of Luxembourg Faculty of Law, Economics and Finance. 2018.
[21] Peers, Steve. EU Justice and Home Affairs Law. Oxford EU Library. 4th Edition, Volume II. 2016. Pg. 303.
[22] Treaty on the European Union and on the Functioning of the European Union [2007] 2012/C 326/01.
[23] Id. at 307.
[24] The process for acquiring the information implicated in a "hit/no hit" search varies depending on the database. Law enforcement will not have the automatic right to access content data immediately in all situations.

for immigration purposes by border agents, is it lawful for police in State B to access that information in the course of a criminal investigation? Though the new search portal is intended to allow access rights only as they are currently distributed, the mere ability to flag the existence of a record raises questions of purpose limitation.[25]

Supposing the same scenario in the US, we likely come to a different conclusion. In the reverse vertical data sharing scenario, we might imagine that an agent of the Federal Bureau of Investigations (FBI) wishes to investigate a crime in part by searching the federal immigration database, which includes various biometric data such as fingerprint records. After retrieving the suspect's fingerprint record, the agent may gain access to a local Fusion Center to cross-check the many databases for a match. The Fusion Center is a creation of the post-9/11 government which sought to make information sharing between federal and local authorities more accessible. As a result many states and large cities are home to a center which houses millions of public records, police records, CCTV screens and sophisticated police hardware.[26] These centers allow law enforcement authorities at local and federal levels to share criminal and non-criminal records, while simultaneously adding new data. In addition to a level of interoperability that exceeds any conception of purpose limitation, the center can also scan for new data. One of the ways this is done, is through automated license plate readers, which record all license plates passing a particular camera. This record contributes to any single individual's footprint in the database.[27] Because all the data is presumably collected with the tacit knowledge of the subject, privacy has been forfeited and there is no longer an expectation this data is private. For instance, in our example the suspect willingly gave a fingerprint record at the border to gain admission, and the license plate registration matches his identity with his car, and the pattern of his car, as evidenced by his license plate, driving on public roads lead to his employer, giving the agent his location. None of these facts would be considered private under the given circumstances.

The difference in outcome for these two scenarios hinges on several factors. The first and most obvious factor, is the difference in what is a legal use of personal data and what is not. In the EU example, purpose limitation restricts access to personal data without a legitimate security need that justifies the interference to privacy. In the US case, purpose limitation is precluded by the expectation of privacy test, which is used to determine when personal data is private. As stated early in this paper, the EU citizen controls her data as relevant to her personal life and therefore her privacy, whereas the US citizen's personal data once willingly shared, is no longer private.[28] When the border agent collects the EU resident's biometric traits to ensure her identity when granting her a visa, that personal data about her is intended only for immigration purposes. In the example of the US resident, her right to privacy is predicated upon a reasonable expectation that the data in question remains private. Because she drives her car around in public, she cannot reasonably expect her movements to be private. Similarly, she cannot expect that the biometric data she freely gave to immigration authorities will be private, therefore she cannot expect it will not be used

[25] Council of the EU. "Interoperability between EU information systems: Council Presidency and European Parliament reach provisional agreement." Press Release 67/19, February 5, 2019.
[26] Department of Homeland Security. "National Fusion Center Factsheet." <https://www.dhs.gov/national-network-fusion-centers-fact-sheet>.
[27] Ozer, Murat. "Automatic license plate reader (ALPR) technology: Is ALPR a smart choice in policing?" The Police Journal: Theory, Practice and Principles." 2016, Vol. 89(2) 117-132. pp 120.
[28] Gonzalez Fuster at 255.

for a secondary purpose. Not discussed in this paper, is the boundary at which surveillance and the accumulation of a consistent flow of data is treated in the realm of privacy.[29]

3. Horizontal sharing in the multi-level regime

Finally, this section will briefly unpack the analysis borne of this comparison. The previous section laid out two examples in which personal data may be shared by law enforcement within a vertical framework of interoperable databases. In the EU scenario, it can be foreseen that purpose limitation may be itself limited if and when EU level databases become more widely interoperable. However in the US system, the conception of privacy is such that this type of interoperability is often legally unremarkable, as data falls under a more general concept of privacy.

This leads to the final piece of the puzzle, the potentially divergent effects of horizontal data sharing. In looking at the EU example, we find that the manner of collecting data for law enforcement purposes is not entirely consistent across states. For instance, one could imagine that Country A has a very strict process for the securement of a warrant to collect cellular metadata. It is updating EU-wide databases with data it collects according to national law. The same EU databases are also being fed data from Country B, which has the minimal safeguards necessary under the Law Enforcement Directive. Once these data are in the system, they are theoretically accessible to law enforcement across the EU. Therefore, even if purpose limitation is honored by restrictions to access by law enforcement, the fundamental rights granted to an individual by his state will not necessarily be honored. In this example, if State A acquires evidence from an interoperable database and prosecutes the citizen based on cellular metadata which was collected in State B (under the less arduous warrant process), his rights in State A, where that data would have been protected, are not being honored. The example is hypothetical and does not take into account rules of evidence or criminal procedure, however it is meant to illustrate potential misalignment of data protection laws between states.

Conversely, the US example is a little less speculative, though it arguably shows there is less protection to persons against the sharing of personal data. As previously mentioned, the US does not have a uniform standard for data protection in most fields. Often policing methods are judged by the courts using the expectation of privacy test on a case by case basis.[30] As a result, numerous advances in technology are being used both openly and discreetly by police units. Some of these technologies, such as the cellular interception devices titled “Stingrays,” are considered by many to be incredibly intrusive, however their use varies across jurisdictions and many states have not even attempted to regulate or pass judgment on their use.[31] Therefore when a resident of State C, which may have a law against the use of a Stingray, has his cellular information intercepted by police in State D where it is legal, that data will still ostensibly become part of an interoperable database accessible to police in State C. Again, though criminal procedure in US states will be forced to deal with many of these questions, the horizontal analysis in both the EU and US perspectives is more complicated.

This section briefly described the way in which the sharing of data in a horizontal direction differs between the EU and the US, based again on the different approaches to

[29] Brayne, Sarah. “Big Data Surveillance: The Case of Policing.” American Sociological Review 2017, Vol. 82(5) 977-1008. pp. 992.
[30] Takhar, Phillip. “D.C. Court of Appeals Rules that Cell-Site Simulators Constitute a Search.” October 2, 2017. Harvard Journal of Law & Technology.
[31] Id.

data protection. However unlike in the vertical sharing examples which appear more straightforward, both systems run into trouble when faced with interoperability between states with differing levels of protection for personal data. This difference in privacy versus data protection, overlaid with interoperability plays out differently across and through multi-level enforcement systems, and will be important to bear in mind as data protection policy evolves with technology.

Conclusion

The past two decades have seen great change in the sharing of information by law enforcement. The above discussion gave a brief overview of the conception of data protection in the EU, and the idea of privacy in the US context. The US has been slow to adopt federal regulation, however the enveloping of personal data protection under the principle of privacy more generally, has made the horizontal nature of law enforcement tenable. In the EU the Law Enforcement Directive leaves huge swathes of details to be determined by Member States in the implementation phase. The discussion then illustrated how these notions of privacy play out in real life when law enforcement seeks the use of personal data for an ongoing investigation. Using examples for both the vertical and horizontal flows of data, it is clear that in a multi-level systems the difference between privacy and data protection in both the EU and US dramatically change the rights of individuals in the law enforcement context. These issues will continue to evolve and be monitored.

Bibliography

1. A. Westin, 'Privacy and Freedom' (New York: 1970)
2. Article 29 Data Protection Working Party [2013] Opinion 03/2013
3. Bureau of Public Safety and Homeland Security, Federal Communications Commission, 'Interoperability' [last accessed 2019] Factsheet
4. Council of the EU, 'Interoperability between EU information systems: Council Presidency and European Parliament reach provisional agreement' [2019] Press Release 67/19
5. Department of Homeland Security, 'National Fusion Center Factsheet' [last accessed 2019]
6. Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995]
7. EU Charter of Fundamental Rights. Article 8(1). Official Journal of the European Union [2007] C 303/17
8. European Commission. "New European Interoperability Framework, Promoting seamless services and data flows for European public administrations." 2017
9. G. Gonzalez Fuster, 'The Emergence of Personal Data Protection as a Fundamental Right of the EU' (Switzerland: 2014)
10. Katz v. United States, 389 U.S. 347 (1967)

11. M. Ozer, ‘Automatic license plate reader (ALPR) technology: Is ALPR a smart choice in policing?’ [2016] The Police Journal: Theory, Practice and Principles Vol. 89(2)
12. M. Tzanou, ‘Is Data Protection the Same as Privacy? An Analysis of Telecommunications’ Metadata Retention Measures’ [2013] Journal of Internet Law
13. N. Forgo, S. Hanold and B. Schutze, ‘The Principle of Purpose Limitation and Big Data’ [2017] New Technologies, Big Data and the Law
14. P. Takhar, ‘D.C. Court of Appeals Rules that Cell-Site Simulators Constitute a Search’ [2017] Harvard Journal of Law & Technology
15. Regulation (EU) 2016/679 General Data Protection Regulation [2016]
16. S. Peers, ‘EU Justice and Home Affairs Law’ (Oxford EU Library: 2016)
17. S. Brayne, ‘Big Data Surveillance: The Case of Policing’ [2017] American Sociological Review Vol. 82(5)
18. T. Quintel, ‘Connecting personal data of Third Country Nationals, Interoperability of EU databases in the light of the CJEU’s case law on data retention’ [2018] Law Working Paper Series, Paper University of Luxembourg Faculty of Law, Economics and Finance
19. The Economist, ‘The power of privacy’ [2019]
20. Treaty on the European Union and on the Functioning of the European Union [2007] 2012/C 326/01
21. United National General Assembly resolution 217A Declaration of Human Rights [1948]
22. United States Constitution [1788]
23. V. Packard, ‘The Naked Society’ (Canada: 1964)

IMPACT OF TAX TECHNOLOGIES ON CURRENT AND FUTURE TAX COMPLIANCE

Indra Burneikaitė[1]

Abstract

This article analyses the current tax technologies used by tax authorities, taxpayers and tax advisors. Certain success stories and ambitious endeavours for the future are mentioned as well. All these examples show the multilevel impact tax technologies can have in respect of tax compliance. The main concern is that in certain cases measures are taken too far and can easily lead to enhanced battles between taxpayers and tax authorities each side armed with advanced tax technologies in the future. In order to avoid such perspective, tax authorities should consider the OECD suggestion to establish enhanced relationship with taxpayers so that their inner motivation and respective usage of tax technologies would be oriented towards greater tax compliance rather than smarter tax avoidance.

Keywords: tax technologies, tax administration, enhanced relationship.

Introduction

As the OECD acknowledges, taxpayers pay very little interest in taxes and activities of tax authorities, and have an expectation that payment of taxes should be as easy as online shopping. In even more advanced form, taxpayers expect that in the future tax authorities should be able to deduct precise tax amounts out of taxpayers' accounts without any filling. Taxpayers also want to view processed data stored by tax authorities in real time or near real time, analyse it and report inconsistences, if any. Instant feedback is what taxpayers expect from tax authorities nowadays. Speaking about digitally mature taxpayers, their expectations take even more advanced level where taxpayers expect to be serviced rather than just informed. This means that tax authorities should use tax technologies to make adjusted calculations and provide a ready-made comparison for consideration of taxpayers instead of sending a standard letter listing inconsistencies identified, and asking taxpayers to process, analyse and fix them.[2]

All these tendencies bring new challenges to tax authorities doing their best to keep up with changes of business processes highly influenced by disruptive technologies. A constant goal to balance between quality and reasonable spending has now evolved to a whole new level. Nowadays, not only businesses, but also tax authorities use technologies to differentiate taxpayers and respectively allocate further human and technological resources. Personalized approach defines directions in which tax authorities use technologies. And the

[1] PhD candidate at Vilnius University, Faculty of Law, with research interests that include international tax law, tax administration, tax law history, tax law theory, tax technologies.
[2] OECD, 'Technologies for Better Tax Administration. A Practical Guide for Revenue Bodies' (Paris: OECD Publishing 2016) 26-27.

use of technologies should lead tax authorities towards more accurate audits, new or improved services and, respectively, more trust from taxpayers.

1. Tax Technologies and Tax Authorities

Seeking for the mentioned goals, tax authorities are going digital across all over the world. Process of digitalization has already reached five levels each having a different level of data gathering and use of technologies.

Tax authorities operating on the 1st level (e-filling) use payroll, financial and other standard data gathered electronically from received tax returns and periodically match this data looking for inconsistencies, if any *(in this level operate the Netherlands, Sweden, Switzerland and Ukraine)*.

Tax authorities operating on the 2nd level (e-accounting) use accounting, trial balances and other additional data gathered electronically from received standard reporting files *(in this level operate Austria, Belgium, Finland, Germany, Greece, Italy, Lithuania, Luxembourg, Norway, and the United Kingdom)*.

Tax authorities operating on the 3rd level (e-matching) use even more advanced data such as bank statements in order to match data across different tax types, taxpayers and jurisdictions in real time or near real time *(in this level operate the Czech Republic, Denmark, France, Hungary, Ireland, India, Poland, Portugal, Slovakia and Turkey)*.

Tax authorities operating on the 4th level (e-auditing) cross-check received tax fillings in real time or near real time to map the geographic economic ecosystem, in this level taxpayers receive from tax authorities electronic audit assessments to review *(in this level operate Russia)*.

Tax authorities operating on the 5th level (e-assessing) assess tax dues without e-filling, in this level taxpayers are allowed to audit government calculated tax *(in this level operate Spain)*.[3]

Success stories of particular countries are presented in this section below in order to show how much difference technologies have already made to standard ways of communication with taxpayers, data gathering and other processes of tax administration.

Most countries have developed special platforms as safe channels through which tax authorities communicate with taxpayers and receive electronic tax returns and other data. For instance, according to Making Tax Digital Plan[4], by 2020 in the United Kingdom most businesses, self-employed people and landlords will be required to keep track of their tax affairs digitally and provide updates to tax authorities at least quarterly via their digital tax account.[5]

[3] EY, 'Tax Authorities Are Going Digital: Stay Ahead and Comply with Confidence' [2017] 1.
[4] See HM Revenue & Customs official website: https://www.gov.uk/government/publications/making-tax-digital/overview-of-making-tax-digital.
[5] OECD, 'Technologies for Better Tax Administration. A practical Guide for Revenue Bodies' (Paris: OECD Publishing 2016) 88.

Some countries have implemented new methods allowing to identify taxpayers. For instance, in Australia voice biometric authentication service has been acknowledged as one of the most successful projects across the federal government. What started as a modest project in 2014 to improve the call centre experience for frustrated citizens has since expanded to the Australian Taxation Office's mobile app, and could have a future with the whole-of-government GovPass identity platform[6]. All taxpayers need to do is save their voiceprint with the ATO[7]. In New Zealand voice biometrics are also deployed to identify taxpayers calling for customer support.[8]

Seeking to tackle tax fraud and receive correct and accurate tax data, many countries developed special platforms for taxpayers allowing them to perform invoicing, accounting, filling and payment electronically. For instance, Chile introduced its e-invoicing system in 2002, which became mandatory for all businesses in January 2014. Swedish e-invoicing system includes a simplified accounting system for businesses, which provides the taxpayer with monthly financial statements and generates prefilled annual returns.[9]

Nowadays, Big Data solutions are inseparable from tax data cross-checking procedures in many countries. For instance, since 2015 the Russian tax authorities have been using Big Data software "ASK VAT-2"[10] to monitor value added tax (VAT) compliance. VAT tax returns containing information about sales and purchase transactions are filed digitally in the XML file format. All incoming data is cross-matched and potential fraud cases are identified automatically. According to official information, implementation of the system allowed to increase revenue from VAT in 2015 by 12.2%.[11]

Dealing with increase in e-Commerce, in 2005 the OECD Committee on Fiscal Affairs published the first version of the Standard Audit File for Tax (SAF-T) guidance encouraging revenue bodies to incorporate SAF-T into their audit and verification methodologies for tax audits. In 2010, the OECD Committee on Fiscal Affairs released guidance for the SAF-T Version 2.0.[12] In 2012, European Commission endorsed an Action Plan to Strengthen the Fight Against Tax Fraud and Tax Evasion. One of means to enhance tax compliance was EU SAF-T[13]. SAF-T was first introduced in Portugal in 2008, then Luxembourg, France, Austria, Lithuania and Poland. Countries next expected to adopt SAF-T in some capacity are Germany, the United Kingdom, Ireland and Czech Republic. Implementation of SAF-T in the OECD jurisdictions will provide greater opportunities for smoother international reporting as well as international auditing.[14]

---

[6] See: https://www.itnews.com.au/news/ato-touts-voice-biometrics-success-471136.
[7] See Australian Taxation Office official website: ttps://www.ato.gov.au/General/Online-services/Voice-authentication/.
[8] OECD, 'Technologies for Better Tax Administration. A practical Guide for Revenue Bodies' (Paris: OECD Publishing 2016) 83.
[9] OECD, 'Tax Administration 2017. Comparative Information on OECD And Other Advanced and Emerging Economies' (Paris: OECD Publishing 2017) 60.
[10] See: http://www.korpusprava.com/en/publications/analytics/vat-2015-big-data-collection-system-change-of-the-procedure-of-control-of-deductions-and-consequences-for-taxpayers.html.
[11] OECD, 'Technologies for Better Tax Administration. A practical Guide for Revenue Bodies' (Paris: OECD Publishing 2016) 56.
[12] OECD, 'Forum on Tax Administration. Guidance Note: Guidance for The Standard Audit File – Tax Version 2.0' [2010] 7.
[13] European Commission, Communication from The Commission to The European Parliament and The Council COM (2012) 722 final concerning an action plan to strengthen the fight against tax fraud and tax evasion [2012] 14.
[14] See: https://www.geanetwork.com/news-and-resources/articles/standard-audit-file-for-tax-saf-t-in-the-eu-and-beyond

Countries that are moving towards e-assessment seek not only greater integration with internal systems of taxpayers, but also to implement integration with natural systems (accounting software, point-of-sale systems, cloud-based banking, etc.), which allows tax authorities to receive data straight from the systems of intermediaries who provide innovative services to taxpayers.[15] In even better way, tax authorities assist intermediaries to develop products that would be primarily integrated with Big Data technologies of tax authorities. For instance, in the United Kingdom, tax authorities work closely with software developers to enable them to create new and more sophisticated products, for instance, application programming interfaces (APIs) with richer capabilities. Currently tax authorities have Application Programming Interface (API) in place for 21 of their services and the majority of transactions carried out online with tax authorities come via third party software.[16]

In recent years, tax authorities also began to use predictive techniques driven by technologies to identify proactive and responsive actions to assist taxpayers to meet their obligations. Such model has been launched, for instance, in Belgium. It informs tax collectors on the solvency or default risk and assists decision making process to enable early recovery action to be taken, in line with the predicted risk of bankruptcy. In Portugal such system even sends remainder notices to potential debtors.[17]

As in most countries, Lithuanian tax authorities use smart web portals such as EDS, Mano VMI system in order to communicate with taxpayers and allow them to submit tax returns electronically. In Lithuania SAF-T was introduced in 2015.[18] Lithuanian taxpayers have to submit data of received and issued VAT invoices electronically using i.SAF subsystem and data of consignment notes and other cargo documents electronically using i.VAZ subsystem since October 2016. i.SAF data submitted by the purchaser and seller is cross-checked on the monthly basis. The Lithuanian tax authorities also assist taxpayers by preparing preliminary personal income tax returns, advance corporate income tax returns (prepared for the first time in March 2017[19]), VAT returns (prepared for the first time in June 2017[20]). i.APS subsystem, which is basically a simplified free of charge accounting system, has been launched in 2019, and is available for Lithuanian taxpayers who carry out business

[15] OECD, 'Technologies for Better Tax Administration. A practical Guide for Revenue Bodies' (Paris: OECD Publishing 2016) 80.
[16] HMRC, 'Third Party Tax Software and Application Programming Interface (API) Strategy' [2015].
[17] OECD, 'Tax Administration 2017. Comparative Information on OECD And Other Advanced and Emerging Economies' (Paris: OECD Publishing 2017) 110-111.
[18] Procedure Concerning Submission of Accounting Data Using Standard Audit File for Tax approved by the 1 July 2015 Order No 699 of the Lithuanian Government. TAR, 2015, No 10833.
[19] See Lithuanian tax authorities' official website: http://www.vmi.lt/cms/teises-aktai-ir-komentarai20/-/asset_publisher/Vi4M/content/pirmaji-karta-suformuotos-preliminariosios-avansinio-pelno-mokescio-deklaracijos;jsessionid=C5E36292C3D627BC2DF4EDA1A73BDE49?_101_INSTANCE_Vi4M_redirect=http%3A%2F%2Fwww.vmi.lt%2Fcms%2Fteises-aktai-ir-komentarai20%3Bjsessionid%3D11F754FB266AE99ECBF946F724C81045%3Fp_p_id%3D101_INSTANCE_Vi4M%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-1%26p_p_col_count%3D2%26p_r_p_564233524_resetCur%3Dfalse.
[20] See Lithuanian tax authorities' official website: http://www.vmi.lt/cms/vmi-naujienos/-/asset_publisher/SyuQPdSIE49Y/content/mokesciu-moketojams-pristatoma-nauja-i-mas-paslauga-%E2%80%93-preliminarioji-pvm-deklaracija

activities based on licence or certificate[21]. Electronic cash registers (as well as related i.EKA subsystem) should be introduced as of 2021[22].

2. Tax Technologies and Taxpayers

Taking into consideration the fact how complex tax regulation and tax compliance procedures may be (for instance, in the United States, tax regulation in printed form exceeds 75,000 pages[23]), it comes by no surprise that taxpayers and especially tax consultants invest their resources in creating tax technologies which, at the basic level, allow them to accelerate certain accounting, tax assessment and filling procedures, and, at the advanced level, simplify global tax planning. Although, there is a huge global demand for tax technologies derived by eagerness to simplify tax matters, current supply is not even close to satisfy such demand.

Usage of Big Data, cloud as well as Robotic Process Automation solutions[24] are old news to taxpayers and their advisors. Nowadays taxpayers seek for even more advanced tax technologies and tools driven by Artificial Intelligence design. For instance, optical character recognition enabled by Artificial Intelligence has already became a common feature of printers scanning checks and VAT invoices, recognizing data and including this data into accounting systems, and various tax fillings. Another example, system called Dexter has been used to optically read tens of thousands of tax fillings without human data entry or interventions.[25] These examples show that currently Artificial Intelligence has been used at the basic (1st) level so called "self-service"[26]. Some tax consultants use it at more advanced (2nd) level by creating tax data visualizations.[27] However, project Odele is by far the most ambitious endeavour towards simplification of tax matters. If succeeded, tax planning assistant software, called Odele, will be able to compare taxes and income for a variety of tax configurations, assumptions and projections, and recommend optimal global tax planning configuration for a particular taxpayer. This software will be driven by Artificial Intelligence design (3rd level).[28] However, release of this software is still far from reality. Financial Gravity, the developer of this project, even launched a special prize[29] for a person

[21] See Lithuanian tax authorities' official website: http://www.vmi.lt/cms/about-vmi/-/asset_publisher/hU6yeb4bVUJN/content/id/9434365 http://www.vmi.lt/cms/mokesciu-naujienos/-/asset_publisher/DkY4/content/id/9434192.

[22] See Lithuanian tax authorities' official website: http://www.vmi.lt/cms/lt/naujienos/-/asset_publisher/Gizm3fjHUUgi/content/vmi-pasirase-es-finansavimo-sutarti-del-i-eka-posistemio-sukurimo;jsessionid=C52C22F96CB2888280EB6A53DB9E7F5B?accessibility=true.

[23] Dr. Cas Milner, Dr. Bjarne Berg, PwC, 'Tax Analytics. Artificial Intelligence and Machine Learning – Level 5" [2016] 8.

[24] See: https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-wins-americas-tax-innovator-award.html.

[25] Dr. Cas Milner, Dr. Bjarne Berg, PwC, 'Tax Analytics. Artificial Intelligence and Machine Learning – Level 5" [2016] 16.

[26] Ibid., 3.

[27] See: https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-wins-americas-tax-innovator-award.html.

[28] See: https://financialgravity.com/odele/.

[29] See: https://financialgravity.com/financial-gravity-companies-inc-announces-herox-prize-odele-ai-enabled-strategic-tax-planning-software/.

who will create an application which would connect natural persons and their personal situations to the most ideal tax planning scenario.[30]

Looking forward, we may expect even greater application of Artificial Intelligence. In tax area it means that predictive analytics, tax modelling and decision automation (4th level) as well as adaptive learning (data mining, machine learning, etc., 5th level) will exceed the greatest wish of taxpayers – due to services of digital tax assistants paying taxes will be much easier than online shopping.

3. Tax Technologies and Tax Compliance

From legal perspective, the increasing usage of tax technologies by tax authorities, taxpayers and tax consultants give raise to a fundamental question – what effect these changes will have in respect of compliance with tax laws?

From the perspective of taxpayers, it should be mentioned that, first of all, improvements of tax technologies do not always save money for taxpayers. For instance, in Brazil after introducing Public Sector of Digital Bookkeeping program, which includes e-invoices, it has been acknowledged that most of taxpayers ultimately suffered from higher compliance costs basically due to increased expenses for IT support and data management solutions[31].

Also, as mentioned before, tax authorities seek to apply personalized approach in respect of taxpayers in order to perform more accurate audits and improve services. However, such measures sometimes can create new issues to taxpayers. For instance, as of 2018, new definitions of "reliable taxpayer" and "non-reliable taxpayer" were introduced in the Lithuanian Law on Tax Administration. Taxpayers depending on a specific category they wall within are subject to different statute of limitations, standard or simplified VAT refund procedure, etc. Among other things, non-reliable taxpayers are not allowed to participate in public procurement and are included in officially announced black list[32]. Speaking about large multinational companies, they usually have a materiality threshold, below which tax risks and inconsistencies are tolerated. Considering these new definitions, such multinational companies established in Lithuania are now at high risk of being listed among non-reliable taxpayers and, respectively, suffering from potential reputation loss of certain level.

On the other hand, the mentioned future trends of tax technologies show that taxpayers and tax consultants look for Artificial Intelligence designs which eventually would perform automated tax planning. Such attitude creates an issue to tax law makers and tax authorities aiming to tackle tax avoidance schemes. It also means that in case future Artificial Intelligence designs do not combine tax planning decisions with economic arguments of taxpayer's business model and simply seek for the maximum tax advantage, taxpayers accepting such proposals will end up at high risk of tax exposure due to committed breach of General Anti-Abuse Rule implemented by the Council Directive in

[30] See: https://www.herox.com/financialgravity.
[31] PwC, 'Brazilian Tax in A Context' [2013] 12.
[32] Law on Tax Administration of the Republic of Lithuania. Valstybės žinios No 63-2243 [2004] Article 40[1].

2016[33]. In addition to this, tax advisors as well as developers of Artificial Intelligence designs aiming to provide effective tax planning schemes should consider whether these schemes are subject to reporting obligations set forth by the Model Mandatory Disclosure Rules implemented by the OECD in 2018[34] and Mandatory Disclosure Regime which should be applied by the Member States as of 1 July 2020 for the arrangements carried out as of 25 June 2018[35].

Considering the above mentioned, it seems that usage of technologies will not necessarily lead to greater tax compliance. In fact, the actual outcome of these technology trends will highly depend on the relationship tax authorities will build with customers, i.e. taxpayers and their advisors. Considering this, the OECD has suggested that tax authorities should move a step forward and start acting as an intermediary between the state and taxpayers, instead of prioritizing state budget's needs only, they should pay greater attention to the rights and legitimate interests of taxpayers[36] and build enhanced relationship with taxpayers[37] based on mutual trust, respect and co-operation. The more success tax authorities achieve in this area, the greater chances will be that taxpayers perceive tax authorities as respected and trusted partner and, consequently, tend to use tax technologies in a way that helps them to achieve greater tax compliance.

This proposal of the OECD was announced twelve years ago, in 2007, and since then some countries have taken certain steps towards this new level of tax administration. The most popular way to enhance relationship with taxpayers is horizontal monitoring – when taxpayers share real time tax data with tax authorities, and receive instant advise and consultation of tax authorities regarding unclear tax matters. This can be even used as a measure to ensure that statute of limitations will close with submission of tax return[38]. Another very effective mean of enhancing relationship with those taxpayers who want to rehabilitate from the shadow is voluntary disclosure programs. Australia, based on this program, collected 127 million AUD of income from avoided taxes in 2015. In exchange for voluntary disclosure, Australia agreed to impose maximum penalty of 10 percent and release disclosed taxpayers from late payment interest as well as further criminal prosecution[39]. The best example of enhanced relationship between tax authorities and taxpayers by far is Switzerland. Although Swiss tax authorities operate on the modest 1st level of tax administration, they represent all the above-mentioned qualities that enhanced relationship is all about. In short, Swiss tax authorities actually care for their taxpayers. For this reason, 96 percent of Swiss cantons' tax authorities amend tax fillings of taxpayers if, based on their information, taxpayers have reported higher taxable income than they actually should. Switzerland is also the only country where behaviourists found out that

[33] Council Directive (EU) 2016/1164 laying down rules against tax avoidance practices that directly affect the functioning of the internal market [2016] OJ L 193 Article 6.
[34] OECD, 'Model Mandatory Disclosure Rules for CRS Avoidance Arrangements and Opaque Offshore Structures' (Paris: OECD Publishing 2018).
[35] Council Directive (EU) 2018/822 amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation in relation to reportable cross-border arrangements [2018] OJ L 139 Article 2.
[36] OECD, 'Working Paper 3: Overview – The Emerging Direction of The Study' [2007].
[37] OECD, 'Working Paper 6: The Enhanced Relationship [2007].
[38] For instance, since 2005 the USA implements Compliance Assurance Process, based on which tax authorities receive and evaluate tax data of taxpayers on real-time basis and all the disputes have to be solved before submitting tax return to the tax authorities. KPMG, 'IRS Extends CAP Program, Modifying Some Rules and Signalling More Significant Changes May Lie Ahead' [2018].
[39] OECD, 'Tax Administration 2017. Comparative Information on OECD And Other Advanced and Emerging Economies' (Paris: OECD Publishing 2017) 65. OECD, 'Update on Voluntary Disclosure Programmed. A pathway To Tax Compliance' [2015] 31.

majority of taxpayers is not interested in looking for loopholes and tends to pay taxes voluntarily actually following the substance of tax laws.[40] Switzerland is a great example that tax technologies are not everything. People pay taxes, they decide whether to comply or avoid, and even if tax technologies make a lot of decisions on behalf of taxpayers in the nearest future, beyond these decisions the ultimate beneficiary will be a human taxpayer. Therefore, long term investment in building friendly relationship and mutual trust, as a counterbalance to technology driven tax administration scenario, is worth to be considered.

Conclusions

Technologies have a multilevel impact on tax compliance. Nowadays, they help taxpayers to eliminate manual, repetitive tasks and, by doing so, accelerate tax compliance procedures. However, technologies can also facilitate tax avoidance by presenting thoroughly structured global tax planning schemes having no economic reasoning. Considering this, the main focus should be placed not upon technologies, but on the users and their motivation. Respectively, tax authorities work hard to provide taxpayers with updated, digital, user-friendly channels for data exchange and communication with the tax authorities. On the other hand, there are still examples where tax authorities show lack of understanding how much these good new measures will actually cost for taxpayers and how they will be comprehended by taxpayers. In order to avoid future enhanced battles between taxpayers and tax authorities each side armed with advanced tax technologies, tax authorities should place greater focus on the OECD suggestion to establish enhanced relationship with taxpayers so that their inner motivation would be oriented towards greater tax compliance rather than smarter tax avoidance.

Bibliography

1. OECD, 'Technologies for Better Tax Administration. A Practical Guide for Revenue Bodies' (Paris: OECD Publishing 2016).
2. OECD, 'Tax Administration 2017. Comparative Information on OECD And Other Advanced and Emerging Economies' (Paris: OECD Publishing 2017).
3. OECD, 'Forum on Tax Administration. Guidance Note: Guidance for The Standard Audit File – Tax Version 2.0' [2010].
4. OECD, 'Model Mandatory Disclosure Rules for CRS Avoidance Arrangements and Opaque Offshore Structures' (Paris: OECD Publishing 2018).
5. OECD, 'Working Paper 3: Overview – The Emerging Direction of The Study' [2007].
6. OECD, 'Working Paper 6: The Enhanced Relationship [2007].
7. OECD, 'Update on Voluntary Disclosure Programmed. A pathway To Tax Compliance' [2015].
8. Council Directive (EU) 2016/1164 laying down rules against tax avoidance practices that directly affect the functioning of the internal market [2016] OJ L 193.

[40] Lars P. Feld, Bruno S. Frey, 'Trust Breeds Trust: How Taxpayers are Treated' [2002] 87-99.

9. Council Directive (EU) 2018/822 amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation in relation to reportable cross-border arrangements [2018] OJ L 139.
10. European Commission, Communication from The Commission to The European Parliament and The Council COM (2012) 722 final concerning an action plan to strengthen the fight against tax fraud and tax evasion [2012].
11. Law on Tax Administration of the Republic of Lithuania. Valstybės žinios No 63-2243 [2004].
12. Procedure Concerning Submission of Accounting Data Using Standard Audit File for Tax approved by the 1 July 2015 Order No 699 of the Lithuanian Government. TAR, 2015, No 10833.
13. HMRC, 'Third Party Tax Software And Application Programming Interface (API) Strategy' [2015].
14. Lars P. Feld, Bruno S. Frey, 'Trust Breeds Trust: How Taxpayers are Treated' [2002].
15. Dr. Cas Milner, Dr. Bjarne Berg, PwC, 'Tax Analytics. Artificial Intelligence and Machine Learning – Level 5" [2016].
16. EY, 'Tax Authorities Are Going Digital: Stay Ahead and Comply with Confidence' [2017].
17. KPMG, 'IRS Extends CAP Program, Modifying Some Rules and Signalling More Significant Changes May Lie Ahead' [2018]
18. PwC, 'Brazilian Tax in A Context' [2013].
19. HM Revenue & Customs official website: https://www.gov.uk/government/publications/making-tax-digital/overview-of-making-tax-digital.
20. Australian Taxation Office official website: ttps://www.ato.gov.au/General/Online-services/Voice-authentication/.
21. Lithuanian tax authorities' official website: http://www.vmi.lt/cms/teises-aktai-ir-komentarai20/-/asset_publisher/Vi4M/content/pirmaji-karta-suformuotos-preliminariosios-avansinio-pelno-mokescio-deklaracijos;jsessionid=C5E36292C3D627BC2DF4EDA1A73BDE49?_101_INSTANCE_Vi4M_redirect=http%3A%2F%2Fwww.vmi.lt%2Fcms%2Fteises-aktai-ir-komentarai20%3Bjsessionid%3D11F754FB266AE99ECBF946F724C81045%3Fp_p_id%3D101_INSTANCE_Vi4M%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-1%26p_p_col_count%3D2%26p_r_p_564233524_resetCur%3Dfalse.
22. Lithuanian tax authorities' official website: http://www.vmi.lt/cms/vmi-naujienos/-/asset_publisher/SyuQPdSIE49Y/content/mokesciu-moketojams-pristatoma-nauja-i-mas-paslauga-%E2%80%93-preliminarioji-pvm-deklaracija.
23. Lithuanian tax authorities' official website: http://www.vmi.lt/cms/about-vmi/-/asset_publisher/hU6yeb4bVUJN/content/id/9434365, http://www.vmi.lt/cms/mokesciu-naujienos/-/asset_publisher/DkY4/content/id/9434192.
24. Lithuanian tax authorities' official website: http://www.vmi.lt/cms/lt/naujienos/-/asset_publisher/Gizm3fjHUUgi/content/vmi-pasirase-es-finansavimo-sutarti-del-i-eka-posistemio-sukurimo;jsessionid=C52C22F96CB2888280EB6A53DB9E7F5B?accessibility=true.
25. https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-wins-americas-tax-innovator-award.html.

26. https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-wins-americas-tax-innovator-award.html.
27. https://financialgravity.com/odele/.
28. https://financialgravity.com/financial-gravity-companies-inc-announces-herox-prize-odele-ai-enabled-strategic-tax-planning-software/.
29. https://www.herox.com/financialgravity.
30. http://www.korpusprava.com/en/publications/analytics/vat-2015-big-data-collection-system-change-of-the-procedure-of-control-of-deductions-and-consequences-for-taxpayers.html.
31. https://www.geanetwork.com/news-and-resources/articles/standard-audit-file-for-tax-saf-t-in-the-eu-and-beyond.
32. https://www.itnews.com.au/news/ato-touts-voice-biometrics-success-471136.

TECHNO-LEGAL SYNERGY AND IMPLICATIONS FOR LEGAL RESEARCH: THROUGH THE EXAMPLE OF TRANS-DISCIPLINARY RESEARCH IN LAW AND LANGUAGE ENDANGERMENT

Karan Choudhary[1]

Abstract

Technological advances have influenced every facet of our lives. Even the discipline of law is impacted by it. It has brought with it many challenges which legal community must address. Broadly speaking, direct nexus of technology and law can be witnessed in areas of data security, data privacy, artificial intelligence, competition law, use of technology in the workings of machinery of law in other words the justice delivery system. On the other hand, technological advances have also influenced the way researches are carried out in field of law for instance, jurimetrics, trans-disciplinary research, socio-legal research.

Through this paper, by taking example of my ongoing trans-disciplinary research, I intend to portray the challenges which I encountered while addressing the research problem through the traditional framework of law. The insights can be profitably used by researchers in field of law who propose to address real life problems. Legal research can be enriched by the technological advances and this synergy can assist in designing better solutions and justice conscious remedies.

Keywords: Social Innovation, Emergent model approach, Language policy designs, Multilingualism, Cultural rights.

Introduction

We live in a world which is ever evolving. Social innovation, technological advances are impacting various spheres of human affairs. It would be no exaggeration to suggest that technology influences us right from the cradle to the death bed and sometimes even beyond.[2] Every sphere of law is impacted by it. Direct nexus of law and technology can be witnessed in areas of data security, data privacy, artificial intelligence, competition law, use of technology in the workings of machinery of law in other words the justice delivery system. However, it is not to suggest that interaction between the two is limited only to those charted areas. Advances in technology has also impacted/influenced the way in which legal researches are imagined, fashioned and carried out.

[1] Is joint PhD Candidate at Université Paris Nanterre and National Law University Delhi. **He is currently researching on cultural heritages, law and policy.** Can be reached at E-mail: karan.choudhary@parisnanterre.fr; karan.choudhary@nludelhi.ac.in; ORCID ID - 0000-0002-6621-0962.

[2] For example, influence of technology can be seen in ART (Assisted Reproductive Technology), fetal medicines, eco-friendly funerals. As regards, post-death situations, character merchandising can be example. See, Elvis Presley Enterprises Inc v Sid Shaw Elvisly Yours, [1999] EWCA Civ 964.

Legal Research

Traditionally, legal research was conceived to be a philosophical cum jurisprudential inquiry. It entailed solemnly thinking about solving legal problems using the legal information/data collected from various legal sources (for example primary and secondary sources of law). The whole research process was aided by various forms of reasoning and analytical tools. A classic image which pops up in mind is that of a person smoking a pipe on a rocking chair in solitariness and thinking about legal issues. It required mental agility, tranquility, ability to develop strategies in mind and foresee their consequences and years of experience to master the researching skills. Especially in the practice of law, research skills like ability to locate relevant law, ability to cogitate, develop strategies in mind and foresee consequences are more pronounced.[3] Lawyers used these skills in court of law to win cases.

The important points to cull out from the preceding paragraph are - how the legal research was predominantly understood, what was legal data for the research, what were the sources of such data, what was the process for conducting such a research, what was the major purpose of such research? To put succinctly, we must ask how legal research was imagined, conducted, fashioned and for what purpose?

With the passage of time, there has been unprecedented growth in the field of Information and Communications Technology. It has brought to fore issues such as globalization, glocalisation and the whole world is just a click away.[4] Technological advances have also influenced the field of legal research.[5] Contemporary legal researches are relying more and more on modern technological and statistical tools to their advantage.

An example can be taken of field of comparative law. While earlier, it was difficult to access legal material for conducting comparative research (one had to be physically present in order to collect the relevant legal data of the nation concerned) but with the technological advances, most of the material can be easily accessed.[6]

Even the substantive part of the legal research has been influenced. The very dynamics of legal research have been influenced. Law is no longer viewed as an

[3] Example of it can be the chess-fight scene between Roberty Downey, Jr (Sherlock Holmes) and Jared Harris (Professor Moriarty) in the movie 'Sherlock Holmes: A Game of Shadows', wherein each participant is required to cogitate and develop strategies and also predict the result of such strategies, if acted upon in order to achieve the successful outcome. A single miscalculation is enough to cost the game. This example resonates especially with the adversarial legal system wherein lawyers of opposite parties argue case before an impartial judge.

[4] Especially in present times, scholars are trying to think about and address global issues. For example, see Global problems and smart solutions (Edited by by Bjørn Lomborg, published by Cambridge university press); Global Problems, Global Solutions: Prospects for a Better World (by JoAnn Chirico, published by Sage Publications).

[5] Mercedes Bunz and Laima Janciute. Artificial Intelligence and the Internet of Things: UK Policy Opportunities and Challenges. London: University of Westminster Press, 2018. http://www.jstor.org/stable/j.ctv5vddtc.

[6] See Mark Van Hoecke, 'Methodology of Comparative Legal Research', December 2015, DOI: 10.5553/REM/.000010. Further See, Constitute Project, which provides easy access to the constitutions of the world. Can be accessed from URL https://www.constituteproject.org/content/about?lang=en.

exclusive field meant only for lawyers or legal actors. It is opening up to other disciplines like economics, sociology, psychology, statistics, and others.[7] The core idea of the legal research in present times is to solve real life problems and providing efficient solutions/justice conscious remedies, even if it requires trans-disciplinary or inter-disciplinary insights.[8] Inter-disciplinarity here would mean, incorporating insights from non-legal disciplines.[9]

But why have interdisciplinary legal research? For Wendy, answer to the question lies in internal and external effectiveness of law. Internal effectiveness of a legal system refers to the consistency and coherency of the legal norms and their definitions. Issue of internal effectiveness may relate to both *de lege lata* (is a specific legal instrument consistent and coherent as it stands) as well the *de lege feranda* perspective (how could a specific legal approach be optimised). External effectiveness measures whether a legal norm is effective in real life, so it concerns the law in action. Thus internal effectiveness gives us insight into legal reality while the external effectiveness gives us insight into real/lived reality. To take an example, in India, there is a legislation titled 'The Scheduled Castes and the Scheduled Tribes (Prevention of Atrocities) Act 1989' which prohibits atrocities on these vulnerable groups. This legislation was internally effective however not externally effective. Hence there were subsequent amendments taking into account social reality to make this piece of legislation externally effective.

Claes Sandgren similarly observes that traditional legal methodology has shortcomings.[10] He observes that renaissance is needed to make legal research more relevant. The legal positivistic tradition needs to be complemented with empiricism.

Thus we see how evolution in the technological realm has influenced the legal research methodology. With the advances in statistical tools and software, there is drastic increase in computational ability, and we see 'meta-analysis' and 'big data' being used for making law and policy decisions in law. We now can conduct researches in law which were earlier, if not impossible but were difficult. For example, Research center called 'Project 39A' at National Law University Delhi, conducted empirical legal research using modern technology and analyzing the 'big data' made pertinent suggestions for changes in the law and policy.[11] We see use of regression plots and other statistical tools to aid legal research.

Another issues which arises is whether, Artificial intelligence or Algorithms can be used to give justice conscious remedies? This is another research question in itself.

---

[7] One relevant quote here would be of Oliver Wendell Holmes, who observed "For the rational study of law the black-letter man may be the man of the present, but the man of the future is the man of statistics and the master of economics".

[8] See Wendy Schrama, How to carry out interdisciplinary legal research: some experiences with an interdisciplinary research method, Utrecht law review, Volume 7, Issue 1 (January) 2011. Further see, Terry Hutchinson,The Doctrinal Method: Incorporating Interdisciplinary Methods in Reforming the Law, DOI 10.5553/ELR.000055, accessed from URL https://www.elevenjournals.com/tijdschrift/ELR/2015/3/ELR-D-15-003_006 and Werner Menski, Asking for the Moon: Legal Uniformity in India from a Kerala Perspective, KERALA LAW TIMES, 2006(2).

[9] Ibid, Foot Note 7. Further See, K.L. Levine, 'The Law is not the Case: Incorporating Empirical Methods into the Culture of Case Law Analysis', wherein it is observed by the author that legal research methods are not sufficient to answer the real life questions and social science techniques are indispensable.

[10] See Claes Sandgren: On Empirical Legal Science, Stockholm Institute for Scandinavian Law accessed from http://www.scandinavianlaw.se/pdf/40-17.pdf

[11] Can be accessed form URL http://deathpenaltyindia.com/Death-Penalty-India/home.jsp;jsessionid=7AD6F5D7111FDBB8556A7BA08B64EC48.

However, I would like to note pertinent observation made by Prof. Eric[12], " we must distinguish between terms 'decision' and 'reason'…AI can give us a decision, it is just like tossing a coin to find a decision but can it give us reason?" Here I would like to add scholars like Prof. Uprendra Baxi[13] and Prof. Werner Menski[14] who have further explored this theme and underlined the importance of response-able decision making and justice conscious remedies (including process for arriving at the same). I would like to add another term that is 'justice'. Can AI and algorithms give justice? Is justice dependent on facts and circumstances of each case or is it something that can be mechanically reached at? However, I am not going to explore these questions in this paper.

Trans-Disciplinary Research

Language endangerment is both local and global issue. India has highest number of endangered languages in the world. The issue become of further concern when conjoint reading of the UNESCO report and the Linguistic Survey of India report by Government of India[15], reveals that communities facing threat of language endangerment are scheduled tribes, scheduled castes and other socially and economically backwards communities. There have been myriad of efforts undertaken but still the issue is not adequately addressed and the unbridled language erosion continues. Recently, it was reported that last speaker of Bo[16] died and the language was not even documented.

Due to the advancement in the technology we now have better understanding of the gravity of the issue. In other words, we have a sharper and clearer picture of the issue.[17] The UNESCO World atlas on endangered languages, is indicative of how can technology be used in research.[18]

Relying on the data, from UNESCO and other authoritative sources, I try to fathom whether these issues can be addressed through law and policy framework. And why is it that present framework is not bearing fruitful results? Is it about the policy design of the present framework or about the implementation issues? Interestingly, if I take the traditional research framework then it will be not of much avail. Law if looked only from the statutes (or in other

[12] Prof. Dr. Eric Millard is professeur de droit public at Université Paris Nanterre. He made these observations during the International conference, Law 2.0: New Methods and New laws held at Vilnius.

[13] Emeritus Professor of law at University of Warwick and Delhi. See Upendra Baxi, Demosprudence and Socially responsible/Response-able criticism, 9 NUJS L. Rev. 153 (2016). Can be accessed from URL http://nujslawreview.org/2017/01/09/demosprudence-and-socially-responsibleresponse-able-criticism-the-njac-decision-and-beyond/.

[14] Emeritus Professor of South Asian laws, School of law, SOAS, University of London. See Werner Menski, Still Asking for the Moon? Opening Windows of Opportunity for Better Justice in India accessed from https://www.nomos-elibrary.de/10.5771/0506-7286-2016-2-125/still-asking-for-the-moon-opening-windows-of-opportunity-for-better-justice-in-india-jahrgang-49-2016-heft-2.

[15] Data on language and mother tongue, Census of India 2011, Office of the Registrar General & Census Commissioner, Ministry of Home Affairs, Government of India accessed from http://censusindia.gov.in/Census_Data_2001/Census_Data_Online/Language/data_on_language.aspx.

[16] One of the 10 tribes that comprise ethnic group called the Great Andamanese people.

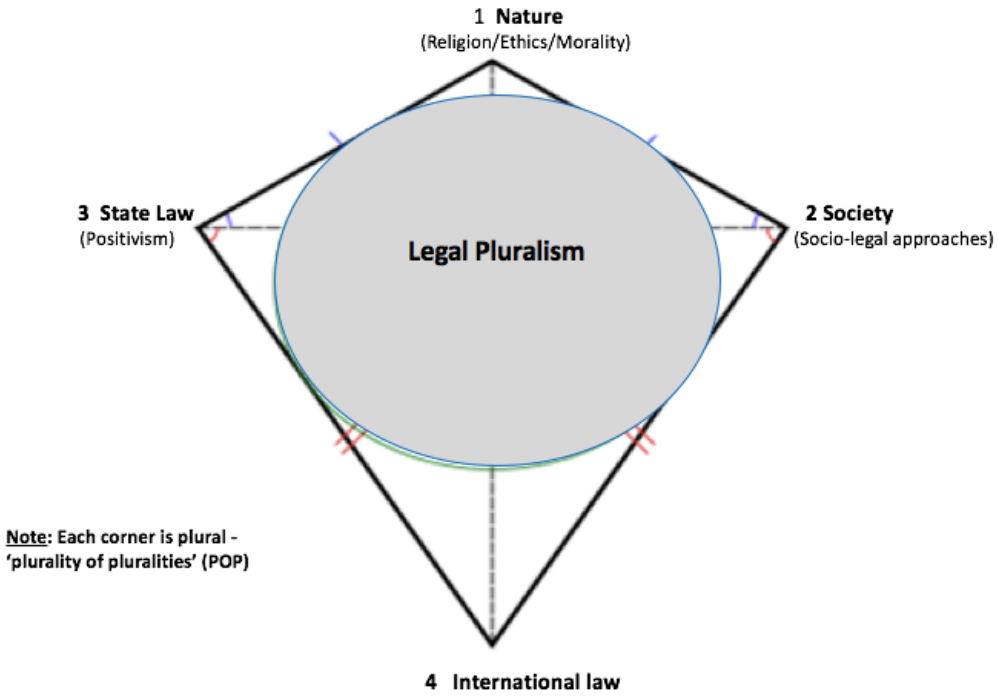
[17] Compare it to recently released first image of Black hole captured by event horizon telescope. It exemplifies the technological advancement and computational abilities of humankind.

[18] UNESCO Atlas of The World Languages In Danger (interactive online edition) accessed from URL http://www.unesco.org/new/en/culture/themes/endangered-languages/atlas-of-languages-in-danger/

words state centric perspective) would not yield valuable insights especially with regards to the research problem I intend to address. Therefore, I undertake legal pluralism framework.

The phrase, legal pluralism simply stated means presence in social field of more than one legal order.[19] Accordingly, it would be fundamental confusion to think state acquiescence to recognise non state sources of law as pluralism and inconsistent with the ideology of state legal centralism. In other words, it is a messy compromise which the ideology of legal centralism feels itself obliged to make with recalcitrant social reality.[20] In other words, Can legal pluralism help in offering some practical alternatives, where the centralism fails.[21]

Prof. Werner Menski notes that responsible decision making is like an alert kite flying. His kite model can be useful in legal research, especially for coming to a justice conscious outcomes.[22]



Diagrammatic Representation of Prof Menski's Early kite model

[19] See J. Griffiths, "What is Legal Pluralism?" Journal of Legal Pluralism and Unofficial Law, vol. 32 no. 24 (1986):5

[20] The Journal of *Legal Pluralism* and Unofficial Law. Volume 18, 1986 - Issue 24, What is *Legal Pluralism*? *John Griffiths*. Pages 1-55, accessed from http://www.tandfonline.com/doi/abs/10.1080/07329113.1986.10756387

[21] Sherman A. Jackson, *Legal Pluralism Between Islam and the Nation-State: Romantic Medievalism or Pragmatic Modernity?*, 30 Fordham Int'l L.J. 158 (2006). Available at: http://ir.lawnet.fordham.edu/ilj/vol30/iss1/5. Also See, K. Günther, "Legal Pluralism and the Universal Code of Legality: Globalisation as a Problem of Legal Theory. Available at http://www.helsinki.fi/nofo/NoFo5Gunther.pdf

[22] Werner Menski, Still Asking for the Moon? Opening Windows of Opportunity for Better Justice in India accessed from https://www.nomos-elibrary.de/10.5771/0506-7286-2016-2-125/still-asking-for-the-moon-opening-windows-of-opportunity-for-better-justice-in-india-jahrgang-49-2016-heft-2

Taking a real life problem, I plan to undertake trans-disciplinary legal research and using non traditional legal framework I plan to suggest justice conscious remedies. Traditional legal framework restricts me to the state centric understanding of law and hence the recommendation from my research will have that orientation. However, with the pluralist framework, I see state is not the only solution to the issue rather a multi-pronged strategy is required to address the issue. The focus then is not only on the law and policy framework with state centrist orientation but also non-state alternatives for example community oriented initiatives. In fact, this is what Prof. Ganesh Devy suggests that NGO's and other non-state alternatives needs to focused upon inorder to nurture for example Particularly Vulnerable Tribal Groups (PVTGs).[23]

Of course, there are other set of questions, for example, what if the concerned community itself is not interested in preserving its language? Even in those scenario, the least that can be done is that the language should be duly documented and its grammar should be prepared, If possible. I address these questions in detail in my PhD thesis and they are not relevant to the purpose of this research paper.

Conclusion

Advancement in technological realm has impacted and influenced legal research methodology. While earlier legal research was considered predominantly to be a philosophical inquiry, now it is imperative that the focus of legal research should be to solve real life problems and give efficient remedies. There is need for empiricism and inter-disciplinarily and need to give up the silos mentality. Traditional legal framework can be debilitating and one can seek contemporaneous frameworks to come to justice conscious remedies. Traditional framework of black letter law is not conducive to such modern legal researches. Inputs from various disciplines can be utilised to enrich legal research.

With the drastic increase in computational abilities, new researches are now possible. It can assist in fields such as jurimetrics, designing better law and policy frameworks. It can help us in having a clearer and sharper image of the problem and better solutions. Possibilities are limitless and it depends how we use technology and concomitant legal frameworks to solve the problems of the society and thereby making field of law even more relevant.

Bibliography

1. Claes Sandgren: On Empirical Legal Science, Stockholm Institute for Scandianvian Law accessed from http://www.scandinavianlaw.se/pdf/40-17.pdf

2. Data on language and mother tongue, Census of India 2011, Office of the Registrar General & Census Commissioner, Ministry of Home Affairs, Government of India accessed from http://censusindia.gov.in/Census_Data_2001/Census_Data_Online/Language/data_on_language.aspx.

[23] Linguist and the 2011 UNESCO Linguapax laureate. Accessed from URL http://www.tata.in/sustainability/articlesinside/Dying-tongues.

3. J. Griffiths, “What is Legal Pluralism?” Journal of Legal Pluralism and Unofficial Law, vol. 32 no. 24 (1986):5
4. K.L. Levine, ‘The Law is not the Case: Incorporating Empirical Methods into the Culture of Case Law Analysis’
5. Mark Van Hoecke, 'Methodology of Comparative Legal Research', LaM december 2015, DOI: 10.5553/REM/.000010.
6. Mercedes Bunz and Laima Janciute. *Artificial Intelligence and the Internet of Things: UK Policy Opportunities and Challenges*. London: University of Westminster Press, 2018. http://www.jstor.org/stable/j.ctv5vddtc.
7. Terry Hutchinson,The Doctrinal Method: Incorporating Interdisciplinary Methods in Reforming the Law, DOI 10.5553/ELR.000055, accessed from URL https://www.elevenjournals.com/tijdschrift/ELR/2015/3/ELR-D-15-003_006.
8. The constitute project, at URL https://www.constituteproject.org/content/about?lang=en
9. UNESCO *Atlas of The World Languages In Danger* (interactive online edition) accessed from URL http://www.unesco.org/new/en/culture/themes/endangered-languages/atlas-of-languages-in-danger/
10. Upendra Baxi, Demosprudence and Socially responsible/Response-able Criticism, 9 NUJS L. Rev. 153 (2016).
11. Wendy Schrama, How to carry out interdisciplinary legal research: some experiences with an interdisciplinary research method, Utrecht law review, Volume 7, Issue 1 (January) 2011.
12. Werner Menski, *Asking for the Moon: Legal Uniformity in India from a Kerala Perspective*, KERALA LAW TIMES, 2006(2)
13. Werner Menski, Still Asking for the Moon? Opening Windows of Opportunity for Better Justice in India accessed from https://www.nomos-elibrary.de/10.5771/0506-7286-2016-2-125/still-asking-for-the-moon-opening-windows-of-opportunity-for-better-justice-in-india-jahrgang-49-2016-heft-2

OPEN DATA, TRANSPARENCY AND FIGHT AGAINST CORRUPTION IN PUBLIC PROCUREMENT

Francois Curan[1]

Abstract

Law 2.0 refers to the existence of a change in the paradigm while at the same time it depicts its digital nature. The interactions between law and digital have very many forms, so we propose to focus on a type in the context of this article. The digital is often perceived as a vector of efficiency, its purpose being the possibility of carrying out traditional tasks with more speed and precision. Digital tools appear in particular as instruments not only "regulated" by law, but also intended to increase the efficiency and effectiveness of legal norms. We propose to deal with it in the light of the Big Data tool that is highlighted in the context of transparency and anti-corruption in the field of public procurement. Thus, the obligation of administrations to enter data and make them public must lead to a better control of public action by citizens. France has implemented such open data strategy as part of its recent reform of public procurement law. Thus a certain amount of information called "essential data" must be entered then published ow specific websites. This approach is already perceived by some as a way of ensuring much better oversight of purchasing policies. The judges would have precise information on the amounts and the holders of markets throughout France. Moreover, this transparency is supposed to have a prophylactic effect by producing an increased surveillance effect of the public action. It is clear that the digital is used in this context as an instrument at the service of the effectiveness of the fight against corruption in the public order. Hence, the question of the practice of a Law 2.0 in this context is to determine whether the Big Data of the public procurement allows a greater efficiency of this norm.

Introduction

French news is animated every year with corruption scandals related to public procurement. Thus, the former president of the National Audiovisual Institute has been condemned and removed from the presidency for favoritism[2]. This event seems to remind everyone of the sad conclusion made by the OECD in a 2016 report highlighting the fact that "public procurement is one of the most vulnerable government activities to corruption"[3].

In an Anglo-Saxon perspective, fighting corruption actually helps ensuring a certain efficiency of procurement. The underlying idea is that corruption inevitably involves economic inefficiency rather than being an evil against which it is necessary to fight. The notion of corruption used here is broader than the only reference to the

[1] Francois Curan is PHD candidate in public law at Université Paris Nanterre. His work concerns digital normativity.
[2] For example this article
[3] OECD, Prévention de la corruption dans la commande publique, 2016, p. 5.

offenses defined by the French Penal Code, namely active bribery[4], passive bribery[5] or illegal taking of interests[6]. Indeed, we will adopt an approach more similar to the OECD which encompasses "misappropriation of funds, undue influence in the assessment of needs, the corruption of civil servants involved in the award process, or fraud in the evaluation of bids, invoices or contractual obligations "but also" significant risks [that] result from conflicts of interest "as well as" concerted bids and cartels "[7]. Corruption is understood in this article as widely as possible as any fraudulent behavior producing effects on the award step in public procurement.

The development of transparency appears as one of the main solutions to fight against fraudulent behavior in the public order. It must first increase the opening of the biding process. A transparent public procurement is perceived as a procurement that gives companies confidence and encourages them to participate. As a result, the competition increases and ensures a competitive situation. This transparency, enshrined in legal principles, is at the intersection of several objectives of public action. Indeed, national and European judges have a principle of transparency in terms of public procurement. The European Court of justice has widened the scope of contracts covered by the transparency obligation[8]. The Conseil constitutionnel[9] has, for its part, consecrated the transparency of the proceedings as a principle with constitutional value. A few years later the Conseil d'État also established the transparency of procedures as a *general principle of law* in public procurement[10].

In the perspective of deploying this prevention through transparency, different means are set up by the public buyers themselves or by the State. The transparency of the biding process has allowed the judge to fill in gaps by setting out obligations for the buyers. The main obligation requires that the buyer organizes a "proper advertisement"[11]. This principle has also made it possible to develop the regime applicable to the advertising of the selection criteria of an offer[12] or to the issuing of modifications in the context of a public service delegation contract[13]. In a broader dynamic of transparency, we see the development of multiple charters, recommendations of good practices, procurement regulations specific to each public access community. Buyers are therefore publishing some kind of code of conduct which, according to them, they have to follow. In doing so, they are not limited to the fact of buying, but explain how they buy, according to which criteria and which rules. The field of darkness favoring arbitrariness would thus be reduced. In this dynamics of deployment of instruments favoring transparency, the digital age brings a new one, supposed to allow a major step forward. Indeed, the use of *Big Data* should make it possible to improve the control of the public action. The court of auditors' Attorney General said in his speech of the 2018 about *Big Data* that they must "allow to better control, but also, by an upstream analysis of the issues and risks, to better program our work, targeting our audits where they will bear the most fruit"[14]. *Open Data* offers important opportunities for administrative contracts. The panorama

[4] Criminal Code, article 433-1.
[5] Idem, article 432-11.
[6] Idem, article 432-12.
[7] OECD, Prévention de la corruption dans la commande publique, 2016, p. 5.
[8] Telaustria Verglags GmbH, Case C-324/98 [2000] ECJ, § 60-61.
[9] Loi habilitant le gouvernement à simplifier le droit, Case n°2003-473 DC [2003] Cons. Const.
[10] Etablissement public du musée et du domaine de Versailles, Case n°328827 [2009] CE.
[11] Telaustria Verglags GmbH, Case C-324/98 [2000] ECJ, § 62.
[12] Veolia Eau – Compagnie générale des eaux, Case n°420296 [2019] CE.
[13] Compagnie des parcs et passeurs du Mont-Saint-Michel, case n°409972 [2019] CE.
[14] https://www.ccomptes.fr/sites/default/files/2018-01/20180122-GJ-Audience-solennelle-rentree.pdf.

offered on the ways of buying will clearly facilitate a kind of exchange of good practices. As a result, the management of the public service and public funds will be improved. In addition, the publicity of performance indicators and the use of public money will make it possible to have a much better view of the quality of public management facilitating audits. On the other hand, if at first it could involve additional workload for the administrations it is possible to see a way for it to implement a study of their own management. This is data that administrations can take over for themselves. In the fight against corruption, big data would then appear as the miracle solution marking finally the advent of an era of transparency for public action and its moralization.

What is called *open data* is actually a combination of a policy of transparency and the handling of big data. Indeed, the Open Data consists, literally, in an opening of the data. This requires the possession of data (Big Data) and a publication policy based on the principle of transparency (Open). The first important step of Open Data can be identified as the moment when "access to public legal data, initially organized by decrees, was qualified as a public service by the Conseil d'État in 1997"[15]. The decrees[16] evoked have initiated the construction of the Légifrance website on which jurisprudence and legislation is in open access. The reuse of public data was framed by the law of 28 December 2015[17]. More recently, the Loi pour une République numérique (*Law for a digital Republic*) has been the opportunity to set up a common system for the publication of certain so-called reference data[18]. Open Data can be defined as the fact of considering that "Public information contained in documents communicated or published by the administrations mentioned in the first paragraph of Article L. 300-2 may be used by any person who wishes purposes other than those of the public service mission for which the documents were produced or received"[19]. From then on, in terms of public procurement, the interest appears clearly. One can easily imagine setting up a purchasing observatory to see what the communities are buying, to whom, for what amount, etc. Open Data may well lead to an ideal implementation of the principle of transparency. It would be possible for everyone to watch from home how taxes paid are used.

The problem addressed therefore aims to study Law 2.0 as a Law using digital tools to "guarantee or facilitate the application of the rules of law"[20]. It is therefore important to emphasize that *Big Data* may well be an instrument for the effectiveness of legal standards aimed at fighting corruption in a transparent way (I). However, it would be hasty to see a miracle cure. So there is a good reason to question the risk for *Big Data* to look more like *Shadow Data* (II).

I. Public procurement *Open Data* as an efficient tool in fight against corruption

To highlight the undeniable benefits that open data can present for the implementation of a policy of transparency in the purchase it is necessary to clarify

[15] L. Cluzel-Métayer 'La construction d'un service public de la donnée' [2018] n°167 RFAP 491.
[16] French Parliament loi relative à la gratuité et aux modalités de la réutilisation des informations publiques 2015-1779 [2015] JORF n°0301 du 29 décembre 2015 p. 24319.
[17] French government Decrees service public des banques et bases de données juridiques 84-940 and 96-481 [1984] [1996]
[18] French Parliament loi pour une république numérique 2016-1321 [2016]
[19] Code des relations entre le public et l'administration, article L.321-1.
[20] P-E Moyse, V. Gautrais, 'Droit et Machine', (Montreal : Thémis 2017) 71.

the positive law relating to the *open data* in procurement. (A) before highlighting the potential exploitation prospects for transparency (B).

The modest french standard for Open data in public procurement

The internationalization of administrative[21] law as a transposition movement at the national level of internationally-designed standards is a good example of *Open Data* public procurement. Indeed, this open data policy seems to be based on France's participation in the Open Government Partnership[22]. This approach, however, needs to be qualified in that the implementation of these obligations is essentially based on the voluntarism of the French State, which has not adhered to any binding structure. This is a voluntary membership of an international initiative in which France has registered its *Open Data* approach. France joined this initiative on May 2nd, 2014[23]. Although not registered as an independent legal entity, this initiative allows for exchanges and agreements on a dynamic of openness of the data relating to the activity of the States. Thus, participation in this initiative assumes compliance with numerous conditions such as the presentation of an implementation plan for open data in the applicant state[24]. The action plan proposed by France for its accession in 2014 makes it possible to establish a link with the obligation relating to the publication of "essential data" appearing in particular in Articles R.2196-1, for public procurement, and R .3131-1, for concessions, of the Public Buying Code. Indeed, following this plan « This transparency must be further improved : in fact, it is as much an issue of accountability, demonstrating the proper management of public funds, as an economic issue, facilitating the fair access of companies to public procurement, and an issue of the public action efficiency, allowing better control of this policy by public managers »[25]. The willingness to implement such an approach in the context of the transposition of the directives market and concession apparently easy in this plan when it is enormously « The transposition of three European directives between now and April 2016 (two directives on public procurement and one directive on concession contracts) will improve this transparency »[26], or there is no such obligations in the directives on public procurement[27] and concession[28]. One can assume transposition of directives has been taken by government to initiate a sector *open data* policy. The report published in 2018 and taking stock of the action plan proposed by France in 2015 confirms this idea since we can read the fact that « Completion of this activity is substantial on paper but, given that the implementation deadline remains a year away at the time of this report, the completion level cannot yet be assessed. Article 107 of the decree n°2016-360 makes it mandatory, not later than October 1st 2018, for buyers to provide free

[21] L. Richer, F. Lichère, 'Droit des contrats administratifs', (Paris : LGDJ 2016) 527.
[22] Read Legal affairs Department of de french minister of economy : «It is part of the policy of open data whose culmination is the participation of France in the "Partnership for Open Government", she has held the Presidency until September 2017"
[23] Read the letter available here.
[24] Open government partnership: articles of governance, II) Participation in the Open Government Partnership, available here.
[25] Presidency of the Republic, For a transparent and collaborativ government : France national action plan 2015-2017, 2015, p. 14.
[26] Idem.
[27] Parliament Directive (EU) 2014/24 on public procurement, [2014] JOUE 28/03/2014, L 94/65.
[28] Parliament Directive (EU) 2014/23 on the award of concessions contracts [2014] JOUE 28/03/2014, L 94/65.

access to data regarding public contracts above the threshold of 25,000€ (pre-tax value). Etc. »[29].

As stated above, the obligation to publish the so-called essential data referred to above, was codified in the Public buying Code with Decree No. 2018-1075 of 3 December 2018. A ministerial order was issued March 22, 2019 to accurately identify the data, the place of publication and the format in which they are to be published. Article 2196-1 of the French Public Buying Code refers to: "1) the procurement procedure; 2) The content of the contract; 3) The performance of the contract, including, where appropriate, its modifications ". With regard to concessions, article R.3131-1 offers the same wording as the article on public procurement. For markets as for concessions, the codification does not include all the elements appearing in the market decree[30] and the concession decree[31]. In these decrees it was possible to observe a differential in the quantity of information relating to the markets and that relating to concessions. It was explained by the fact that three additional pieces of information had to be published each year for the concessions. If one sticks to the order of March 22, 2019 a certain number of data are common to the concessions and the procurement: object of the contract, duration, name of the buyer and the holder, main place of performance etc. In summary, this is very basic information intended to account in the general lines of the use of public funds. The term "data" must be distinguished from the notion of information. Indeed, the notion of data refers to a very specific unit so that one piece of information can be indicated by the publication of several data if it is technically necessary. For example, the identification of the buyer is one and the same information that can be given through the name and the SIRET number which is a national identifier used in France. This distinction seems to us all the more clear with the codification which retains three pieces of information in articles R.2196-1 and 3131-1 of the Public Buying Code to which correspond many *data* that are found in the order of March 22 2019. Another example illustrates this by referring to the information on "the nature and purpose of the market" which seems to be two pieces of information. Appendix 1 of the decree of 22 March 2019, however, highlights the existence of three data associated with this information: the CPV code, the text-based object of the market and the nature of the market that has values defined in the decree (market, partnership market, framework agreement or subsequent contract). A closer reading leads to the identification of thirty-one data set in the order of 22 March 2019 for the three pieces of information covered by article 2196-1 of the Public buying Code.

For the most part, the information required by the substantive law relates to attribution except for the three elements related to enforcement. However, many pieces of information, nevertheless relevant to citizens and / or businesses, deserve to be included in the list of so-called "essential" data. One can think, in particular, about information on the final realization and / or the cancellation. Indeed, the economic analysis shows that often information asymmetry leads a buyer to underestimate the value of his need. As a result, the actual performance may lead to a higher amount than he had estimated at the time of the conclusion. This is only an example, but it would be possible to identify many other relevant data. As a result, the standard adopted by French legislation seems modest in the current state of

[29] S. Wickberg, Independant Reporting Mechanism (IRM) : France End-of-Term Report 2015-2017, 2018, p. 30.
[30] French Government relatif aux marchés publics 2016-360 [2016]
[31] French Government relatif aux concessions 2016-86 [2016]

affairs. Modest as it is, this standard still opens real possibility of using these datasets.

Important ways of exploiting Big Data of public procurement

The public order Big Data can be used as part of the preventive and repressive aspects of the fight against corruption.

As a preventive measure, we can think of the prophylactic effect of setting up a procurement observatory. Indeed, by a kind of a panoptic effect it will be possible for each and everyone to monitor the purchases made by any legal person using public funds. One can expect a discouragement of behavior that would then be rendered impossible by the clear highlighting of choices that hasn't been revealed in the dark until now. In addition of citizens, companies that participate in procurement procedures will appropriate this data over time and will be able to "watch" each other. On the other hand, it is quite possible that buyers use the publication of these data for purposes of communication about their morality. For example, a mayor could set up a page on the website of his community with all information and a constantly updated infographic to show that he has good practices and that all contracts awarded under his mandate have been in accordance with the law. Even businesses could develop such use of this type of data. For example, a company could publish on its website and keep a table reproducing the price differential between a market at its conclusion and the actual billing at the end of the contract. It would show the buyers that it does not lower the amount of its offers to win the market and then charge a higher price. Those practices will not appear immediately, however in the future these new instruments to be appropriated by the different actors of public procurement.

Uses in the repressive and litigious aspect may appear more obvious. Indeed, big data will be a new instrument available to the authorities for the implementation of the legal norms related to corruption as it has been emphasized in the introduction. In France, we can identify three magistrates likely to use these data. The criminal judge, the administrative judge and the financial judge will all be able to make use of these data in different ways. To be more precise, the administrative judge performs two functions in the contractual field. The judge can intervene urgently to cancel the conclusion of a contract at the request of an evicted company. The judge may also intervene during the execution of the contract to settle a dispute between the administration and its service provider. The financial judge checks the regularity of the receipts, the expenses described in the accounts of organizations which fall within his competence as well as the regularity of the acts of management; he also assesses the results achieved in relation to the objectives set, whether it concerns the state[32] or local authorities[33]. Finally, the criminal judge's mission is the repression of criminal offenses. Therefore, the same behavior can be captured by these different judges and treated each according to his mission. For each of them, however, the constitution of big data of the public order represents a real opportunity for the improvement of their works. This will allow them to make comparisons, histories and all kinds of analysis operations very quickly and easily. It will be possible to retrace a history by buyer and see if a holder returns too frequently and at prices yet higher than those of the market. It remains that the contentious treatment of these data is not fixed. If the question may seem innocuous, statistics

[32] Code des juridictions financières, article L. 111-2.
[33] Idem, article L. 211-3.

are only statistics. It remains complicated to prejudge their binding force. Each of these judges will do they want and the time for litigation is slower than that of digital. Moreover, the reliability of all these data should not be prejudged. Indeed, the origin of these data remains a human seizure, which does not escape the possibility of error. While this possibility may remain marginal, other issues deserve to be raised in a more critical perspective of the big data tool in public procurement. Finally, the judge controlling the awarding of contracts will probably be able to make limited or no use of it. Indeed, the order of March 22, 2019 provides that the data must be published within 2 months after notification of the contract[34]. Therefore, emergency litigation to be introduced before signature or immediately thereafter may not give rise to use of these data by the judge. Similarly, as the appeal against the validity of the contract is closed within two months of "appropriate publicity measures"[35], it is unlikely that the judge uses the information contained in these published data. On the other hand, it is possible to imagine an emergency dispute over the publication of these data in the event that a buyer does not publish them within the given deadline. Article L. 521-3 of the Code of Administrative Justice allows the judge "to order all other useful measures without hindering the execution of any administrative decision". Challenges remain both in the very notion of transparency and in its implementation through the constitution of big data.

II. *Big Data*, *shadow data*? Complex implementation of transparency principle

The point here is to show that the Open Data policy implemented is in fact dependent on the way of conceiving and inscribing the principle of transparency in the legal order (A). As a result, it will be possible to highlight a number of issues associated with its concrete implementation (B).

Necessary choice of concept of transparency

As trivial as this question may seem, the definition of the notion of transparency is a real issue.

In its famous decision of 2003[36] mentioned above, the Conseil constitutionnel decided that "the public contracts respect the principles of freedom of access to the public order, of equality of treatment of the candidates and transparency of the procedures". The Conseil constitutionnel chose to uphold these principles on Articles 6 and 14 of the Declaration of the Rights of Man and of the Citizen of 1789. Article 6 of this declaration states that "The law is the expression of the will General. All citizens have the right to compete personally, or through their representatives, in its formation. It must be the same for everyone, whether it protects or punishes. Etc." enshrining the principle of equality before the law. For its part, Article 14 provides that "All citizens have the right to ascertain, by themselves or by their representatives, the necessity of the public contribution, to freely consent to it, to monitor its use, and to determine the quota, the base, the recovery and the duration ", dedicating the principle of the consent to the tax. Transparency of procedures can therefore be interpreted through the principle of equality following this approach. Indeed, it does not embody a general principle of transparency applicable to the law

[34] Read form on essential data here.
[35] Département du Tarn-et-Garonne, Case n°358994 [2014] CE.
[36] Loi habilitant le gouvernement à simplifier le droit, Case n°2003-473 DC [2003] Cons. Const.

of the public order as a whole. The principle is indeed a "principle of transparency of procedures", which is already more restrictive than a principle of transparency alone. The Court of Justice of the European Union follows a similar approach in considering that the obligation of transparency "consists in guaranteeing, in favor of any potential tenderer, a degree of adequate publicity allowing an opening of the market of services to the competition and the control of the impartiality of the tendering procedures "[37]. This perspective makes it possible to assert as François Llorens that the transparency of the procedures allowed "to lead to a body of non-negligible solutions that the only principle of equality would not have made it possible to release as easily"[38] confirming the status of transparency as a sort of spare wheel of equality. Linked to the principle of equality that underpins it, a transparent procedure is a procedure that guarantees fair treatment to all companies wishing to participate[39]. If these remarks may seem trivial, we can not be surprised by this choice regarding the absence of reference to Article 15 of the Declaration of the Rights of Man and of the Citizen in support of this principle, which states that "The society has the right to demand that any public official be accountable to his administration". The Conseil constitutionnel, however, makes use of this provision on public procurement as in a 2008 decision in which it considers that the "good use of public money [is a] requirement of constitutional value that derives from Articles 14 and 15 of the Declaration of 1789 "[40]. Therefore, only the proper management of public funds derives from Article 15 of the 1789 Declaration.

However, the law relating to the *Open Data* of the public commission does not seem to base the obligation relative to the publication of the essential data on the principle of transparency of the procedures as the Conseil constitutionnel has dedicated it. The transparency involved in publishing this data is much broader than just the issue of procedure. Indeed, the publication of the amount of the amendments[41] shows, for example, a broader ambition than the mere transparency of the procedure. The Legal Affairs Department of the French Ministry of the Economy shares this broader vision according to what one can read on its website : "This obligation is part of the policy of transparency of public life"[42] which refers to a broader approach than the only angle of the procedures.

Because of its more closed texture the transparency of the procedures may weigh as a constraint on this broader approach. Indeed, following the approach of Professor François Llorens[43], if we retain transparency as a spare wheel of the principle of equal treatment we see that the use of this principle is restricted. In this perspective, the regulation of corruption is done through a market mechanism. If we consider the principle of transparency of procedures as a source of law, then it risks acting as a constraint on the very construction of an Open Data policy. As a result, the opening of market data is likely to occur only in the perspective of addressing only the economic operators. Indeed, if we should not advocate what would be the correct interpretation or the right legal standard to adopt in the context of a transparency policy, it is at least possible for us to identify the different possible

[37] Telaustria Verglags GmbH, Case C-324/98 [2000] ECJ, § 62.
[38] F. Llorens 'Transparence et contrats publics' [2004] n°1 Chron. 1.
[39] F. Llorens 'Transparence et contrats publics' [2004] n°1 Chron. 1.
[40] Loi relative aux contrats de partenariat, Case n°2008-567 DC [2008] Cons. Const.
[41] France Order du 22 mars 2019 relatif aux données essentielles dans la commande publique [2017] modified by a France Order du 27 juillet 2018 [2018]
[42] Website of Legal Affairs Direction of the minister of economy.
[43] F. Llorens 'Transparence et contrats publics' [2004] n°1 Chron. 1.

meanings of a principle and in contrast to put forward which ones may be more difficult to draw from a principle. In this case, the purpose is to summarize underlining the fact that a principle of "transparency of procedures" is more binding than a more general principle of "transparency" applicable to the whole public procurement more than just the question of procedures.

The role of the concept becomes all the more clear when one examines the legal issues associated with the implementation of this principle in the publication of market data.

Fight against corruption, between public service and biding strategy

The implementation of transparency in an approach to the fight against corruption appears ambivalent, as is the concept itself, depending on whether it is widely or more narrowly envisaged. Indeed, on the one hand, it is tempting to relate this approach to the more general one of setting up a public data service[44] by entering into a broad conception of the notion of transparency. On the other hand, if we stick to a more restricted conception of the notion, the construction of this *Open data* of the order can be included only in a process of pursuit of efficiency of the procedures of transfer from which it would result a reduction of corruption situations. One can indeed consider that there is antagonism between these two approaches or on the contrary that they combine without difficulty. The problem is eminently complex and it would be very ambitious to wish to solve it in these few lines.

While echoing the debate on the notion of transparency that we wish to retain for public procurement, this ambivalence also questions the legal architecture of the implementation of transparency. This ambivalence indeed has consequences on the legal regime applicable to the publication of these data relating to the purchase. This questions in particular the articulation of the competences and rights of the various entities involved in the publication of these data. This problem is all the more open as in positive law, the essential data of the public order do not fall within the field of the nine data sets known as "reference" which are part of the public service mission of Etalab[45], State startup in charge of *Open Data* in France. Therefore, essential public procurement data can be considered as being only part of a sectoral approach and therefore subject to a regime entirely specific to them. It is also possible to question the evolution prospects of Open Data, such as Lucie Cluzel-Métayer : "Can this enrichment of the offer go as far as covering all the" general interest "data? By introducing this notion, the law for a digital Republic intended to put in Open Data data, sometimes produced by private actors independently of a public service mission but can be very useful for the public authorities, as for the citizens "[46]. Therefore one might be tempted to break the purely sectoral regime of publication of the essential data of the public order by an official qualification of data of general interest. However, this qualification is lacking in both case law and positive law. The essential data of the public order therefore remain in the state an isolated island.

The modalities of publication of these essential data are today fixed by the decree of March 22, 2019 relative to the essential data of the aforementioned public order. There are two ways of publishing this data for buyers subject to the Public Order Code, one of which is mandatory and the other optional. The mandatory way

[44] L. Cluzel-Métayer 'La construction d'un service public de la donnée' [2018] n°167 RFAP 491.
[45] Idem.
[46] Idem.

is a publication on the buyer profile[47] and the optional channel a publication on "the single interministerial portal intended to collect and freely make available all public information"[48]. This portal is today the site data.gouv. The legislation encourages buyers to publish on this portal by reducing the duration of the obligation to keep its data on their buyer profile. Indeed, a publication on the buyer profile alone requires a five-year retention on it while a publication on more data.gouv reduces the duration to one year[49].

However, depending on the mode of publication that is done, the actors involved in the publication vary. In the case where the buyer chooses to make only one publication on his buyer profile then the operation falls within his sole competence and the contractual relationship he has with the provider of his buyer profile. On the other hand, if the buyer chooses to publish on the mentioned interdepartmental portal, ETALAB intervenes in addition to the actors already mentioned.

So there is a legal architecture to build on the implementation of what are called data flows. Indeed, the legal problem is then to identify who has the obligation to set up a *data flow,* and therefore to finance it. The statutes of broadcasters and producers of data leave unanswered the question of the competence of which the construction of the flow itself falls. Although without a clear regulatory response, the solution has been a rather complex tinkering process of attaching essential market data to existing data streams that ETALAB would retrieve[50]. These two categories are also not taken up by the provisions of the decree of March 22, 2019. Indeed, Article 7 of the decree of March 2019 remains very impersonal in its formulation allowing not precisely identify the distribution of obligations and competences. As a reminder, paragraph two states that "However, when the essential data are made public on the single interministerial portal intended to collect and make freely available all the public information, they are kept available on the buyer profile for a minimum period of one year. In other words, it only takes note of a possible publication on the portal maintained by Etalab without specifying how to set up this publication. The legal architecture for implementing a broader conception of transparency therefore seems quite complex. It is thus easy to understand how tempting it is to adopt a more restricted approach to transparency whose "purpose is to disseminate the data, not to" any person "but to the" right person "[51]. From this point of view, it is considered that the essential data only fulfill a function of guaranteeing the efficiency of the procurement procedures by being part of the more restricted view of a principle of "transparency of procedures".

Conclusions

If we take the standpoint of the fight against corruption, two *Open Data* approaches appear clearly. On the one hand, by adopting a principle of transparency that is widely understood, we see the emergence of a policy to fight against corruption, which is part of the wider wake of public transparency and moralization. On the other side is the possibility of an anti-corruption policy that would result from

[47] Code of Public Buying, article R.2196-1 and R.3131-1.
[48] France Order du 22 mars 2019 relatif aux données essentielles dans la commande publique [2019], article 7.
[49] France Order du 22 mars 2019 relatif aux données essentielles dans la commande publique [2019].
[50] See the diagram on he website Data.gouv.
[51] L. Cluzel-Métayer 'La construction d'un service public de la donnée' [2018] n°167 RFAP 491.

an increase in market mechanisms and their guarantee in the procurement and competitive processes. Far from constituting antagonistic approaches, it seems that the first step can encompass the second while the opposite appears more technically complicated. Indeed, the legal architecture that is set up reveals that the first encompasses the second since the resulting obligations are added to those resulting from the smaller scope of publication. The evolution of public policies in Open Data will decide in favor of one approach or the other. Moreover, the political and technical obstacles are not to be neglected in that the implementation of an open data policy requires that all the actors involved in the data production and dissemination chain agree on categories of data, formats etc. The object public commission is all the more difficult to approach from this angle in France. Indeed, the state, the hospital sector and the local authorities have practices that vary and it is sometimes difficult to build common legal frameworks while respecting their freedom.

Bibliography :

1. Code for finance jurisdictions [2019] ;
2. Code for relations between public and administration [2019] ;
3. Code of public buying [2019] ;
4. Compagnie des parcs et passeurs du Mont-Saint-Michel, case n°409972 [2019] CE ;
5. Criminal Code [2019] ;
6. *Département du Tarn-et-Garonne*, Case n°358994 [2014] CE ;
7. *Etablissement public du musée et du domaine de Versailles*, Case n°328827 [2009] CE ;
8. F. Llorens 'Transparence et contrats publics' [2004] n°1 Chron. 1 ;
9. French Government Decree relatif aux concessions 2016-86 [2016] ;
10. French Government Decree relatif aux marchés publics 2016-360 [2016] ;
11. French Parliament loi relative à la gratuité et aux modalités de la réutilisation des informations publiques 2015-1779 [2015] JORF 0301 ;
12. French Parliament Loi 2016-132 pour une République numérique [2016] JO 0235 ;
13. L. Cluzel-Métayer 'La construction d'un service public de la donnée' [2018] n°167 RFAP 491 ;
14. L. Richer, F. Lichère, 'Droit des contrats administratifs', (Paris : LGDJ 2016) ;
15. Loi habilitant le gouvernement à simplifier le droit, Case n°2003-473 DC [2003] Cons. Const. ;
16. *Loi relative aux contrats de partenariat*, Case n°2008-567 DC [2008] Cons. Const. ;
17. OECD, *Prévention de la corruption dans la commande publique*, [2016] ;
18. Parliament Directive (EU) 2014/23 on the award of concessions contracts [2014] *JOUE* 28/03/2014, L 94/65 ;
19. Parliament Directive (EU) 2014/24 on public procurement, [2014] *JOUE* 28/03/2014, L 94/65 ;
20. P-E Moyse, V. Gautrais, 'Droit et Machine', (Montreal : Thémis 2017) ;
21. Presidency of the Republic, *For a transparent and collaborativ government : France national action plan 2015-2017*, [2015] ;
22. S. Wickberg, *Independant Reporting Mechanism (IRM) : France End-of-Term Report 2015-2017*, [2018] ;

23. *Telaustria Verglags GmbH*, Case C-324/98 [2000] ECJ ;
24. *Veolia Eau – Compagnie générale des eaux*, Case n°420296 [2019] CE.
25. G. Johanet, 'Audience solenelle de rentrée' [2018], https://www.ccomptes.fr/sites/default/files/2018-01/20180122-GJ-Audience-solennelle-rentree.pdf ;
26. Legal affairs department of the French Minister of economy website : https://www.economie.gouv.fr/daj
27. Open data portal of France : https://www.data.gouv.fr/fr/posts/le-point-sur-les-donnees-essentielles-de-la-commande-publique/ .

Law 2.0 – Robots, Social Media and the Traditional Legal Framework

Jan De Bruyne[1], **Cedric Vanleenhove**[2]

Abstract

Society has tremendously changed the last decade and still is in a transitional period because of different technological evolutions. These technological developments affect our way of thinking, doing business, communicating, interaction and the work/life balance. Some argue the law will need a fundamental make-over as well. The question that arises from a legal point of view is thus whether the existing long-standing legal principles are compatible with technological evolutions or, instead, new legislation will need to be adopted. If this is the case, we will formulate some (general) recommendations that can be taken into account by policy-makers, judges and lawyers when creating or applying the law in the 'society of tomorrow'. Our presentation will try to provide an answer to these fundamental issues through a case-study of recent evolutions in two different fields of law, namely the introduction of self-driving cars (SDCs) in traffic for liability law and the use of social media in court proceedings for procedural law.

Keywords: Technology, Social Media, Artificial Intelligence, Robots, Self-Driving Cars, Legal Reform

Introduction

Society has changed tremendously in the last decade. It still is in a transitional phase because of different technological developments. These evolutions affect our way of thinking, doing business, communicating, interaction and the work/life balance. It is, therefore, not surprising that several aspects related to those technological evolutions are increasingly being studied in academia[3] and addressed by policymakers.[4] The question that arises from a legal point of view is whether some of the existing long-standing legal

[1] Dr. Jan De Bruyne (Master in Law, Ghent University & Master EU Studies, Ghent University) is Post-Doctoral Researcher at the Faculty of Law and Criminology of Ghent University. He was a van Calker scholar at the Swiss Institute of Comparative Law in Lausanne in 2018. He has been a Visiting Fellow at the Institute of European and Comparative Law of Oxford University in 2014 and at the Center for European Legal Studies of the University of Cambridge in 2015.

[2] Prof. Dr. Cedric Vanleenhove (Master in Law Ghent University & LL.M Cambridge) is Professor at the University of Liège as well as Post-Doctoral Researcher in the field of transnational law at Ghent University. He was a Visiting Fellow at the Institute of European and Comparative Law of Oxford University in 2013, a Visiting Researcher at Harvard Law School in 2014 and a Van Calker Fellow at the Swiss Institute of Comparative Law in 2017.

[3] See in general: R. Brownsword, E. Scotford & K. Yeung, 'The Oxford Handbook of Law, Regulation and Technology' (Oxford: Oxford University Press 2017) 1339p.

[4] Reference can, for example, be made to a Resolution by the European Parliament of the 16th of February 2017 with recommendations to the Commission on civil law rules on robotics.

principles are compatible with technological evolutions or whether new legislation will need to be adopted. In this regard, some argue that the law lags behind technological development.[5] Technological evolutions may expose gaps in the existing legal framework or may give rise to undesirable conflicts and call for changes.[6] We will try to provide an answer to these fundamental issues through a case-study of recent evolutions in two different fields of law, namely the introduction of self-driving cars (SDCs) in the area of liability law (part 1) and the use of social media for notice of court proceedings in the area of procedural law (part 2). We will briefly summarise the main findings of our article in a conclusion.

1. Self-Driving Cars and Liability

A first example that is analysed is the autonomous vehicle. Once some preliminary considerations have been discussed (part 1.1.), we will proceed with an analysis of aspects related to the liability for damage caused by self-driving cars (part 1.2).

1.1. Preliminary Considerations

Self-driving or autonomous vehicles are no longer a mere futuristic idea. According to recent predictions, fully autonomous vehicles could already be available within five to twenty years.[7] Vehicles, however, will not suddenly become fully autonomous or self-driving. Instead, technology will gradually take over a user's control over the vehicle. Technology has already partly taken over some of the user's tasks in controlling the vehicle. Examples thereof are adaptive cruise control, lane keeping assistance and automatic parking systems. These forms of partial vehicle are covered by the umbrella term Advanced Driver Assistance Systems (ADAS).[8] Vehicles will eventually be able to take persons from one place to another without any human interference.[9] In that case, one can speak of a fully autonomous or driverless vehicle.[10] Today, only prototypes of such vehicles exist. They are currently being tested on the road by companies such as Google and Tesla. [11]

---

[5] See: B. Moses, 'Agents of Change: How the Law "Copes" with Technological Change' [2011] 20 Griffith L.Rev. 764.

[6] R. Leenes et al, 'Regulatory challenges of robotics: some guidelines' [2017] 9 L.I.T. 7.

[7] J.M. Anderson et al., Autonomous Vehicle Technology. A Guide for Policymakers (California: RAND 2016) 4.

[8] See for more information: H. Surden & M.A. Williams, 'Technological Opacity, Predictability, and Self-Driving Cars' [2016] 38 Cardozo L.Rev. 134-135; K. Van Wees, 'Vehicle Safety Regulations and ADAS: Tensions Between Law and Technology' in X, 'IEEE International Conference on Systems, Man and Cybernetics' (The Hague 2004) 4011-4016.

[9] See for an overview of the technology used in autonomous vehicles: H. Surden & M.A. Williams, 'Technological Opacity, Predictability, and Self-Driving Cars' [2016] 38 Cardozo L.Rev.129-150; J.M. Anderson et al., Autonomous Vehicle Technology. A Guide for Policymakers (California: RAND 2016) 55-74.

[10] H. Surden & M.A. Williams, 'Technological Opacity, Predictability, and Self-Driving Cars' [2016] 38 Cardozo L.Rev. 132-133.

[11] See for an extensive discussion and further references: J. De Bruyne & J. Tanghe, 'Liability for Damage Caused by Autonomous Vehicles: a Belgian Perspective' [2018] 8 J.E.T.L. 324-371; J. De Bruyne & C. Vanleenhove, 'The Rise of Self-Driving Cars: Is the Private International Law Framework for non-contractual obligations posing a bump in the road?' [2018] 5 IALS Student Law Review 14-26.

The rise of autonomous vehicle technology has different benefits. Foremost, traffic will become much safer with software operating the vehicle. The number of accidents will reduce as computers are generally much better drivers than their human equivalents. The focus of software systems, for instance, does not diminish due to fatigue, alcohol or checking social media. The ability of software to react is much faster and more accurate than that of humans. Transport will also become more time-efficient with autonomous car technology. Self-driving cars will enable people currently facing restrictions in operating a vehicle – such as the elderly, minors or disabled people – to fully and independently participate in traffic.[12] At the same time, however, the introduction of self-driving cars will present many challenges. Autonomous vehicles will have an influence on various facets of our society such as employment, transportation and public infrastructure.[13] Software might replace those persons nowadays employed in the transportation sector and the related industries.[14] More importantly, road accidents will not suddenly disappear despite the increased safety as a result of SDCs. Autonomous vehicles will share the road with 'regular' non-autonomous cars and other road users during a long transition period. Recent accidents show that the technology used in autonomous vehicles is indeed not entirely flawless. Technological sensors do not work perfectly in exceptional circumstances such as stormy weather or heavy rainfalls. The autopilot sensors of a Tesla car, for instance, were not able to distinguish a white tractor-trailer crossing the highway from the bright sky above, leading to a fatal crash.[15] In February 2016, an autonomous vehicle hit a bus because it did not know that long vehicles are less inclined to stop and give way.[16] More recently, several newspapers reported an accident with a Tesla autopilot vehicle, which resulted in the driver's death.[17]

1.2. Liability and SDCs

Against this background, the question arises whether the legal framework dealing with the liability for damage caused by SDCs will need a fundamental make-over[18] or instead minor changes might be sufficient. In other words, one has to assess "whether tort liability rules – as they are currently shaped – are suited to govern the "car minus driver" complexity,

[12] J.R. Zohn, 'When Robots Attack: How Should the Law Handle Self Driving Cars That Cause Damages?' [2015] 2 U. Ill. J.L. Tech. & Pol'y 471; J. Gurney, 'Sue My Car Not Me: Products Liability and Accidents Involving Autonomous Vehicles' [2013] 2 U. Ill. J.L. Tech. & Pol'y 250-252; J.M. Anderson et al., 'Autonomous Vehicle Technology. A Guide for Policymakers' (California: RAND 2016) xv & 16-17; J. De Bruyne & C. Vanleenhove, 'The Rise of Self-Driving Cars: Is the Private International Law Framework for non-contractual obligations posing a bump in the road?' [2018] 5 IALS Student Law Review 16-17 with references.

[13] See: J.M. Anderson et al., 'Autonomous Vehicle Technology. A Guide for Policymakers' (California: RAND 2016) 38-40.

[14] J.M. Anderson et al., 'Autonomous Vehicle Technology. A Guide for Policymakers' (California: RAND 2016) xvii & 39.

[15] See: Tesla's Blog, 'A Tragic Loss', 30 June 2016, https://www.teslamotors.com/blog/tragic-loss.

[16] See: N. Bowles, 'Google self-driving car collides with bus in California, accident report says', The Guardian, 1 March 2016, https://www.theguardian.com/technology/2016/feb/29/google-self-driving-car-accident-california.

[17] See: N. Boudette, 'Fatal Tesla Crash Raises New Questions About Autopilot System', New York Times, 31 March 2018, www.nytimes.com/2018/03/31/business/tesla-crash-autopilot-musk.html, read on 1 May 2018.

[18] H. Surden & M.A. Williams, 'Technological Opacity, Predictability, and Self-Driving Cars' [2016] 38 Cardozo L.Rev 136.

while simultaneously holding on to their theoretical basis".[19] In any case, some changes to the legal framework will be inevitable. The Belgian Highway Code, for example, is not yet adapted to the introduction of autonomous car technology as it still requires that each vehicle has a 'driver'.[20] The driver must at all times be able to perform the necessary driving actions and must have his vehicle under control.[21] It is conceivable that the situation in other EU Member States will be quite similar. The existing liability rules might also need some changes with the commercialisation of SDCs. Reliance on fault-based liability will become uncertain in the context of autonomous vehicles. It will, for instance, not be easy to determine who the 'driver' is in an autonomous vehicle and whether he can be held liable for a violation of the law that is actually committed by the vehicle itself (e.g. crossing a red light). Research also showed that it is by no means straightforward to hold the user of an autonomous vehicle liable for a negligent act in supervising the technology.[22]

Liability in traffic-related matters will, therefore, evolve from a fault-based mechanism towards forms of strict liability. This means that victims will have to target other parties. There are different alternatives in national law. In Belgium, for instance, a party could sue the custodian of a defective object under Article 1384, first paragraph, of the Belgian Civil Code (BCC). That article imposes a strict liability regime for the custodian of a defective object for the damage caused by that object.[23] Another more interesting possibility is to file a claim against the manufacturer of the vehicles or the software under the EU Product Liability Directive.[24] Article 1 of the Directive stipulates that the producer will be held liable for damage caused by a defect in his product.[25] The question arises whether the Product Liability Directive is adapted to the reality of self-driving cars. In this regard, the GEAR 2030 High Level Group concluded that the motor insurance and product liability directives are sufficient at least for those systems expected by 2020. After that date, however, the application of the Product Liability Directive risks to create a number of problems.[26] Against this background, we will examine whether this framework is inadequate and out of tune with the reality of SDCs by focusing on two elements,[27] namely whether software can be qualified as product (part 1.2.1) and the moment when the vehicle is put into circulation (part 1.2.2.).[28]

[19] A. Davola, 'A Model for Tort Liability in a World of Driverless Cars: Establishing a Framework for the Upcoming Technology', 1 February 2018, 2, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3120679.
[20] Art. 8.1. Koninklijk besluit van 1 december 1975 houdende algemeen reglement op de politie van het wegverkeer en van het gebruik van de openbare weg, Stb. 9 December 1975 (Highway Code). See, however, the recently added article 59/1 allowing tests with SDCs.
[21] Art. 8.3. Highway Code.
[22] See: J. De Bruyne & J. Tanghe, 'Liability for Damage Caused by Autonomous Vehicles: a Belgian Perspective' [2018] 8 J.E.T.L. 344-347.
[23] See: J. De Bruyne & J. Tanghe, 'Liability for Damage Caused by Autonomous Vehicles: a Belgian Perspective' [2018] 8 J.E.T.L. 348-354.
[24] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, OJ L 210 (Product Liability Directive).
[25] Article 1 Product Liability Directive. According to Article 5, a product is defective if it does not provide the safety that a person is entitled to expect, taking all circumstances into account.
[26] High Level Group on the Competitiveness and Sustainable Growth of the Automotive Industry in the European Union (GEAR 2030), 'Ensuring that Europe has the most competitive, innovative and sustainable automotive industry of the 2030s and beyond', October 2017, 43-44.
[27] A. Davola, 'A Model for Tort Liability in a World of Driverless Cars: Establishing a Framework for the Upcoming Technology', 1 February 2018, 2.
[28] See for a discussion: J. De Bruyne & J. Tanghe, 'Liability for Damage Caused by Autonomous Vehicles: a Belgian Perspective' [2018] 8 J.E.T.L. 355-364 & 367-370.

1.2.1. Software as a Product?

Article 2 of the Product Liability Directive defines a product as all movables, with the exception of primary agricultural products and game, even though incorporated into another movable or into an immovable. There is a debate on the question whether software qualifies as product or not. There are several reasons why software cannot be seen as product. For instance, software might be qualified as a service and not as a product. In addition, the Directive only mentions 'movables'. Therefore, it relates to tangible goods only. It would otherwise make no sense to explicitly include electricity in the scope of the Directive.[29] This requirement is problematic for software products. Software is a collection of data and instructions that is imperceptible for the human eye. A software system is thus often regarded as intangible. Accordingly, it might not fall within the scope of the Product Liability Act.[30]

At the same time, however, there are also some reasons why software should fall within the scope of the Product Liability Directive. Software might be seen as the *object* of a service. It is, therefore, covered by the Directive. Software can also be qualified as a product because it is captured on a tangible medium or device (e.g. CD-ROM or USB). This has been affirmed by the European Commission.[31] Software *an sich* might be considered as a material good as well. The Directive could apply to software even if it is qualified as an intangible good. After all, the inclusion of electricity clarifies that the drafters of the Directive aimed at a wide material scope. Legislators did not think of software in the early 1980s as personal computers only became commercially widespread during the second half of the 1980s. It is thus conceivable that software, in a teleological interpretation of the Directive, falls within the scope of the Directive. The European Court of Justice might come to a similar conclusion in the future. The inclusion of software in the Directive would also reflect the current economic reality in which software is a commercial product just as any other product that may entail risks for users and third parties.[32]

1.2.2. Putting the SDC into Circulation

Pursuant to Article 7(b) of Product Liability Directive, the manufacturer of the product can escape liability when he proves that it is probable that the defect causing the damage did not exist at the time when the product was put into circulation or that this defect came into being afterwards. If software is qualified as a product, any update thereof could be considered an act by which the producer brings a new product into circulation. However, it becomes more difficult with so-called self-learning systems. These systems are not periodically updated but continually improve themselves. For defects that are created in this way, a moment of putting the product into circulation cannot be indicated as the manufacturer did not perform an act to that end. The same reasoning also applies to the liability of the manufacturer of the vehicle. The changes made by a self-learning system and

[29] Article 2 in fine Product Liability Directive.
[30] J. De Bruyne & J. Tanghe, 'Liability for Damage Caused by Autonomous Vehicles: a Belgian Perspective' [2018] 8 J.E.T.L. 355-357.
[31] See: Written Question no. 706/88 of 5 July 1988 and Answer by Lord Cockfield on behalf of the Commission on 15 November 1988, OJ 114/42, 8 May 1989.
[32] J. De Bruyne & J. Tanghe, 'Liability for Damage Caused by Autonomous Vehicles: a Belgian Perspective' [2018] 8 J.E.T.L. 355-357.

the updates performed by the software producer can create defects for which the car manufacturer is no longer liable. Indeed, those defects did not exist at the time when he put the vehicle into circulation. Although the vehicle meets the definition of a product, its manufacturer might thus easily escape liability if the damage is caused by a dysfunction in the software. One could argue that Article 7(b) Product Liability Directive should be inapplicable in those circumstances. This makes it possible for victims to file a claim against the manufacturer of the software even when the defect is created through the continuous self-development of software.[33]

2. Using Social Media for Service of Process

After some preliminary considerations on the use of social media in services of process (part 2.1), we describe the current common law trend of effecting service of process through social networking sites (part 2.2). We then give a short overview of how service of process is effectuated in Belgium, as an example of a civil law country (part. 2.3). Finally, having taken note of the service of process framework in Belgium and the absence of social media as a form of acceptable notice, we reflect on the possible introduction of such service within that jurisdiction (part 2.4).

2.1. Preliminary Considerations

Imagine you open Facebook Messenger and you see the new message notification. It is a message informing you that you have been sued and that you are to appear in court as defendant in a family law case involving proof of paternity. Or: you are browsing through Instagram when you suddenly receive a DM (Direct Message). There is a lawsuit pending against you. You have been served in an insurance matter through the DM. Or: you often use LinkedIn to keep track of your contacts' occupations and achievements. One day your LinkedIn inbox indicates that you have a new message. The LinkedIn message contains a summons and a claim form. A foreign company is taking you to court for trademark infringement. Futuristic scenario's? Think again! These situations have actually taken place in the last decade in Australia[34], Canada[35] and the United States[36] respectively.

In a number of common law jurisdictions around the world courts have allowed plaintiffs to notify the defendant of the commencement of legal proceedings (*i.e.* service of process) through the use of social networking platforms. The list of social media is long but the ones most often used for service of process are Facebook, Twitter, LinkedIn and Instagram. When mentioning this relatively recent line of private law cases to lawyers with civil law backgrounds, reactions ranging from mild amused surprise to utter shock and disgust can be observed. In civil law nations effecting service of process through social

[33] J. De Bruyne & J. Tanghe, 'Liability for Damage Caused by Autonomous Vehicles: a Belgian Perspective' [2018] 8 J.E.T.L. 362-363 & 370.
[34] Federal Magistrates Court of Australia, Byrne & Howard, 21 April 2010, [2010] FMCAfam 509.
[35] A. Robinson, 'Toronto lawyer serves claim with Instagram', 2 February 2018, http://www.canadianlawyermag.com/legalfeeds/author/alex-robinson/toronto-lawyer-serves-claim-with-instagram-15294/.
[36] United States District Court, Eastern District of Virginia, Alexandria Division, WhosHere, Inc. v. Gokhan Orun, 20 February 2014, 2014 WL 670817.

media is completely unknown. Whereas the use of e-mail for service purposes seems to have become increasingly more well established, the use of social media as an avenue for notification of the commencement of proceedings appears to be in a whole different ballpark. As such, scholars in civil law EU Member States have not yet addressed this relatively new development within the common law world. This is unfortunate as getting insight into the practice might prove valuable for enhancing our own service rules. This contribution, therefore, undertakes an analysis of the reported cases to subsequently contemplate on a general level whether social media service will ever form part of the service methods on the EU continent.

2.2. Social Media Service: a Common Law phenomenon

As mentioned, social media service has been observed in common law jurisdictions. After a brief discussion of the roots of the use of social media in service of process (part 2.2.1.), we will examine the conditions laid down by the case law more thoroughly (part 2.2.2.).

2.2.1. How it all begun

The actual cradle of social media service is to be situated in Australia (at least judging by the reported cases). In *MKM v. Corbo & Poyser* the defendants had taken out a home refinancing loan with MKM Capital but had failed to keep up with payments.[37] MKM obtained a default judgment permitting seizure of the property. Before the judgment could be executed it had to be served on the defendants. However, defendants had moved away, had switched jobs and had changed their phone numbers. Repeated efforts at personal service as well as service by mail and publication did not lead to the desired result. MKM therefore made the ground-breaking move of seeking permission to effect service through the defendants' Facebook accounts. The lawyers had located both defendants on the social networking site. To that end they used the personal information the couple had supplied themselves during the loan application process. They were able to link the defendants' date of birth and their e-mail addresses to the Facebook profiles (which were not protected by stringent privacy settings). Master Harper therefore gave plaintiff MKM the green light to inform defendants of the entry and terms of the default judgment via a private Facebook message. In addition, the order had to be served via e-mail and by leaving a sealed copy at their last known address.

Although the origin of social media service lies Down Under, the current centre of gravity for this rather contentious method of service has shifted to the United States. The first approval by an American court came in the case of *Jessica Mpafe v. Clarence Mpafe*.[38] A wife wished to divorce her husband but it was believed he had left the territory of the

[37] Supreme Court of the Australian Capital Territory, MKM Capital Pty Ltd. v. Corbo & Poyser, 16 December 2008, no. SC 608.
[38] Fourth District Family Court of Minnesota (Hennepin County), Jessica Mpafe v. Clarence Mpafe, 10 May 2011, no. 27-FA-11-3453.

United States.[39] Judge Kevin S. Burke noted: "*The traditional way to get service by publication is antiquated and is prohibitively expensive. Service is critical, and technology provides a cheaper and hopefully more effective way of finding Respondent.*"[40] The judge is further quoted as stating that: "*Nobody, particularly poor people, is going to look at the legal newspaper to notice that their spouse wants to get divorced.*"[41] He ordered service to include, but not be limited to, contact via any Facebook, Myspace, or other social networking site, contact via e-mail and contact through information that would appear through an internet search engine such as Google.[42]

2.2.2. Conditions

State court litigation is governed by state law provisions whereas the Federal Rules of Civil Procedure (FRCP) determine the service regime for federal cases. For domestic service Rule 4(e)(1) FRCP refers to state provisions as it permits following state law for serving a summons in an action brought in courts of general jurisdiction in the state where the district court is located or where service is made. Under state law more unconventional methods of service are available in comparison to the federal rules. In some states catch-all provisions are in place. §308(5) of the New York Civil Practice Law and Rules (N.Y. CPLR), for instance, states that the court may order service in any manner, if the other (traditional) methods of service provided by § 308 N.Y. CPLR are impracticable. Impracticability however "does not require proof of due diligence or of actual prior attempts to serve a party under the other provisions of the statute".[43] For service abroad, Rule 4(f)(3) FRCP gives the judge the possibility to order any method he deems appropriate, as long as the method is not prohibited by international agreement. The provision offers this option without any need for the plaintiff to first attempt service via the other methods listed in Rule 4(f) FRCP.[44]

A scrutiny of the available cases reveals that the majority of courts have approved of social media service in combination with another form of service. In *Mpafe v. Mpafe*, for instance, service through social networking platforms was ordered together with *inter alia* e-mail service.[45] In *Ferrarese v. Shaw* plaintiff begun proceedings against his elusive ex-wife who had disappeared with their daughter. The federal court decided that service on the ex-wife should be effected via e-mail, Facebook message and certified mail on defendant's last

[39] H. Van Horn, 'Evolutionary Pull, Practical Difficulties, and Ethical Boundaries: Using Facebook to Serve Process on International Defendants' [2013] 26 Global Business & Development Law Journal 566; A. Eisenberg, 'Keep Your Facebook Friends Close and Your Process Server Closer: The Expansion of Social Media Service of Process to Cases Involving Domestic Defendants' [2014] 51 San Diego L.Rev. 790.
[40] Fourth District Family Court of Minnesota (Hennepin County), Jessica Mpafe v. Clarence Mpafe, 10 May 2011, no. 27-FA-11-3453.
[41] S. Ward, 'Our Pleasure to Serve You: More Lawyers Look to Social Networking Sites to Notify Defendants' [2011] 97 A.B.A.J. 14.
[42] Fourth District Family Court of Minnesota (Hennepin County), Jessica Mpafe v. Clarence Mpafe,10 May 2011, no. 27-FA-11-3453.
[43] District Court for the Southern District of New York, Fortunato v. Chase Bank, 7 June 2012, 2012 WL 2086950; District Court for the Southern District of New York, S.E.C. v. HGI, Inc., 8 November 1999, 99 Civ. 3866, 1999 WL 1021087.
[44] United States Court of Appeals, Ninth Circuit, Rio Properties, Inc. v. Rio International Interlink, 20 March 2002, 284 F.3d, 1015.
[45] Fourth District Family Court of Minnesota (Hennepin County), Jessica Mpafe v. Clarence Mpafe, 10 May 2011, No. 27-FA-11-3453.

known address and on defendant's sister.[46] The Family Court decision in *Noel Biscocho v. Anna Maria Antigua* is another excellent example of the judicial hesitance to completely step away from traditional methods of service in favour of the newly discovered service channel offered by social media. A father who was seeking to modify an order of child support was allowed to serve the mother via Facebook. However, he also had to follow up with a mailing of the summons and the petition to the mother's last known address, even though the court recognised that prior service at that address had been unsuccessful and her physical whereabouts uncertain.[47] This cautious attitude is, however, not shared by all courts. *Baidoo v. Blood-Dzraku* appears to be the first reported case in which the court approved service by Facebook message as the sole method of service. The plaintiff was a married woman who wanted to divorce her husband. She had no physical address for him and he could not be served in person. The court did not require service via publication as a backup method to Facebook, deeming the former to be "*essentially statutorily authorized non-service*".[48]

The available case law tends to impose two requirements regarding the social media account to be served. First, the plaintiff has to provide the court with evidence that the account actually belongs to the defendant (authentication requirement). Second, the plaintiff needs to demonstrate that the defendant makes regular use of his account (evidence of use requirement). Both are logical conditions given the fact that the Due Process Clause of the Fourteenth Amendment to the U.S. Constitution imposes that notice should be "*reasonably calculated, under all circumstances, to apprise interested parties of the pendency of the action and afford them an opportunity to present their objections*".[49]

In *Baidoo v. Blood-Dzraku* the plaintiff was aided by the existence of conversations between her and her husband on Facebook. She submitted an affidavit to which she annexed copies of the exchanges between her and the defendant on Facebook and in which she identified the defendant as the subject of the photographs on the Facebook page in question. This satisfied the court that the account did belong to the defendant. As to evidence of regular use, the court was equally convinced by the exchanges between both parties as they indicated that the defendant regularly logged into his account.[50] Conversely, in *Fortunato v. Chase Bank* the defendant wanted to bring the plaintiff's daughter into the litigation. The request for service through the Facebook account of the daughter was denied for reasons of uncertainty regarding the authenticity of said account. The court argued that: "*anyone can make a Facebook profile using real, fake, or incomplete information, and thus, there is no way for the Court to confirm whether the Nicole Fortunato the investigator found is in fact the third-party defendant to be served*."[51]

2.3. Belgian Legal Framework

In Belgium civil proceedings are initiated either by a writ of summons or by means of a petition. The most common method is the delivery of the writ of summons to the defendant

[46] United States District Court, Eastern District of New York, Giovanni Ferrarese v. Vinda Shaw, 19 January 2016, 164 F.Supp.3d 361.
[47] Family Court of the State of New York (County of Richmond), Noel B. v. Anna Maria A., 12 September 2014, no. F00787-13/14B, 2014 N.Y. Misc. LEXIS 4708.
[48] Supreme Court of New York County, Baidoo v. Blood-Dzraku, 27 March 2015, 48 Misc 3d 316.
[49] U.S. Supreme Court, Mullane v. Central Hanover Bank & Trust Co., 24 April 1950, 339 U.S. 314 (1950).
[50] Supreme Court of New York County, Baidoo v. Blood-Dzraku, 27 March 2015, 48 Misc 3d 314-315.
[51] District Court for the Southern District of New York, Fortunato v. Chase Bank, 7 June 2012, 2012 WL 2086950.

by the bailiff. The Belgian Judicial Code (BJC) lists a number of methods to effect this service of process (art. 33 *et seq*.). The bailiff will respect a certain order and will try to serve the defendant in person first. Service in person means that the bailiff hand delivers the writ of summons to the defendant.[52]

If service in person is not possible, service can be effected at the domicile or, in absence of a domicile, the place of residence of the defendant, by leaving a copy of the writ with a relative, servant or agent, provided that the person is 16 years old or above.[53] If the previous method of service is not possible, the bailiff can leave a copy of the writ in a sealed envelope at the domicile or the place of residence of the defendant, followed by a letter via registered mail the next business day.[54]

Since 31 December 2016 the possibility for the bailiff exists to serve through e-mail. In civil matters the bailiff may choose the method of service (personal service or electronic service via e-mail) depending on the circumstances specific to the case.[55] The bailiff can either use the "*gerechtelijk elektronisch adres*" (a unique e-mail address, issued by the government[56]) of the defendant or, for people who do not have such an address, the "*adres van elektronische woonstkeuze*" (a regular e-mail address, not issued by the government)[57]. In the latter case explicit consent needs to be obtained from the defendant each time the bailiff wishes to serve him through that e-mail address.[58] In both cases the e-mail sent by the bailiff does not contain the actual document to be served. Rather, the content of the documents can only be consulted on a secure digital platform created for that purpose.

If the defendant does not have a known domicile or place of residence at all (neither in Belgium nor abroad), the bailiff will serve the writ on the public prosecutor of the jurisdiction of the court which will deal with the claim.[59]

2.4. Social Media Service in Belgium?

It is not our intention to forecast whether the Belgian legislator will ever decide to incorporate social media service as a service method. We will, however, set out which choices can be made and will signal some of the issues that will have to be dealt with.

First of all, one can wonder which advantages social media offer. One distinct advantage of social media service lies in the fact that it is able to achieve a high likelihood of actual notice. Users of social media platforms typically access their accounts on a regular basis.[60] A recent press release by Facebook, for instance, showed that there were 2.32 billion monthly active users as of 31 December 2018.[61] Social media are oftentimes accessed on mobile devices. On these devices users run applications that push instant

[52] Art. 33 BJC.
[53] Art. 35 BJC.
[54] Art. 38, §1 BJC.
[55] Art. 32quater/3, §2 BJC.
[56] Art. 32, 5° BJC.
[57] Art. 32, 6° BJC.
[58] Art. 32quater/1, §1, 2nd sentence BJC.
[59] Art. 40, para. 2 BJC.
[60] K. Knapp, '#serviceofprocess @socialmedia: Accepting Social Media for Service of Process in the 21st Century' [2014] 2 La.L.Rev. 564.
[61] See in this regard: https://investor.fb.com/investor-news/press-release-details/2019/Facebook-Reports-Fourth-Quarter-and-Full-Year-2018-Results/default.aspx

notifications alerting the account holder of activity on his profile.[62] Besides, if service is performed via a private Facebook message or via a post on the defendant's Facebook wall, the likelihood of actual notice is even amplified. Under the default settings, the defendant will receive a notification through e-mail of the message or of the post and any subsequent comments.[63]

Compared to the second-newest kid on the block, e-mail service, social media holds a few trump cards. In case of service via e-mail there is no possibility to determine whether the e-mail address belongs to the defendant unless the defendant states so himself.[64] A social media account, on the other hand, can be scrutinised to verify the identity of the holder if the privacy settings allow it. Additionally, e-mail is more prone to spam attacks.[65] In that regard, social media networks fare better.[66] Spam messages are less common on social media platforms and malicious messages are less problematic because users can often view the sender's profile without opening the message or they can adjust their settings to disallow messages from individuals who they have not added as "friends".[67]

A subsequent question would be whether there is a need for this type of service to be implemented in Belgium. It is unlikely that the Belgian legislator will introduce social media service as a self-standing independent method. For Belgium, where e-mail service is still in its infancy, this would be too radical. In our opinion, there could nevertheless be a place for this innovative method in the Belgian system.

In part 3.3 it was explained that service on defendants who do not have a known domicile or place of residence is replaced by service on the public prosecutor of the jurisdiction of the competent court.[68] In Belgium the National Chamber of Bailiffs does not keep statistics on the number of times service is in that regard effected on the public prosecutor. In the Netherlands, on the contrary, such figures are available. The Dutch service rules also require that a defendant without a known domicile or place of residence be served through the office of the public prosecutor at the court where the claim will be heard. Before that date these so-called "public writs" were published in daily newspapers. According to a study around 45.000 public writs are served each year.[69] Additionally, it is stated that bailiffs receive little or no response to public writs published in newspapers.[70]

There is no reason why these findings cannot be transposed to Belgium. It is extremely likely that the "artificial" service on the prosecutor does not inform the persons in

[62] A. Upchurch, '"Hacking" Service of Process: Using Social Media to Provide Constitutionally Sufficient Notice of Process' [2016] 38 U.Ark.Little Rock L.J. 601.
[63] District Court for the Southern District of New York, FTC v. PCCare247 Inc., 7 March 2013, 2013 WL 841037, 5.
[64] K. Knapp, '#serviceofprocess @socialmedia: Accepting Social Media for Service of Process in the 21st Century' [2014] 2 La.L.Rev. 569.
[65] J. Wolber, 'Opening a Can of Worms and Viruses: The Impact of E-Service on E-Mail Users Everywhere' [2016] 61 N.Y.L.Sch.L.Rev. 450, footnote 1.
[66] A. Shultz, 'Superpoked and Served: Service of Process via Social Networking Sites' [2009] 43 U.Rich.L.Rev. 1525, footnote 205 (statement made in the context of Facebook).
[67] J. Wolber, 'Opening a Can of Worms and Viruses: The Impact of E-Service on E-Mail Users Everywhere' [2016] 61 N.Y.L.Sch.L.Rev. 450, footnote 1.
[68] Art. 40, para 2 BJC.
[69] Openbare exploten en ambtelijke publicaties – Artikel 54 en enkele andere artikelen van het Wetboek van Burgerlijke Rechtsvordering opnieuw bezien, Preadvies ter gelegenheid van het 10-jarig bestaan van de KBvG, 53-54.
[70] Openbare exploten en ambtelijke publicaties – Artikel 54 en enkele andere artikelen van het Wetboek van Burgerlijke Rechtsvordering opnieuw bezien, Preadvies ter gelegenheid van het 10-jarig bestaan van de KBvG, 31.

question, given the results in the Netherlands where service on the prosecutor is even combined with service by publication. It is here that social media service could play a role. Belgian lawmakers could make it obligatory for plaintiffs to undertake a reasonable attempt to serve the elusive defendant via his social media channels, if any. It can be expected that such a subsidiary place for social media service will prompt less resistance than embracing it as a full-blown mechanism. Furthermore, because social media service is deployed as a supplement to an established method, it will alleviate at least some of the sceptical concerns raised by its opponents.

As to the concrete organisation of social media service, the Belgian legislator will face further issues. Certain safeguards relating to the authentication and regular use of the account will need to be construed. The American experience might serve as a source of inspiration. A further specific difficulty that can be identified relates to the bailiff who has to effect the service. Does the bailiff have to use an official account or can he use the account of the plaintiff or can he even send the notice via a fake account? Time will tell to what extent Belgium will "connect" with social media, if at all.

Conclusion

The article examined whether some of the existing legal principles in two different fields are compatible with technological evolutions. With regard to self-driving cars, some legal changes at the national level are inevitable. Legislation dealing with road safety is not yet adopted to the introduction of autonomous vehicles. We have also shown that the application of some of the concepts used in the Product Liability Directive might become problematic when SDCs will be commercialised. For instance, the moment of putting the product into circulation might be incompatible with autonomous systems. In any case, when policymakers would change the legal framework, they should take into account that a minor modification of one aspect (e.g. qualification of software) can have major consequences on the liability of the manufacturers of software or of the SDC. Therefore, we suggest a balanced and well-considered approach when it comes to adapting the existing legal framework to technological evolutions.[71]

As to service of process via social media, the article explored the remarkable finding that some courts in common law countries have allowed the notice of the commencement of civil proceedings to be effected via one or more social media accounts belonging to the defendant. In contrast, in civil law EU jurisdictions this phenomenon does not exist. The article laid the conditions imposed by American courts for this type of service bare and subsequently gave an overview of the Belgian procedural framework. Even though it remains to be seen whether the Belgian legislator will ever be tempted by this novel method of service, it is submitted that social media service could be useful as a second layer of subsidiary notice when the defendant does not have a known address.

Bibliography

[71] See also: J. De Bruyne & J. Werbrouck, 'Merging self-driving cars with the Law' [2018] 34 Computer and Security Law Review 1150-1153.

Legislation

1. Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, OJ L 210.
2. Koninklijk besluit van 1 december 1975 houdende algemeen reglement op de politie van het wegverkeer en van het gebruik van de openbare weg, Stb. 9 December 1975.
3. Openbare exploten en ambtelijke publicaties – Artikel 54 en enkele andere artikelen van het Wetboek van Burgerlijke Rechtsvordering opnieuw bezien, Preadvies ter gelegenheid van het 10-jarig bestaan van de KBvG, 76 p.

Books

1. M. Anderson et al., Autonomous Vehicle Technology. A Guide for Policymakers (California: RAND 2016) 185p.
2. R. Brownsword, E. Scotford & K. Yeung, 'The Oxford Handbook of Law, Regulation and Technology' (Oxford: Oxford University Press 2017) 1339p.

Journals

1. A. Eisenberg, 'Keep Your Facebook Friends Close and Your Process Server Closer: The Expansion of Social Media Service of Process to Cases Involving Domestic Defendants' [2014] 51 San Diego L.Rev. 779-822.
2. A. Shultz, 'Superpoked and Served: Service of Process via Social Networking Sites' [2009] 43 U.Rich.L.Rev. 1497-1528.
3. A. Upchurch, '"Hacking" Service of Process: Using Social Media to Provide Constitutionally Sufficient Notice of Process' [2016] 38 U.Ark.Little Rock L.J. 559-625.
4. B. Moses, 'Agents of Change: How the Law "Copes" with Technological Change' [2011] 20 Griffith L.Rev. 764-794.
5. H. Van Horn, 'Evolutionary Pull, Practical Difficulties, and Ethical Boundaries: Using Facebook to Serve Process on International Defendants' [2013] 26 Global Business & Development Law Journal 555-576.
6. H. Surden & M.A. Williams, 'Technological Opacity, Predictability, and Self-Driving Cars' [2016] 38 Cardozo L.Rev. 121-181.
7. J. De Bruyne & J. Tanghe, 'Liability for Damage Caused by Autonomous Vehicles: a Belgian Perspective' [2018] 8 J.E.T.L. 324-371.
8. J. De Bruyne & C. Vanleenhove, 'The Rise of Self-Driving Cars: Is the Private International Law Framework for non-contractual obligations posing a bump in the road?' [2018] 5 IALS Student Law Review 14-26.
9. J. Gurney, 'Sue My Car Not Me: Products Liability and Accidents Involving Autonomous Vehicles' [2013] 2 U. Ill. J.L. Tech. & Pol'y 247-277.
10. J. Wolber, 'Opening a Can of Worms and Viruses: The Impact of E-Service on E-Mail Users Everywhere' [2016] 61 N.Y.L.Sch.L.Rev. 449-470.
11. J.R. Zohn, 'When Robots Attack: How Should the Law Handle Self Driving Cars That Cause Damages?' [2015] 2 U. Ill. J.L. Tech. & Pol'y 461-485.
12. K. Knapp, '#serviceofprocess @socialmedia: Accepting Social Media for Service of Process in the 21st Century' [2014] 2 La.L.Rev. 547-579.

13. K. Van Wees, ‘Vehicle Safety Regulations and ADAS: Tensions Between Law and Technology’ in X, ‘IEEE International Conference on Systems, Man and Cybernetics’ (The Hague 2004) 4011-4016.
14. R. Leenes et al, ‘Regulatory challenges of robotics: some guidelines’ [2017] 9 L.I.T. 1-44.
15. S. Ward, ‘Our Pleasure to Serve You: More Lawyers Look to Social Networking Sites to Notify Defendants’ [2011] 97 A.B.A.J. 14-16.

Case law

1. U.S. Supreme Court, Mullane v. Central Hanover Bank & Trust Co., 24 April 1950, 339 U.S. 306 (1950).
2. District Court for the Southern District of New York, S.E.C. v. HGI, Inc., 8 November 1999, 99 Civ. 3866, 1999 WL 1021087.
3. United States Court of Appeals, Ninth Circuit, Rio Properties, Inc. v. Rio International Interlink, 20 March 2002, 284 F.3d 1007.
4. Supreme Court of the Australian Capital Territory, MKM Capital Pty Ltd. v. Corbo & Poyser, 16 December 2008, no. SC 608.
5. Federal Magistrates Court of Australia, Byrne & Howard, 21 April 2010, [2010] FMCAfam 509.
6. Fourth District Family Court of Minnesota (Hennepin County), Jessica Mpafe v. Clarence Mpafe, 10 May 2011, no. 27-FA-11-3453.
7. District Court for the Southern District of New York, Fortunato v. Chase Bank, 7 June 2012, 2012 WL 2086950.
8. District Court for the Southern District of New York, FTC v. PCCare247 Inc., 7 March 2013, 2013 WL 841037.
9. United States District Court, Eastern District of Virginia, Alexandria Division, WhosHere, Inc. v. Gokhan Orun, 20 February 2014, 2014 WL 670817.
10. Family Court of the State of New York (County of Richmond), Noel B. v. Anna Maria A., 12 September 2014, no. F00787-13/14B, 2014 N.Y. Misc. LEXIS 4708.
11. Supreme Court of New York County, Baidoo v. Blood-Dzraku, 27 March 2015, 48 Misc 3d 309.
12. United States District Court, Eastern District of New York, Giovanni Ferrarese v. Vinda Shaw, 19 January 2016, 164 F.Supp.3d 361.

Other Sources

1. A. Davola, ‘A Model for Tort Liability in a World of Driverless Cars: Establishing a Framework for the Upcoming Technology’, 1 February 2018, 2, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3120679.
2. A. Robinson, ‘Toronto lawyer serves claim with Instagram’, 2 February 2018, http://www.canadianlawyermag.com/legalfeeds/author/alex-robinson/toronto-lawyer-serves-claim-with-instagram-15294.
3. High Level Group on the Competitiveness and Sustainable Growth of the Automotive Industry in the European Union (GEAR 2030), ‘Ensuring that Europe has the most competitive, innovative and sustainable automotive industry of the 2030s and beyond’, October 2017, 54p + Annexes.
4. N. Bowles, ‘Google self-driving car collides with bus in California, accident report says’, The Guardian, 1 March 2016,

https://www.theguardian.com/technology/2016/feb/29/google-self-driving-car-accident-california.

5. N. Boudette, ‘Fatal Tesla Crash Raises New Questions About Autopilot System’, New York Times, 31 March 2018, www.nytimes.com/2018/03/31/business/tesla-crash-autopilot-musk.html, read on 1 May 2018.

6. Tesla’s Blog, ‘A Tragic Loss’, 30 June 2016, https://www.teslamotors.com/blog/tragic-loss.

7. Written Question no. 706/88 of 5 July 1988 and Answer by Lord Cockfield on behalf of the Commission on 15 November 1988, OJ 114/42, 8 May 1989.

RISKS RELATED TO THE USE OF BLOCKCHAIN AND THE RELEVANT CRIMINAL PROTECTION OF THE CRIMINAL LAW IN LATVIA

Juris Janums[1]

Abstract

At the moment, in the recording of a transaction in the block chain there is no assessment made – whether it is good faith and whether the subject of the transaction is legal. Nor is the question of what data and in how wide peer-to-peer computer network to store. Thus, in his publication, the author to the described issues offers a view on criminal law protection of the use of a blockchain in Latvia, looking at issues such as the theft of financial identity, the protection of information to be transmitted, personal data, other data in the block chain as a subject of crime, as well as fraud cases related to the use of a blockchain and individual issues regarding criminally acquired or related to it property in the block chain. As a result, the author identifies some shortcomings and raises the question of the need to consider individual amendments to the Criminal Law in Latvia.

Keywords: Blockchain, object of a criminal offence, smart contracts, criminal law

Introduction

"Blockchain is a data structure that is used to create a digital transaction ledger that, instead of resting with a single provider, is shared among a distributed network of computers. The result is a more open, transparent, and publicly verifiable system for digital transactions."[2] Although there are other explanations of the term of the blockchain, but their differences just seems different and they all contains the signs of the blockchain: "1) Structured data system (register or so called ledger); 2) Contains information related to bilateral or multilateral transactions (incl. *bitcoin, cryptocurrency* and other transactions); 3) Being stored in a single distributed network of computers (*Peer-to-peer*)."[3]

One of the most common applications of blockchain technology is cryptocurrency.[4] It has been recognized in the legal literature, that "cryptocurrency is a commodity with a certain value, which is also a means of exchange, that encrypted with cryptographic

[1] PhD student at University of Latvia, Faculty of Law. Research interests include legal aspects of cryptocurrency in criminal law, cybercrime and computer related crime

[2] Database of Academy of Science of Latvia, http://termini.lza.lv/term.php?term=blokķēde&list=blokķēde &lang=LV, accessed on March 24, 2019

[3] J. Janums, 'Blokķēdes krimināltiesiskās aizsardzības aspekti.' [2019] LU 77. starptautiskās zinātniskās konferences rakstu krājums

[4] Blockchain Top Trends In 201, https://channels.theinnovationenterprise.com/articles/blockchain-top-trends-in-2017, accessed on March 24, 2019

methods is being kept in blockchain in memory of computer systems."[5] Thereby, cryptocurrency as a blockchain technology is potentially one of the most threatened blockchain technologies.

However, the technology of the blockchain in the field of information technology is increasingly being introduced in other applications, that are not related to a cryptocurrency. For example, an international information technology corporation "International Business Machines Corporation" (IBM) in September 2016 informed, that global banks and other financial institutions introduce blockchain technology in financial services systems faster as it was originally expected.[6] Similarly, the International Monetary Fund, in its January 2016 study, was focusing on the issues of smart contracts as a future form of transactions.[7] Furthermore in the legal periodicals, the digitized land registry[8] and even digitized arbitration process[9] stored in the blockchain has been already described.

Thus, due to the significant use of blockchain technology in the field of cryptocurrency, smart contracts, transactions and financial services, as well as in other areas, the question arises – whether the Criminal Law in Latvia contains the necessary criminal legal protection for the cases of block chain threats identified by the author previously[10] – i.e. with the existence and use of the blockchain related threats?

1. Legal threats related to use of the blockchain

One of the first threats blockchain technology developers name are the risks to the infrastructure necessary to the existence of the blockchain itself.[11] Since one of the features of the blockchain is that the system stores data in a decentralized network of distributed computers, thus - endangering the operation of the network and the operation of the computers in it, especially their availability to the computer network, threatens the blockchain itself.[12] Likewise, the operation of the blockchain system requires a stable computer operation, so also the operation of the computers in the blockchain itself is a threat object.[13] Thus, assessing the risks of the existence of a blockchain, it is necessary to analyze the related legal protection of computer and computer networks.

[5] J. Janums, 'Jaunas kriptovalūtas emisija un tās kolektīvās finansēšanas krimināltiesiskie aspekti.'[2018] LU 76. starptautiskās zinātniskās konferences rakstu krājums 417

[6] J. Kelly, Banks adopting blockchain 'dramatically faster' than expected: IBM, https://www.reuters.com/article/us-tech-blockchain-ibm-idUSKCN11Y28D, accessed on March 24, 2019

[7] IMF staff discussion note. Virtual Currencies and Beyond: Initial Considerations. January, 2016, SDN/16/03, https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf , accessed on March 24, 2019

[8] S. Lidere S., 'Digitalizēts zemesgrāmatu reģistrs, kas balstīts uz blokķēdes darbības principiem', [2018] 47 (1053) Jurista Vārds

[9] L.L.Rieba, 'Blokķēdes tehnoloģijā balstīts šķīrējtiesas process', [2018] Jurista Vārds 47 (1053) Jurista Vārds

[10] J. Janums, 'Blokķēdes krimināltiesiskās aizsardzības aspekti.' [2019] LU 77. starptautiskās zinātniskās konferences rakstu krājums

[11] Bitcoin Developer Guide, https://bitcoin.org/en/developer-guide , accessed on March 24, 2019

[12] J. Janums, 'Blokķēdes krimināltiesiskās aizsardzības aspekti.' [2019] LU 77. starptautiskās zinātniskās konferences rakstu krājums

[13] Ibid.

The second - legally much wider - range of threats is related to the use of block chain technologies, where, based on publications by industry experts[14], the main issues would be related to the nature and availability of information to be kept in the blockchain. Accordingly, for example:

1) In the secure blockchain – sequential transaction records system – an illegal transaction is being recorded – it is understood to mean both transactions where the object of which is not permitted, such as drugs being bought at the *Dark Net / Dark Web* (dark net – peer-to-peer network with mutually limited and anonymous access)[15], or transactions related to money laundering, such as fraud, embezzlement and other illicit activities, for example bribe or illegal financing of political parties;

2) In the secure blockchain personal data is being stored and subsequently processed in the manor that violates a person's right to privacy, which is furthermore stored on an unlimitedly distributed computer network.[16]

2. Legal protection of the blockchain in Criminal Law in Latvia

Taking into account the identified threats associated with the operation of the blockchain, for the protection of the interests of the operation of the blockchain in the Criminal Law in Latvia, we can mainly distinguish such groups of offenses:

1. Criminal offenses in the security of information systems – as the criminal offenses provided for in the Criminal Law as regards the existence of the blockchain itself,

In turn, with regard to the nature and availability of information to be kept in the block chain, we can talk about such groups of criminal offenses:

2. Criminal Offences against Fundamental Rights and Freedoms of a Person,
3. Criminal Offences against Property, and
4. Criminal Offences in the field of Finance and Credit.[17]

2.1. Criminal offenses in the area of security of information systems regarding the existence of a blockchain itself

Criminal offenses in the area of security of information systems are included in the Criminal Law Chapter XX “Criminal Offences against General Safety and Public Order” and they are united by a common threat – group object – the general interest of security of the society. Thereby, taking into account, for example, data from the “*coinmarketcap.com*”, where you can keep online track of changes in the value of more than 2'000 crypto currencies, the total value of cryptocurrency market at the moment (March 2019) has

[14] K. Iesalnieks, Blokķēdes tehnoloģija – mīti un patiesība par kriptorevolūciju, https://www.delfi.lv/news/versijas/kaspars-iesalnieks-blokkedes-tehnologija-miti-un-patiesiba-par-kriptorevoluciju.d?id=49522737 , accessed on March 24, 2019

[15] Database of Academy of Science of Latvia, therm: Darknet, http://termini.lza.lv/term.php?term=darknet&lang=EN and https://en.oxforddictionaries.com/definition/darknet , accessed on March 24, 2019

[16] J. Janums, ‘Blokķēdes kriminālatiesiskās aizsardzības aspekti.’ [2019] LU 77. starptautiskās zinātniskās konferences rakstu krājums

[17] Ibid.

reached more than 120 milliard euros[18], as well as taking into account IBM observations on the widespread use of blockchain technologies in the field of financial services[19], it can be concluded that the use of blockchain technology at present and potentially in the future is very wide. Thereby based on the mentioned above, and taking into account one of the features of the blockchain technology – i.e., its existence on a wide spread computer network, – the threat of the existence of a blockchain technology could jeopardize the general security interests and corresponds to the group object of interest of Chapter XX of the Criminal Law. Among other things, this is also confirmed by the example of the Estonian Central Depository "Nasdaq Estonia", where in the end of the 2016 they've successfully tested the blockchain technology in a electronic vote by shareholders meeting in an electronic environment, and it was recognized by the Stock Exchange as a sufficiently reliable, safe and usable technology for organizing general meetings of shareholders.[20]

However, looking at the specific criminal offenses, united by common threat object - Information Systems Security -, such as Arbitrary Access to Automated Data Processing System Pursuant to Section 241 of the Criminal Law, Interference of Operation of Automated Data Processing System Pursuant to Article 243 of the Criminal Law and Illegal Operations of Information Included in this System, Illegal Activities with Influential Devices Influenced pursuant to Section 244 of the Criminal Law, the acquisition, production, modification, storage and distribution of data, software and equipment provided for pursuant to Section 244.1 of the Criminal Law, as well as violation of the security rules of the information system provided for in Section 245 of the Criminal Law, we can observe, that the criminal offenses listed provide criminal protection for each element of the centralized computer system and for the system as a whole, but for the blockchain – as a decentralized peer-to-peer system – it is much more difficult to apply such sections of law.

For example, in the case of a centralized system, we can talk about a computer system where all information is centrally located in the memory of some computers (servers - network computers) with a single protection system, except for global information technology companies, which in one way or another, nevertheless, keeps different information in their dispersed centralized systems, it in different places in the world[21]. While, for example, in the case of cryptocurrency, the number of computers involved in the blockchain maintenance is measured in millions and stores all information in a single decentralized system. For example, as shown by the numbers of sells of the processors used for cryptocurrency mining in year 2017 more than 3 million units were sold[22]. So the size of the computers involved in the blockchain for providing a cryptocurrency system is measurable in millions. Moreover, unlike the centralized system architecture, where destroying any of its elements endangers the system as a whole, in case of a blockchain, to paralyze it, almost all the computers involved in the block chain should be destroyed, because each of the computers stores information about the entire system database, and

[18] Cryptocurrencies by Market Capitalization, https://coinmarketcap.com/, accessed on March 24, 2019

[19] J. Kelly, Banks adopting blockchain 'dramatically faster' than expected: IBM, https://www.reuters.com/article/us-tech-blockchain-ibm-idUSKCN11Y28D , accessed on March 24, 2019

[20] Nasdaq's Estonia E-voting Blockchain Solution, https://business.nasdaq.com/marketinsite/2017/Is-Blockchain-the-Answer-to-E-voting-Nasdaq-Believes-So.html, accessed on April 15, 2019

[21] Google Data Centers, https://www.google.com/about/datacenters/inside/locations/index.html , accessed on April 15, 2019

[22] GPU market declined seasonally in Q4; cryptocurrency provides smaller offset as AIB prices rise, https://www.jonpeddie.com/press-releases/gpu-market-declined-seasonally-in-q4-cryptocurrency-provides-smaller-offset, accessed on April 15, 2019

thereby it is almost impossible to destroy.[23] Hence, damage to a single computer system (element) in a centralized system is more severe than damage to one computer from a million in a blockchain. Among the other things, it is often referred to in the various publications as one of the advantages of the blockchain technology.

It is therefore right to ask a question here – or, in the case of a threat to the computer system in the block chain, one can speak at all – of existence of an criminal offence – against the safety of the block chain operation? And, if we even refer to the criminal offenses currently provided for in the Criminal Law, are liability there isn't overly strict?

For example, currently disrupting the operation of an automated data processing system and unlawful action with information included in this system (Section 243 of Criminal Law) in accordance with Section 7, Paragraph three of the Criminal Law shall be considered a less serious crime (i.e. imprisonment for up to 2 years), but if a greedy intention has been identified (Section 243 Paragraph three of the Criminal Law), even as a serious crime (i.e. a sanction for imprisonment of up to 5 years).

But in the case of a blockchain – as mentioned above – technology itself excludes the possibility of manipulating the validity of the data contained therein, because every computer in the system keeps the system's current mirror image (copy), which at the same time completely eliminates the possibility of interfering with the operation of the blockchain system as a whole, compromising only one or a part of the system computers. Thereby interference of the blockchain in general is almost impossible, hence, compromising the small number of computers or a single computer in the blockchain, the qualifying characteristic of Article 243 of the Criminal Law does not materialize – i.e. interference of the operation of the system –, because as a whole, the system still continues to operate. But, if however, Article 243 of the Criminal Law is being applied in the case of a interference of a single computer in the blockchain, then, taking into account that the block chain still continues to operate, is a less serious crime shall not be considered as too severe classification for such criminal offence?

From the author's point of view, the problem of such regulation of the Criminal Law is related to it, for what kind of information technology architecture and industry rules the relevant norms were developed at the time of their adoption, because at that time no one predicted that once a group of people under the pseudonym Satoshi Nakamoto would offer the world a blockchain technology[24].[25]

2.2. Criminal Offenses related to the use of the block chain

Offenses related to the use of the blockchain are mainly related to the nature and availability of information to be stored in the blockchain, where the author considers Criminal Offences against Fundamental Rights and Freedoms of a Person (Chapter XIV of The Criminal Law), Criminal Offences against Property (Chapter XVIII of The Criminal Law) and

[23] A. Dorri, M.Steger, S.S.Kanhere, R.Jurdak, 'BlockChain: A Distributed Solution to Automotive Security and Privacy' [2017] 12/55 IEEE Communications Magazine

[24] S.Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, accessed on March 24, 2019

[25] J. Janums, 'Blokķēdes krimināltiesiskās aizsardzības aspekti.' [2019] LU 77. starptautiskās zinātniskās konferences rakstu krājums

criminal offences in the field of finance and credit (Chapter XIX of The Criminal Law).[26]

So, when evaluating what data, how widely distributed computer network to store, and how to transfer and store them, it is reasonable to consider the criminal offenses provided in Chapter XIV of the Criminal Law, i.e. criminal offences against the fundamental rights and freedoms of the person, for example, such as Section 144, which provides for criminal liability for breach of the confidentiality of information transmitted over electronic communications networks and Section 145 of The Criminal Law, where criminal liability is provided for the illicit actions involving personal data. Initially looking at these offenses, the author has previously identified both the challenges of the General Data Protection Regulation[27] and relate to it Section 145 of The Criminal Law. For example, what is the subject of a criminal offense in the case of breach of the confidentiality of information transmitted over electronic communications networks in case of "Monetizr", a Latvian startup registered in the US, that stores in a blockchain information about computer games players gaming habits in the US, and afterwards offers its to a computer games distributors and makers[28], or data on voters' political views, as it happened in the scandal of *Cambridge Analytica*[29], when such information was illegally transferred to political consulting companies.[30] However, given the features of the blockchain technology described above, In the case of Article 144 of the Criminal Law it would be reasonable to ask a question, or the responsibility for the offenses contained therein could be at all, because the data in the blockchain is stored in the secure form of encryption. Thus, even if intercepted, they would not be usable, as long as the criminals do not have the user key (code), with which you can process encrypted information – incl. to read it. Thus, in relation to the criminal protection of correspondence as information on the blockchain could only be referred to as unfinished crimes. – i.i. their attempts – and only in very rare cases as completed crimes – as already mentioned, if the criminal has a decryption key (code). In contrast, the main issue with the composition of the criminal offense under Article 145 of the Criminal Law, that could be related to the blockchain, is the nature of the data stored in the blockchain – i.e. what information should be kept in a publicly accessible and simultaneously encrypted block chain (i.i. to process). Likewise, no less important issue is related to the criminal protection in the space, but it is more of a jurisdictional issue that will not be dealt with this time. Thus the qualifying characteristics of Article 145 of the Criminal Law are the violation of a person's private life, which has caused significant damage. However, as the Supreme Court of the Republic of Latvia rightly admits: "Not every violation of the rights guaranteed by the Republic of Latvia Satversme [Constitution] itself, without the evaluation of the violation, shall be considered a significant damage within the meaning of Article 23 of the Law "On the Procedure of Entry into Force and Application of the Criminal Law". Significant damage shall be determined on the basis of evidence verified by the court, assessing the nature, content,

[26] Ibid.

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

[28] T. Zoldnere, Latvieši Silīcija ielejā: ar blokķēdes tehnoloģiju pēta datorspēlētājus, https://www.delfi.lv/bizness/tehnologijas/latviesi-silicija-ieleja-ar-blokkedes-tehnologiju-peta-datorspeletajus.d?id=50818225, accessed on March 24, 2019

[29] Ted Cruz using firm that harvested data on millions of unwitting Facebook users, https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data, accessed on March 24, 2019

[30] J. Janums, 'Blokķēdes krimināltiesiskās aizsardzības aspekti.' [2019] LU 77. starptautiskās zinātniskās konferences rakstu krājums

interest bearer, or the nature of the person at risk, and the attitudes towards the particular risk."[31] Therefore, the answer to the question - what information should be stored (i.e. processed) in a publicly available and at the same time encrypted blockchain system depends on the data subject's own attitude to the risk of the particular interest and should be assessed on a case-by-case basis.

In turn, considering that the block chain can hold both the property itself and the right to such property, it is reasonable to look at the criminal offenses in Chapter XVIII of the Criminal Law against property. Such as The regulation of theft provided for in Article 175 of the Criminal Law, the regulation of fraud provided for in Article 177 of the Criminal Law, the regulation of fraud in the automated data processing system provided for in Article 177.1 of the Criminal Law, as well as the regulation of misappropriation provided for in Article 179 of The Criminal Law.[32] Hence it is possible to immediately spot the characteristics of the blockchain, such as that it is not possible to steal the blockchain record as a property value itself, therefore, the Article 175 of The Criminal Law regarding the theft would not apply to it.

Similarly, the essence of the blockchain technology excludes false data entry to affect the block chain, as the block chain system allows recording only after the automated system has verified the accuracy of the data, therefore, the Article 177.1 of The Criminal Law regarding the fraud in the automated data processing system in essence, not even relevant to the blockchain. Conversely, in order to record a transaction in a block chain, an encryption key is required – which can be considered as an access right for each specific record – then you could reasonably talk about fraud. Here, however, there is the question of financial identity theft and its association with fraud (Section 177 of The Criminal Law). You can also talk about fraud with system keepers, who by "mining" upkeeps the blockchain, such as company "BitFury", who receive a reward in a cryptocurrency for a "mining" and whose value is 400 million. USD[33] (Section 177 of The Criminal Law). Lastly, as with fraud, embezzlement can also be considered, for example, from the encryption key (code) providers and keepers (Section 179 of The Criminal Law)[34].[35]

Finally, although the legal definition of cryptocurrency in Article 2.2 of the Law on the Prevention of Money Laundering and the Financing of Terrorist Financing paragraph 2.2[36], as the legislator has clearly stated in Latvia, that it is a reflections of a value, but not the legal means of payment, at the same time in the light of the criminal offenses provided in The Chapter XIX of the Criminal Law in the field of Finance and credit, could expand the discussion on the cryptocurrency stored in the blockchain as the subject of Article 193 of the Criminal Law, because, as it is well known you can pay for goods and services by the cryptocurrency like as by legally defined means of payment. In addition, it would be worthwhile to discuss the data in the blockchain as such, and it would be reasonable to ask

[31]The decision of the Supreme Court of The Republic of Latvia of 29.09.2016. in case № SKK-190/2016 (11816003310), http://www.at.gov.lv/downloadlawfile/3640 , accessed on March 24, 2019

[32] J. Janums, 'Blokķēdes krimināltiesiskās aizsardzības aspekti.' [2019] LU 77. starptautiskās zinātniskās konferences rakstu krājums

[33] Bitcoin company made by Rigans valued at $400m, https://eng.lsm.lv/article/economy/economy/bitcoin-company-made-by-rigans-valued-at-400m.a261722/ , accessed on March 24, 2019

[34] J. Janums, 'Jaunas kriptovalūtas emisija un tās kolektīvās finansēšanas krimināltiesiskie aspekti.'[2018] LU 76. starptautiskās zinātniskās konferences rakstu krājums 417

[35] J. Janums, 'Blokķēdes krimināltiesiskās aizsardzības aspekti.' [2019] LU 77. starptautiskās zinātniskās konferences rakstu krājums

[36]Amendments of 26.10.2017. to a Law on the Prevention of Money Laundering and the Financing of Terrorist Financing of the Republic of Latvia, https://likumi.lv/ta/id/294868-grozijumi-noziedzigi-iegutu-lidzeklu-legalizacijas-un-terorisma-finansesanas-noversanas-likuma, accessed on March 24, 2019

the question - whether theft or the stealing of the payment instrument from the blockchain would be realistic or have a different objective expression. It would also be reasonable to ask the question about Article 193.1 of the Criminal Law – regarding the acquisition, production, distribution, use and storage of data, software and equipment for illegal activities with financial instruments and means of payment, not only the question of obtaining access data for cryptocurrency wallet with encryption keys, but also with regard to software aimed at destroying, blocking and, in this case, competing with the provisions of the offense referred to in Section 244 of the Criminal Law.[37] In the view of the author, the value of the cryptocurrency as an element of the blockchain with the property value is to be recognized as a means of payment within the meaning of Article 193 of the Criminal Law.[38] Thus, taking into account, for example, the size of the cryptocurrency market, it would be reasonable to consider whether the liability for the risks is high enough, or whether it would be necessary to supplement the Criminal Code with the financial and credit composition of the offenses that would also include liability for special entities. That provides the circulation of specific blockchain technology data to its users, such as cryptocurrency developers or cryptocurrency exchange keepers. For example, the news about the cryptocurrency exchange "QuadrigaCX", which is the largest cryptocurrency exchange in Canada, has recently alarmed the world, when its main developer died, the access to property – in electronic form – with value of 190 million USD is being lost, because only the developer alone knew encrypted access code to those transactions.[39] Thus, the legislator should consider the need to regulate security requirements in the relevant sphere and to provide for such cases responsibility in the Criminal Law.

Conclusions

[1] The threat to the existence of blockchain technology is consistent with the threat to the general security interests and hence corresponds to the interest of the group protected under Chapter XX of the Criminal Law.

[2] Damage to a single computer system (element) in a centralized system is significantly more severe than the damage that can be caused to one computer from a million in the blockchain system.

[3] Interference of some of the computers in the blockchain system does not damage the operation of the blockchain, hence the qualifying feature of Article 243 of the Criminal Law – interference of the operation of the systems – does not occur, because in this case the system continues to operate as a whole.

[4] Offenses related to the use of the blockchain are mainly related to the nature and availability of the information to be kept in the blockchain.

[5] As regards the criminal protection under Article 144 of the Criminal Law of correspondence as information on the blockchain, could only be referred to as an unfinished crimes – i.i. their attempts – and only in very rare cases as completed crimes – i.e. in cases if the criminal has a decryption key (code).

[6] The question of what information should be stored (i.e. processed) in a publicly available and at the same time encrypted blockchain depends on the data subject's own

[37] J. Janums, 'Blokķēdes krimināltiesiskās aizsardzības aspekti.' [2019] LU 77. starptautiskās zinātniskās konferences rakstu krājums

[38] Ibid.

[39] Cryptocurrency investors locked out of $190m after exchange founder dies, https://www.theguardian.com/technology/2019/feb/04/quadrigacx-canada-cryptocurrency-exchange-locked-gerald-cotten, accessed on March 24, 2019

attitude to the risk of the particular interest and should be assessed on a case-by-case basis.

[7] Thus, the legislator should consider the need to regulate security requirements in the sphere of cryptocurrency developers and cryptocurrency exchange keepers, and provide for such cases necessary responsibility in the Criminal Law, which is not currently provided for in the Criminal Law.

Bibliogaphy

1. A.Dorri, M.Steger, S.S.Kanhere, R.Jurdak, 'BlockChain: A Distributed Solution to Automotive Security and Privacy' [2017] 12/55 IEEE Communications Magazine
2. Amendments of 26.10.2017. to a Law on the Prevention of Money Laundering and the Financing of Terrorist Financing of the Republic of Latvia, https://likumi.lv/ta/id/294868-grozijumi-noziedzigi-iegutu-lidzeklu-legalizacijas-un-terorisma-finansesanas-noversanas-likuma, accessed on March 24, 2019
3. Bitcoin company made by Rigans valued at $400m, https://eng.lsm.lv/article/economy/economy/bitcoin-company-made-by-rigans-valued-at-400m.a261722/ , accessed on March 24, 2019
4. Bitcoin Developer Guide, https://bitcoin.org/en/developer-guide , accessed on March 24, 2019
5. Blockchain Top Trends In 201, https://channels.theinnovationenterprise.com/articles/blockchain-top-trends-in-2017, accessed on March 24, 2019
6. Cryptocurrencies by Market Capitalization, https://coinmarketcap.com/, accessed on March 24, 2019
7. Cryptocurrency investors locked out of $190m after exchange founder dies, https://www.theguardian.com/technology/2019/feb/04/quadrigacx-canada-cryptocurrency-exchange-locked-gerald-cotten, accessed on March 24, 2019
8. Database of Academy of Science of Latvia, http://termini.lza.lv/term.php?term=blokķēde&list= blokķēde &lang=LV, accessed on March 24, 2019
9. Database of Academy of Science of Latvia, therm: Darknet, http://termini.lza.lv/term.php?term=darknet&lang=EN and https://en.oxforddictionaries.com/definition/darknet , accessed on March 24, 2019
10. Google Data Centers, https://www.google.com/about/datacenters/inside/locations/index.html , accessed on April 15, 2019
11. GPU market declined seasonally in Q4; cryptocurrency provides smaller offset as AIB prices rise, https://www.jonpeddie.com/press-releases/gpu-market-declined-seasonally-in-q4-cryptocurrency-provides-smaller-offset, accessed on April 15, 2019
12. IMF staff discussion note. Virtual Currencies and Beyond: Initial Considerations. January, 2016, SDN/16/03, https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf , accessed on March 24, 2019
13. J. Janums, 'Blokķēdes kriminālatiesiskās aizsardzības aspekti.' [2019] LU 77. starptautiskās zinātniskās konferences rakstu krājums

14. J. Janums, ‘Jaunas kriptovalūtas emisija un tās kolektīvās finansēšanas krimināltiesiskie aspekti.’[2018] LU 76. starptautiskās zinātniskās konferences rakstu krājums 417
15. J. Kelly, Banks adopting blockchain 'dramatically faster' than expected: IBM, https://www.reuters.com/article/us-tech-blockchain-ibm-idUSKCN11Y28D, accessed on March 24, 2019
16. K. Iesalnieks, Blokķēdes tehnoloģija – mīti un patiesība par kriptorevolūciju, https://www.delfi.lv/news/versijas/kaspars-iesalnieks-blokkedes-tehnologija-miti-un-patiesiba-par-kriptorevoluciju.d?id=49522737 , accessed on March 24, 2019
17. L.L.Rieba, ‘Blokķēdes tehnoloģijā balstīts šķīrējtiesas process’, [2018] Jurista Vārds 47 (1053) Jurista Vārds
18. Nasdaq’s Estonia E-voting Blockchain Solution, https://business.nasdaq.com/marketinsite/2017/Is-Blockchain-the-Answer-to-E-voting-Nasdaq-Believes-So.html, accessed on April 15, 2019
19. Regulation (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1 (General Data Protection Regulation)
20. S. Lidere S., ‘Digitalizēts zemesgrāmatu reģistrs, kas balstīts uz blokķēdes darbības principiem’, [2018] 47 (1053) Jurista Vārds
21. S.Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, accessed on March 24, 2019
22. T. Zoldnere, Latvieši Silīcija ielejā: ar blokķēdes tehnoloģiju pēta datorspēlētājus, https://www.delfi.lv/bizness/tehnologijas/latviesi-silicija-ieleja-ar-blokkedes-tehnologiju-peta-datorspeletajus.d?id=50818225, accessed on March 24, 2019
23. Ted Cruz using firm that harvested data on millions of unwitting Facebook users, https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data, accessed on March 24, 2019
24. The decision of the Supreme Court of The Republic of Latvia of 29.09.2016. in case № SKK-190/2016 (11816003310), http://www.at.gov.lv/downloadlawfile/3640 , accessed on March 24, 2019

THE USE OF BLOCKCHAIN TECHNOLOGY AS A NEW METHOD OF RECORDING LAND TRANSACTIONS

Maria Kaczorowska[1]

Abstract

Blockchain, which is a type of distributed ledger of digital records based on cryptographic techniques and operating within a peer-to-peer network, is gaining importance in various fields of economy and in the public sector. Taking into account the basic idea of distributed ledger technology underlying blockchain, one of its applications is supposed to be maintaining public registers, including land registers. In fact, currently blockchain is under consideration by governments or is already being utilised in the area of land registration in several countries. The innovative role of blockchain technology in improving land registration systems is considered to consist mainly in increasing trust, security and processing efficiency as well as cost reduction.

However, given the specific character and complexity of land transactions, it appears doubtful whether indeed the blockchain concept proves adequate for the purpose of registering rights over immovable property. This is particularly due to the fact that, according to the assumptions, transactions in blockchain shall be carried out without intermediaries, i.e. without any external verification of accuracy of the data to be registered, and the recordation of a transaction shall be irreversible. Such a solution does not seem to comply with the principal functions of land registers which play a crucial role in guaranteeing legal certainty of land transactions thanks to the involvement of professional operators such as notaries and registrars.

This paper aims to analyse how blockchain technology can be adapted to the existing land registration systems in order to effectively streamline their functioning with the essential legal requirements regarding the security of land transfer being met. An illustration of the current tendencies in this respect are practical experiences in developing blockchain-based land registers in selected jurisdictions.

Keywords: blockchain, recordkeeping, land registers, land transactions

Introduction

Along with the progressing technological development new solutions are being proposed to facilitate market transactions and modernise public administration while ensuring an adequate level of security in conditions of increasingly automated legal

This paper has been prepared within the research project 'Informatisation of land and mortgage registers', supported financially by the Polish National Science Centre (no. 2015/17/B/HS5/00460).

[1] Assistant professor, Research Centre for Legal and Economic Issues of Electronic Communication, Faculty of Law, Administration and Economics, University of Wrocław, e-mail: maria.kaczorowska@uwr.edu.pl.

relationships. Currently, disruptive significance as regards enhancing processing efficiency, transparency and certainty in different sectors of economic activity as well as public services is attributed to blockchain technology. The idea of blockchain – as a distributed database (a distributed ledger) utilising cryptographic techniques to store digital data and guarantee their integrity – favours its potential multidirectional application, including the improvement of functioning of public registers[2]. Great interest is focused on the perspective of using blockchain systems in the area of land registration which is also reflected in pilot projects undertaken in many countries around the world, in some cases already completed. Possible applications of blockchain technology in real estate market are also under consideration by the Polish government.

Postulates to apply blockchain on a wide scale in real estate transactions and transform land registers into distributed databases should nevertheless be confronted with the complexity of rules governing land transfer and basic functions of land registration systems, aimed at disclosing the legal status of the property. In this respect, it is worth emphasising that land registers play a key role in assuring certainty and security of conveyancing and mortgage lending which is connected with the involvement of professionals such as registrars, notaries, other specialised lawyers, real estate agents and bankers. The blockchain concept, in contrast, envisages that any two willing parties can transact directly to each other within a peer-to-peer network, without the need of intervention of intermediaries to authorise the transaction. What is more, once recorded on the digital ledger, the transactions shall be irreversible and unalterable. On one hand, it seems that such a mechanism can offer increased efficiency and inviolability of the system, but on the other hand the accuracy of registered data and, consequently, trust to the content of the register are not guaranteed in the absence of an independent verification. The above inconsistencies give rise to questions whether indeed blockchain technology is compatible with the process of recording rights to land, especially in view of its considerable socio-economic relevance as well as importance for the territorial integrity of a state.

The aim of the present contribution is to identify both potential advantages and some legal problems connected with the vision of blockchain-based land registers and then discuss practical experiences of selected countries in testing and introducing blockchain for the purpose of land registration which will serve as a point of reference for the assessment of the possibilities of adapting this innovative technology to specific requirements regarding real estate transactions. In this context, progress already achieved in the field of

[2] M. Hulicki, P. Lustofin, 'Wykorzystanie koncepcji blockchain w realizacji zobowiązań umownych' [2017] 1 Człowiek w Cyberprzestrzeni 37–39; B. Klinger, J. Szczepański, 'Blockchain – historia, cechy i główne obszary zastosowań' [2017] 1 Człowiek w Cyberprzestrzeni 18 ff.; K. Zacharzewski, K. Piech (eds.), 'Przegląd polskiego prawa w kontekście zastosowań technologii rozproszonych rejestrów oraz walut cyfrowych. Stanowisko Strumienia w sprawie kierunków ewentualnych prac legislacyjnych oraz działań regulacyjnych instytucji publicznych' [2017], https://www.gov.pl/documents/31305/52168/przeglad_polskiego_prawa_w_kontekscie_zastosowan_technologii_rozproszonych_rejestrow_oraz_walut_cyfrowych.pdf/f6e74ce0-09e5-776d-bd3b-c21fca96cce2, accessed 19 March 2019, 13 ff.; S. Nascimento, in: P. Boucher, S. Nascimento, M. Kritikos, 'How Blockchain Technology Could Change Our Lives: In-Depth Analysis' (Brussels: European Parliament Research Service 2017) 18 ff.; S. Young, 'Changing Governance Models by Applying Blockchain Computing' [2018] 26(2) The Catholic University Journal of Law & Technology 1 ff.; R. Herian, 'Legal Recognition of Blockchain Registries and Smart Contracts' [2018], https://www.researchgate.net/profile/Robert_Herian/publication/329715394_Legal_Recognition_of_Blockchain_Registries_and_Smart_Contracts/links/5c389e61299bf12be3bfcb67/Legal-Recognition-of-Blockchain-Registries-and-Smart-Contracts.pdf?origin=publication_detail, accessed 19 March 2019, 24 ff.; A. Third, K. Quick, M. Bachler, J. Domingue, 'Government Services and Digital Identity' [2018], https://www.eublockchainforum.eu/sites/default/files/research-paper/20180801_government_services_and_digital_identity.pdf, accessed 19 March 2019, 16 ff.

informatisation of land registration systems in particular jurisdictions should also be considered.

1. General characteristics and typology of blockchain

The idea behind blockchain is to use computer networks and algorithms in order to ensure credibility of transactions between parties who have no particular confidence to each other. This is why blockchain is defined as "a machine for creating trust"[3]. Originally, blockchain has been applied for the purpose of Bitcoin, a cryptocurrency offering a possibility to carry out online payments directly from one party to another without going through financial institutions (trusted third parties)[4].

Blockchain operates as an encrypted shared database designed to maintain a continuously growing list of transaction records called blocks which are linked together, creating an unbreakable chain. Each block contains a timestamp and a reference to a previous block, i.e. a unique identifier known as hash. It results in making any change of a single transaction impossible without modifying subsequent blocks. The immutable data structure used by the digital ledger is globally viewable by every participant in the underlying peer-to-peer network. Transactions to be entered to blockchain are subject to verification performed by users called miners, without the intervention of a central authority. The activity of miners is based on the consensus mechanism which requires that transactions should obtain approval of the network participants. A consensus is reached when the majority of active miners, holding at least 51% of the computing power, agree to an update in the blockchain[5].

Characteristic to blockchain system is that the collected information about transactions is not held by one entity but distributed across nodes, i.e. computers connected to the network which theoretically are unlimited in number and can operate from any location. No single user is able to manipulate the data because usually each node retains a copy of the history of transactions and the copies should match exactly. Integrity and authenticity of records is ensured thanks to the application of asymmetric encryption, based on digital signatures using public and private keys[6].

---

[3] J. Berkley, 'The Trust Machine' [31 October 2015] The Economist, https://www.economist.com/leaders/2015/10/31/the-trust-machine, accessed 27 March 2019.

[4] M. Hulicki, P. Lustofin, op. cit. 31 ff.; B. Klinger, J. Szczepański, op. cit. 11 ff.; A. Żuwała, 'Możliwości wykorzystania technologii Blockchain' [2018] 87 Studies & Proceedings of Polish Association for Knowledge Management 58 ff.; S. Nakamoto, 'A Peer-to-Peer Electronic Cash System' [2008], https://bitcoin.org/bitcoin.pdf, accessed 25 March 2019; J.M. Sklaroff, 'Smart Contracts and the Cost of Inflexibility' [2017] 166(1) University of Pennsylvania Law Review 268 ff.; A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, 'Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction' (Princeton and Oxford: Princeton University Press 2016) 65 ff.; K. Werbach, 'Trust, But Verify: Why the Blockchain Needs the Law' [2018] 33 Berkeley Technology Law Journal 491 ff.

[5] A. Walch, 'The Path of the Blockchain Lexicon (and the Law)' [2017] 36 Review of Banking & Financial Law 720–721, 739; K. Werbach, op. cit. 500 ff.; R. Thomas, 'Blockchain's Incompatibility for Use as a Land Registry: Issues of Definition, Feasibility and Risk' [2017] 6(3) European Property Law Journal 365.

[6] K. Piech (ed.), 'Leksykon pojęć na temat technologii blockchain i kryptowalut' [2016] https://www.gov.pl/documents/31305/0/leksykon_pojec_na_temat_technologii_blockchain_i_kryptowalut.pdf/77392774-1180-79ab-4dd5-089ffab37602, accessed 25 March 2019, 5 ff.; J.J. Szczerbowski, 'Lex cryptographia. Znaczenie prawne umów i jednostek rozliczeniowych opartych na technologii

As regards types of blockchain, it may be of a public or a private character. Moreover, permissioned and permissionless blockchains are distinguished. Public blockchain enables any user to join the network and participate in verifying transactions. Blockchains of this type are often permissionless as no authorisation or authentication of the participants is required and thus they remain anonymous. Access to private blockchain, on the contrary, is restricted to a specific number of authorised users, including either parties who have been privy to the creation of the register, or parties invited to participate according to the system's rules. Private blockchains correspond to the idea of permissioned ones in which participants are identified and can access the system only if they are authorised and authenticated. Permissioned blockchains are therefore considered suitable to be used within corporations, e.g. in the banking sector. Another type of blockchain, which is a combination of private and public ones, is identified as hybrid blockchain. It is characterised by the fact that only specific entities or persons can be part of the blockchain network and participate in the consensus process, but at the same time public blockchain is used in such case for accounting purposes and as a proof of existence[7].

2. Possible benefits deriving from application of blockchain in the field of land registration

As argued by the promoters of modernising land registers with the use of blockchain technology, it can bring advantages consisting primarily in lack of intermediaries, a distributed character of the system, transparency and immutability.

Firstly, blockchain – in its pure form – is considered a trustless system as it enables the parties to enter into peer-to-peer online transactions without the participation of professional facilitators such as registries, notaries, conveyancers, real estate agents and banks. Once an entry in the register is made, it becomes final so that it cannot be altered or erased without the consent of the miners which shall provide protection from tampering and thus, paradoxically, no trust shall be needed anymore. Consequently, it is assumed that bypassing intermediaries shall result in transaction cost reduction, savings in time and increased processing efficiency[8].

---

blockchain' (Warszawa: Wydawnictwo Naukowe PWN 2018) 11 ff.; D. Szostek, 'Blockchain a prawo' (Warszawa: C.H. Beck 2018) 27 ff.; V.L. Lemieux, 'Blockchain Recordkeeping: A SWOT Analysis' [2017] 51(6) Information Management 21; N. Nogueroles Peiró, E.J. Martinez García, 'Blockchain and Land Registration Systems' [2017] 6(3) European Property Law Journal 300; S.S. Shetty, C.A. Kamhoua, L.L. Nijilla, 'Introduction', in: S.S. Shetty, C.A. Kamhoua, L.L. Nijilla (eds.), 'Blockchain for Distributed Systems Security' (Hoboken: Wiley-IEEE Computer Society 2019) 4 ff.

[7] K. Piech (ed.), op. cit. 6; D. Szostek, op. cit. 49, 103 ff.; V.L. Lemieux, op. cit. 22; A. Walch, op. cit. 720; R. Thomas, op. cit. 364; G. Gabison, 'Policy Considerations for the Blockchain Technology Public and Private Applications' [2016] 189 SMU Science & Technology Law Review 330 ff.; J. Vos, 'Blockchain-Based Land Registry: Panacea, Illusion or Something in Between?' [2015] 7th ELRA Annual Publication, https://www.elra.eu/wp-content/uploads/2017/02/10.-Jacques-Vos-Blockchain-based-Land-Registry.pdf, accessed 19 March 2019, 16–19.

[8] R. Thomas, op. cit. 365–366; N. Nogueroles Peiró, E.J. Martinez García, op. cit. 319; V.L. Lemieux, op. cit. 23; M. Barbieri, D. Gassen, 'Blockchain – Can This New Technology Revolutionize the Land Registry System?' [2017], http://www.notartel.it/export/contenuti_notartel/pdf/Land_Poverty_Conference_Blockchain.pdf, accessed 19 March 2019, 3, 4; J. Vos, op. cit. 5, 10; M. Scott, 'Blockchain Technology and the Future of Land Registries' [6 May 2016], https://btcmanager.com/blockchain-technology-and-the-future-of-land-registries/, accessed 11 April 2019; M. Borak, 'Smoother, Faster, Simpler: Blockchain's Promise

Another advantage of blockchain lies in the distribution of information in different nodes which ensures better safety for the system, any attack being more difficult. Since a large number of users participate in the blockchain network, there is no single point of control and in case a part of the network fails, the other parts continue to operate. Thanks to the fact that transactions are broadcast to the blockchain network based on the consensus mechanism, the possibility to dispose of property simultaneously more than once should be eliminated. By way of comparison, when it comes to the existing electronic land registers, they commonly operate as central databases[9].

What is more, the mechanisms governing blockchain shall contribute to increased transparency. This is because all entries in the distributed database are public and can be viewed by the authorised users of the blockchain system, unless the access is restricted which is the case of private blockchains. Once added to the blockchain, every new block is available for anyone to verify its authenticity[10].

Finally, it is emphasised that the application of cryptographic techniques underlying blockchain technology enhances the integrity of the system, protecting it from manipulation for any attempt to change the information recorded can be easily detected[11].

3. Incompatibilities regarding blockchain-based land registers

When considering actual possibilities to use blockchain in the land registration sector, what should be taken into account is the high value of real estate compared to other assets and its particular importance from the socio-economic point of view[12]. This finds expression in strict requirements enshrined in law relating to transfer or establishment of real property rights, among which the involvement of notaries, assisting the parties and authenticating the transactions, needs particular attention. Most European countries (with the exception of Great Britain, Ireland and the Scandinavian countries) follow the Latin model of notariat – notaries act there as persons of public trust vested with competences to draw up agreements of transfer of real estate and the form of notarial deed is compulsory to complete the registration. In Anglo-Saxon jurisdictions, in turn, competence as regards conveyancing is conferred mainly upon specialised lawyers (solicitors)[13]. Both notaries and solicitors play an important role in the land registration proceedings as they submit applications for registration and respective documents to the land registry. Furthermore, it is

for the Real-Estate Industry' [21 December 2018], https://technode.com/2018/12/21/blockchains-promise-for-real-estate/, accessed 24 February 2019.

[9] R. Thomas, op. cit. 366; N. Nogueroles Peiró, E.J. Martinez García, op. cit. 319; M. Barbieri, D. Gassen, op. cit. 3; J. Vos, op. cit. 5; M. Scott, op. cit.

[10] R. Thomas, op. cit. 366; J. Vos, op. cit. 11.

[11] R. Thomas, op. cit. 367; V.L. Lemieux, op. cit. 22; N. Nogueroles Peiró, E.J. Martinez García, op. cit. 319.

[12] M. Barbieri, D. Gassen, op. cit. 8, 11; B. Arruñada, 'Blockchain's Struggle to Deliver Impersonal Exchange' [2018] 19 Minnesota Journal of Law, Science & Technology 78; F.P. Méndez, 'Smart Contracts, Blockchain and Land Registry' [2018], https://www.elra.eu/wp-content/uploads/2018/12/Smart-Contracts-Blockchain-and-Land-Registry-by-F-Mendez.pdf, accessed 19 March 2019, 7–8.

[13] Se e.g. P. Blajer, 'Rejestry nieruchomości – studium prawnoporównawcze' (Warszawa: C.H. Beck 2018) 183 ff.; B. du Marais, D. Marrani, (eds.), 'Legal Certainty in Real Estate Transactions: A Comparison of England and France' (Cambridge: Intersentia 2016) passim; S. van Erp, 'Cross-Border Electronic Conveyancing: Overcoming Problems with Negative and Positive Integration in European Property Law' [2012] 1(1) European Journal of Property Law 6.

essential for the reliability of land registers that they are maintained by public authorities, being either courts or administrative bodies. The scope of control function performed by the register authority depends, however, on the registration model adopted in particular legal order. In case of the title registration system (in force e.g. in Poland, England and Wales, Germany, Spain, Sweden) it is rights over land that are inscribed in the register upon prior examination of their legality, whereas under the deeds registration regime (applied e.g. in France, Italy, the Netherlands) the subject of registration are documents regarding land transactions which only have to comply with some formal requirements[14].

On this basis, it should be noted that the fundamental assumptions of the blockchain concept, fulfilled in its public variant, do not correspond with the abovementioned rules governing land registration, especially in relation to the power of the register authority to check substantive aspects of land transactions according to the rule of legality, which is the case of the title registration model. The reason is that blockchain in the original form excludes any intervention of a specialised authority and thus any external verification of the data submitted to the land register[15]. Due to disintermediation, blockchain cannot offer a legal presumption of accuracy of an entry (a presumption of validity), nor a proof of ownership because validation of a transaction performed by miners may be considered only in a technical sense and not in a legal sense. As a result, the information stored in the land register could not be regarded as reliable[16].

Another point of concern pertains to conferring priority, being an effect of both title registration and deeds registration. Under the existing land registration systems priority assigned to titles or deeds is dependent mainly on the time of application (the moment a relevant document arrives to the land registry). In case of the blockchain system, as opposed to the above precept, the order in which new blocks are added is not based on chronology of transactions received by the nodes but depends on a random act, given the assumed democratic nature of the consensus mechanism[17].

Furthermore, the issue of legal liability for errors affecting the transactions to be recorded in the blockchain-based register remains unclear. As far as traditional land registration systems are concerned, generally it is the state that bears the responsibility and a compensation is paid in case of a loss suffered due to mistakes from the land registry, while blockchain is based on the assumption that there is no single point of failure. It is suggested that the risk of mistakes or responsibility for blockchain system abuses could be incurred by the system administrator, the users of the system (collectively) or a person who

[14] For more details regarding the differences among national land registration systems, see e.g. P. Blajer, op. cit. 337 ff.; T. Stawecki, 'Rejestry nieruchomości, księgi hipoteczne i księgi wieczyste od czasów najdawniejszych do XXI wieku' [2002] 40 Studia Iuridica 167–208; L.M. Martínez Velencoso, 'The Land Register in European Law: A Comparative and Economic Analysis', in: L.M. Martínez Velencoso, S. Bailey and A. Pradi (eds.) 'Transfer of Immovables in European Private Law' (Cambridge: Cambridge University Press 2017) 3 ff.; S. Cámara Lapuente, 'Registration of Interests as a Formality of Contracts: Comparative Remarks on Land Registers within the Frame of European Private Law' [2005] 6 European Review of Private Law 798 ff.; A. Lodde, 'The European Systems of Real Estate Registration: An Overview' [2016] 1 Territorio Italia 23–42; J. Zevenbergen, 'Systems of Land Registration: Aspects and Effects' (Delft: Netherlands Geodetic Commission 2002) 47 ff.

[15] Cf. N. Nogueroles Peiró, E.J. Martinez García, op. cit. 301 ff.; B. Arruñada, op. cit. 95–96; F.P. Méndez, op. cit. 19.

[16] N. Nogueroles Peiró, E.J. Martinez García, op. cit. 315–316, 319; R. Thomas, op. cit. 375, 380 ff. See also J.J. Szczerbowski, op. cit. 42 ff.

[17] N. Nogueroles Peiró, E.J. Martinez García, op. cit. 302–305; F.P. Méndez, op. cit. 15–16, 19–20; V.L. Lemieux, op. cit. 24; J. Vos, op. cit. 11.

has derived a benefit as a result of irregular transactions[18]. However, difficulties to establish rules of liability are enhanced due to the anonymity of the participants of the network which is one of the basic features of blockchain in its pure form. According to the general idea of blockchain, although the participating users are connected to digital certificates, their identity is not revealed. Such problems could affect all the land registration systems, regardless of which model they follow. Therefore, it is postulated to use electronic IDs connected to the public keys[19]. Additionally, there would be a need to determine who could receive a public key in the blockchain and under which procedure. Furthermore, the privacy issue should not be overlooked[20].

In view of the abovementioned incompatibilities, contrary to the arguments put forward by the promoters of blockchain-based land registration, the conveyancing costs may appear to increase rather than decrease. One should take into account that the financial institutions providing services to parties may require the involvement of specialised intermediaries in the transactions as a means of hedging their risk. What is more, extended due diligence exercises and title insurances may be needed and also legal recourse should be considered indispensable. This refers among others to situations in which an encryption key is lost or stolen and it is necessary to recover the property it is associated with[21].

It seems that some of the above difficulties would be reduced when dealing with a private or a hybrid blockchain, based on cooperation among current stakeholders, i.e. registrars, notaries, conveyancers etc. It is argued, however, that in such case blockchain is not open to everyone and therefore its distributed nature is frustrated[22].

4. Using blockchain to record land transactions in practice on the example of selected countries

Actions aimed at testing the possibilities to apply blockchain in the sphere of land registration have been undertaken in such countries as the Republic of Georgia, Sweden, Estonia, Ukraine, the United Kingdom, the Netherlands, Ghana, Kenya, Nigeria, Brazil, Honduras, India, Japan and the United States of America[23]. Thus, it should be noted that innovative solutions offered by blockchain are expected to bring about advantages to both developing and advanced economies. Furthermore, a tendency can be observed that initially tests regarding the application of blockchain have started in small countries and next have been gradually implemented in the big ones.

Significant achievements in modernisation of land registration systems by implementing blockchain can be observed in the Republic of Georgia. Georgia is the first

[18] R. Thomas, op. cit. 387 ff.; N. Nogueroles Peiró, E.J. Martinez García, op. cit. 313–314; L. Gallego, 'Blockchain and Title Registration' [2016] 1 IPRA-CINDER International Review 30–31.
[19] B. Verheye, 'Real Estate Publicity in a Blockchain World: A Critical Assessment' [2017] 6(3) European Property Law Journal 458–459; J. Vos, op. cit. 14; G. Gabison, op. cit. 343 ff.
[20] B. Verheye, op. cit. 459. See also V.L. Lemieux, op. cit. 22–23; R. Herian, op. cit. 26–27.
[21] J.J. Szczerbowski, op. cit. 58–59; J.J. Szczerbowski, 'Transaction Costs of Blockchain Smart Contracts' [2018] 16(2) Law and Forensic Science 1–6; M. Barbieri, D. Gassen, op. cit. 12; J.M. Graglia, C. Mellon, 'Blockchain and Property in 2018: At the End of the Beginning' [2018], https://www.conftool.com/landandpoverty2018/index.php?page=downloadPaper&ismobile=true&filename=02-11-Graglia-864_paper.pdf&form_id=864&form_version=final, accessed 19 March 2019, 8 ff.; M. Borak, op. cit.
[22] Cf. J. Vos, op. cit. 16 ff.
[23] See e.g. R. Herian, op. cit. 41–44; A. Third, K. Quick, M. Bachler, J. Domingue, op. cit. 20 ff.

country that has started registering land titles using blockchain. What needs to be emphasised is that before introducing blockchain technology the Georgian land registration system has been reformed so that it has become relatively efficient and corruption-free[24]. The recent innovations have been introduced as a result of cooperation between the National Agency of Public Registry and a bitcoin mining company Bitfury. The land register is based on a private permissioned blockchain, administered by the National Agency of Public Registry. The scope of the implemented project covers sale of land titles, registration of new titles, mortgages, rentals and notary services[25].

In Sweden in 2016 a pilot project was launched by the Swedish land registry, Lantmäteriet, with the participation of a blockchain startup ChromaWay, a consulting company Kairos Future and a telecommunications company Telia, in order to evaluate potential blockchain applications for real estate transactions. The above initiative was motivated by the fact that, although the land register is digitised, processes of land transfer are still vulnerable to errors and the time from signing the contract of sale until the registration of the property is between 3 to 6 months[26]. It is therefore expected that the use of blockchain will make the register operate more efficiently. The project has already undergone three stages. After two initial phases, including the proof of concept and building a testbed with working technology, the third stage, aimed at conducting a real-world property transfer using the blockchain system, was completed in June 2018[27]. The testbed created for the project is based on a private blockchain network. It is accessible only to authorised parties using a smart contract application that manages the transactions. It is designed to store verification records of documents and not documents themselves, which shall be held by each party to the agreement. Moreover, verification records are summarised in an external blockchain that is transparent to the public. Professional users, such as banks, real

[24] C. Santiso, 'Will Blockchain Disrupt Government Corruption?' [5 March 2018] Stanford Social Innovation Review, https://ssir.org/articles/entry/will_blockchain_disrupt_government_corruption, accessed 19 March 2019.

[25] J.M. Graglia, C. Mellon, op. cit. 33–34; S. Higgins, 'Republic of Georgia to Develop Blockchain Land Registry' [2017], https://www.coindesk.com/bitfury-working-with-georgian-government-on-blockchain-land-registry, accessed 19 March 2019; L. Shin, 'The First Government to Secure Land Titles on the Bitcoin Blockchain Expands Project' [2017], https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/#2ae7c5184dcd, accessed 19 March 2019; M. Nimfuehr, 'Blockchain Application Land Register: Georgia and Sweden Leading' [2017], https://medium.com/bitcoinblase/blockchain-application-land-register-georgia-and-sweden-leading-e7fa9800170c, accessed 19 March 2019; N. Nogueroles Peiró, E.J. Martinez García, op. cit. 317; B. Verheye, op. cit. 448.

[26] J. McMurren, A. Young, S. Verhults, 'Case Study: Addressing Transaction Costs Through Blockchain and Identity in Swedish Land Transfers' [2018], https://blockchan.ge/blockchange-land-registry.pdf, accessed 19 March 2019, 4 ff.; V.L. Lemieux, 'Evaluating the Use of Blockchain in Land Transactions' [2017] 6(3) European Property Law Journal 410 ff.; J.M. Graglia, C. Mellon, op. cit. 38; N. Nogueroles Peiró, E.J. Martinez García, op. cit. 316–317; B. Verheye, op. cit. 447–448; M. Nimfuehr, op. cit.

[27] 'Blockchain and Future House Purchases: Third Phase to Be Completed in April 2018', https://chromaway.com/landregistry/, accessed 19 March 2019; M. Kempe, 'The Land Registry in the Blockchain: A Development Project with Lantmäteriet (The Swedish Mapping, Cadastre and Land Registration Authority), Telia Company, ChromaWay and Kairos Future' [2016], http://ica-it.org/pdf/Blockchain_Landregistry_Report.pdf, accessed 19 March 2019; M. Kempe, 'The Land Registry in the Blockchain – Testbed: A Development Project with Lantmäteriet, Landshypotek Bank, SBAB, Telia Company, ChromaWay and Kairos Future' [2017], https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf, accessed 19 March 2019; C. Kim, 'Sweden's Land Registry Demos Live Transaction on a Blockchain' [2018], https://www.coindesk.com/sweden-demos-live-land-registry-transaction-on-a-blockchain/, accessed 19 March 2019.

estate agents and Lantmäteriet, access the contract in a professional interface, which can be integrated with their own systems. Administrators at the land registry and its technical partners administer the contract through a third interface, with changes overseen by all partners running the blockchain. The project also envisages the application of a digital ID system intended to verify buyers and sellers[28].

The use of blockchain in the public services sector is particularly extensive in Estonia, distinguished by considerable experiences in implementing innovative technologies and an advanced digital society. As far as the existing land registration system is concerned, it is relatively safe and effective. The land register operates fully electronically, it can be easily consulted online by anyone and the applications for registration are submitted by notaries via the IT data transmission system. Within the current preparatory works it is planned to apply blockchain technology for real estate transactions as an additional security. It should be pointed out that according to Estonian law, as a rule, real estate transactions are required to be authenticated by a notary who controls, among others, whether the parties have the necessary legal capacity which is not possible when following the assumptions of blockchain. Consequently, it would be unacceptable to eliminate notaries from the land registration process (in this regard a difference can be seen between the Estonian legal order and the Swedish one). Nevertheless, blockchain is considered to be used for transactions that do not have to be notarised, like lease and rental contracts[29].

Similarly, a growing interest in using blockchain in the field of land registration is observed in Poland. Recently the Polish Ministry of Digital Affairs has established the Working Group on Distributed Ledgers and Blockchain, composed of specialists representing different disciplines of practice and research[30]. As regards real estate transactions, for the time being the ongoing discussion is focused mainly on searching for best solutions to improve the electronic exchange of data regarding land, collected in numerous public registers (including land and mortgage register, cadastre, register of real estate prices and values). It is noteworthy that in the last years the Polish land registration system has undergone far-reaching reforms which, so far, have led to establishing a central land registers' database, ensuring public online access to land registers and creating conditions for the development of electronic land registration proceedings. At the current stage, selected entities, including notaries, are obliged to submit applications for registration electronically, with the use of qualified electronic signatures. The submission of an electronic application is reflected by an automatic notice being made in the land register. The group of users authorised to initiate the land registration proceedings by electronic means is going to increase in the near future[31].

---

[28] J. McMurren, A. Young, S. Verhults, op. cit. 5. See also B. Verheye, op. cit. 458; N. Nogueroles Peiró, E.J. Martinez García, op. cit. 317.

[29] M. Sivart, 'Blockchain – Security Control for Government Registers' [2017], https://e-estonia.com/blockchain-security-control-for-government-registers/, accessed 11 April 2019; J. Rastorgujeva, G. Sein, 'Real Estate Transaction Using Blockchain Technology' [25 May 2018], https://www.njordlaw.com/njord-estonia-real-estate-transaction-using-block-chain-technology/, accessed 11 April 2019; B. Verheye, op. cit. 449.

[30] Ministerstwo Cyfryzacji, Grupa robocza ds. rejestrów rozproszonych i blockchain, https://www.gov.pl/web/cyfryzacja/grupa-robocza-ds-rejestrow-rozproszonych-i-blockchain, accessed 11 April 2019.

[31] See e.g. J. Gołaczyński, A. Klich, 'Informatyzacja ksiąg wieczystych. Uwagi ogólne', in: A. Marciniak (ed.), 'Elektronizacja postępowania wieczystoksięgowego. Komentarz praktyczny. Akty wykonawcze' (Warszawa: C.H. Beck 2016) 31–58; A. Gryszczyńska, 'Nowa Księga Wieczysta. Informatyzacja rejestru publicznego' (Warszawa: LexisNexis 2011) 182 ff.; M. Kaczorowska,

Brazil, in turn, is one of countries that face challenges connected with corruption and frauds due to the lack of a modern, reliable land registration system. The major part of the Brazilian territory is untitled and the registration procedure is quite complex[32]. A blockchain pilot project has been implemented from 2017 by the real estate registry office, Cartório de Registro de Imóveis, in cooperation with a blockchain technology company Ubitquity in the State of Rio Grande do Sul, Municipalities of Pelotas and Morro Redondo. It is intended to improve accuracy, security and transparency of land registration as well as lower costs by introducing a parallel blockchain platform to replicate the existing legal structure of property recording and transfer processes, with the use of the Software as a Service business model to record land transactions on behalf of companies and government agencies. The system architecture consists of web frontend that captures information taken from the general real estate registry as well as a web server and backend storage. In the longer term it is planned to create a system that would incorporate the features of blockchain technology to transform the existing recording and land transactions[33].

In 2015 a similar modernisation project was initiated by a blockchain technology company Factom in Honduras, however it has not brought expected results so far due to problems encountered in the course of its realisation. Reforms introduced before by the government have appeared to be insufficient and the land registration system is not digitised, which hinders the implementation of blockchain technology[34].

Conclusions

As shown by the brief overview of legal aspects of the blockchain concept, the way blockchain in its original form is designed proves not to be consistent with the specificity of land registration with its strict formal and substantive requirements. Notwithstanding significant differences among the models of land registers functioning in different countries, some form of verification is a precondition for guaranteeing legal certainty of the transfer of real property rights. Therefore, the involvement of trusted third parties fulfilling particular qualifications, like registrars, notaries or conveyancers, is indispensable. For that reason blockchain registration cannot replace the existing land registration systems, particularly since they are being successively improved by implementing information and communication technologies. Already, innovative tools such as digital signatures and time-stamping are

'Informatisation of Land Registers in Poland and Other Member States of the European Union: A Comparative Overview' [2019] 17(1) Law and Forensic Science 35 ff.

[32] In 19th century the Torrens system, based on registration of titles, was adopted in Brazil, but it is not much used in practice. See e.g. A. Cash, 'Land Registration in Brazil: An Interview with Alex Ferreira Magalhães' [2016], http://www.rioonwatch.org/?p=29200, accessed 19 March 2019.

[33] V.L. Lemieux, 'Evaluating the Use of Blockchain...' 403 ff.; J.M. Graglia, C. Mellon, op. cit. 56; G. Keirns, 'Blockchain Land Registry Tech Gets Test in Brazil' [2017], https://www.coindesk.com/blockchain-land-registry-tech-gets-test-brazil, accessed 19 March 2019.

[34] V.L. Lemieux, 'Evaluating the Use of Blockchain...' 397 ff.; J.M. Graglia, C. Mellon, op. cit. 44 ff.

used to streamline the process of registering land transactions in many jurisdictions[35]. Furthermore, advanced systems of electronic conveyancing are being developed[36].

However, blockchain can effectively be applied in the land registration sector as a complementary technology to support land registers currently operating in particular countries, provided a private or a hybrid blockchain scheme is used. In addition, it is apparent that successful implementation of blockchain technology should be preceded by informatisation of land registers. The practical examples discussed above confirm that blockchain technology, when incorporated to the existing ICT-based land registration infrastructure administered by competent public authorities, contributes to increasing efficiency of transactions. This is the more so given the fact that achievements in this respect regard also land registers representing the title registration model, which, as indicated, envisages more restrictive requirements relating to the control of transactions to be registered when compared to the deeds registration system. Blockchain appears to be useful primarily in terms of providing a secure method to store information thanks to the distributed character of the system, facilitating its recovery in case of attack or loss. Moreover, it offers new possibilities to make data exchange more efficient and rapid through digital identification and authentication mechanisms as well as to enhance the interoperability of public datasets.

Due to the limited scope of the proposed analysis, only selected issues regarding the use of blockchain in land registration have been addressed. As the initiatives realised in this area in practice are at the early stage of implementation, there is a need for further in-depth examination of the impact blockchain technology can have on land registration and land transfer processes, from both legal and economic points of view.

Bibliography

1. 'Blockchain and Future House Purchases: Third Phase to Be Completed in April 2018', https://chromaway.com/landregistry/, accessed 19 March 2019.
2. B. Arruñada, 'Blockchain's Struggle to Deliver Impersonal Exchange' [2018] 19 Minnesota Journal of Law, Science & Technology.
3. M. Barbieri, D. Gassen, 'Blockchain – Can This New Technology Revolutionize the Land Registry System?' [2017], http://www.notartel.it/export/contenuti_notartel/pdf/Land_Poverty_Conference_Blockchain.pdf, accessed 19 March 2019.
4. J. Berkley, 'The Trust Machine' [31 October 2015] The Economist, https://www.economist.com/leaders/2015/10/31/the-trust-machine, accessed 27 March 2019.

[35] See e.g. P. Blajer, 'Elektroniczna „księga gruntowa". Geneza i aktualny postęp automatyzacji ksiąg gruntowych w Niemczech, Austrii i Szwajcarii' [2016] 4 Krakowski Przegląd Notarialny 9–46; P. Blajer, 'Współczesny kształt title registration w krajach common law (Komputeryzacja rejestrów; e-conveyancing)' [2016] 9 Rejent 9–32; M. Kaczorowska, op. cit. 30–48.

[36] This is illustrated by innovative solutions introduced or planned for implementation, among others, in Finland, Denmark, England and Wales, Ireland. See e.g. M.I. Niemi, 'Electronic Conveyancing of Real Property in Europe: Two Models. The English and the Finnish One', in: L.M. Martínez Velencoso, S. Bailey, A. Pradi (eds.), 'Transfer of Immovables in European Private Law' (Cambridge: Cambridge University Press 2017) 20–53; G. Brennan, 'The Impact of eConveyancing on Title Registration: A Risk Assessment' (Cham: Springer 2015).

5. P. Blajer, ‘Elektroniczna „księga gruntowa”. Geneza i aktualny postęp automatyzacji ksiąg gruntowych w Niemczech, Austrii i Szwajcarii’ [2016] 4 Krakowski Przegląd Notarialny.
6. P. Blajer, ‘Rejestry nieruchomości – studium prawnoporównawcze’ (Warszawa: C.H. Beck 2018).
7. P. Blajer, ‘Współczesny kształt title registration w krajach common law (Komputeryzacja rejestrów; e-conveyancing)’ [2016] 9 Rejent.
8. M. Borak, ‘Smoother, Faster, Simpler: Blockchain’s Promise for the Real-Estate Industry’ [21 December 2018], https://technode.com/2018/12/21/blockchains-promise-for-real-estate/, accessed 24 February 2019.
9. G. Brennan, ‘The Impact of eConveyancing on Title Registration: A Risk Assessment’ (Cham: Springer 2015).
10. S. Cámara Lapuente, ‘Registration of Interests as a Formality of Contracts: Comparative Remarks on Land Registers within the Frame of European Private Law’ [2005] 6 European Review of Private Law.
11. A. Cash, ‘Land Registration in Brazil: An Interview with Alex Ferreira Magalhães’ [2016], http://www.rioonwatch.org/?p=29200, accessed 19 March 2019.
12. S. van Erp, ‘Cross-Border Electronic Conveyancing: Overcoming Problems with Negative and Positive Integration in European Property Law’ [2012] 1(1) European Journal of Property Law.
13. G. Gabison, ‘Policy Considerations for the Blockchain Technology Public and Private Applications’ [2016] 189 SMU Science & Technology Law Review.
14. L. Gallego, ‘Blockchain and Title Registration’ [2016] 1 IPRA-CINDER International Review.
15. J. Gołaczyński, A. Klich, ‘Informatyzacja ksiąg wieczystych. Uwagi ogólne’, in: A. Marciniak (ed.), ‘Elektronizacja postępowania wieczystoksięgowego. Komentarz praktyczny. Akty wykonawcze’ (Warszawa: C.H. Beck 2016).
16. J.M. Graglia, C. Mellon, ‘Blockchain and Property in 2018: At the End of the Beginning’ [2018], https://www.conftool.com/landandpoverty2018/index.php?page=downloadPaper&ismobile=true&filename=02-11-Graglia-864_paper.pdf&form_id=864&form_version=final, accessed 19 March 2019.
17. A. Gryszczyńska, ‘Nowa Księga Wieczysta. Informatyzacja rejestru publicznego’ (Warszawa: LexisNexis 2011).
18. R. Herian, ‘Legal Recognition of Blockchain Registries and Smart Contracts’ [2018], https://www.researchgate.net/profile/Robert_Herian/publication/329715394_Legal_Recognition_of_Blockchain_Registries_and_Smart_Contracts/links/5c389e61299bf12be3bfcb67/Legal-Recognition-of-Blockchain-Registries-and-Smart-Contracts.pdf?origin=publication_detail, accessed 19 March 2019.
19. S. Higgins, ‘Republic of Georgia to Develop Blockchain Land Registry’ [2017], https://www.coindesk.com/bitfury-working-with-georgian-government-on-blockchain-land-registry, accessed 19 March 2019.
20. M. Hulicki, P. Lustofin, ‘Wykorzystanie koncepcji blockchain w realizacji zobowiązań umownych’ [2017] 1 Człowiek w Cyberprzestrzeni.
21. M. Kaczorowska, ‘Informatisation of Land Registers in Poland and Other Member States of the European Union: A Comparative Overview’ [2019] 17(1) Law and Forensic Science.
22. G. Keirns, ‘Blockchain Land Registry Tech Gets Test in Brazil’ [2017], https://www.coindesk.com/blockchain-land-registry-tech-gets-test-brazil, accessed 19 March 2019.
23. M. Kempe, ‘The Land Registry in the Blockchain – Testbed: A Development Project with Lantmäteriet, Landshypotek Bank, SBAB, Telia Company, ChromaWay and Kairos Future’ [2017],

https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf, accessed 19 March 2019.

24. M. Kempe, 'The Land Registry in the Blockchain: A Development Project with Lantmäteriet (The Swedish Mapping, Cadastre and Land Registration Authority), Telia Company, ChromaWay and Kairos Future' [2016], http://ica-it.org/pdf/Blockchain_Landregistry_Report.pdf, accessed 19 March 2019.

25. C. Kim, 'Sweden's Land Registry Demos Live Transaction on a Blockchain' [2018], https://www.coindesk.com/sweden-demos-live-land-registry-transaction-on-a-blockchain/, accessed 19 March 2019.

26. B. Klinger, J. Szczepański, 'Blockchain – historia, cechy i główne obszary zastosowań' [2017] 1 Człowiek w Cyberprzestrzeni.

27. V.L. Lemieux, 'Blockchain Recordkeeping: A SWOT Analysis' [2017] 51(6) Information Management.

28. V.L. Lemieux, 'Evaluating the Use of Blockchain in Land Transactions' [2017] 6(3) European Property Law Journal.

29. A. Lodde, 'The European Systems of Real Estate Registration: An Overview' [2016] 1 Territorio Italia.

30. B. du Marais, D. Marrani, (eds.), 'Legal Certainty in Real Estate Transactions: A Comparison of England and France' (Cambridge: Intersentia 2016).

31. L.M. Martínez Velencoso, 'The Land Register in European Law: A Comparative and Economic Analysis', in: L.M. Martínez Velencoso, S. Bailey and A. Pradi (eds.) 'Transfer of Immovables in European Private Law' (Cambridge: Cambridge University Press 2017).

32. J. McMurren, A. Young, S. Verhults, 'Case Study: Addressing Transaction Costs Through Blockchain and Identity in Swedish Land Transfers' [2018], https://blockchan.ge/blockchange-land-registry.pdf, accessed 19 March 2019.

33. F.P. Méndez, 'Smart Contracts, Blockchain and Land Registry' [2018], https://www.elra.eu/wp-content/uploads/2018/12/Smart-Contracts-Blockchain-and-Land-Registry-by-F-Mendez.pdf, accessed 19 March 2019.

34. Ministerstwo Cyfryzacji, Grupa robocza ds. rejestrów rozproszonych i blockchain, https://www.gov.pl/web/cyfryzacja/grupa-robocza-ds-rejestrow-rozproszonych-i-blockchain, accessed 11 April 2019.

35. S. Nakamoto, 'A Peer-to-Peer Electronic Cash System' [2008], https://bitcoin.org/bitcoin.pdf, accessed 25 March 2019.

36. A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, 'Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction' (Princeton and Oxford: Princeton University Press 2016).

37. S. Nascimento, in: P. Boucher, S. Nascimento, M. Kritikos, 'How Blockchain Technology Could Change Our Lives: In-Depth Analysis' (Brussels: European Parliament Research Service 2017).

38. M.I. Niemi, 'Electronic Conveyancing of Real Property in Europe: Two Models. The English and the Finnish One', in: L.M. Martínez Velencoso, S. Bailey, A. Pradi (eds.), 'Transfer of Immovables in European Private Law' (Cambridge: Cambridge University Press 2017).

39. M. Nimfuehr, 'Blockchain Application Land Register: Georgia and Sweden Leading' [2017], https://medium.com/bitcoinblase/blockchain-application-land-register-georgia-and-sweden-leading-e7fa9800170c, accessed 19 March 2019.

40. N. Nogueroles Peiró, E.J. Martinez García, 'Blockchain and Land Registration Systems' [2017] 6(3) European Property Law Journal.

41. K. Piech (ed.), 'Leksykon pojęć na temat technologii blockchain i kryptowalut' [2016] https://www.gov.pl/documents/31305/0/leksykon_pojec_na_temat_technologii_blockchain_i_kryptowalut.pdf/77392774-1180-79ab-4dd5-089ffab37602, accessed 25 March 2019.

42. J. Rastorgujeva, G. Sein, 'Real Estate Transaction Using Blockchain Technology' [25 May 2018], https://www.njordlaw.com/njord-estonia-real-estate-transaction-using-block-chain-technology/, accessed 11 April 2019.

43. C. Santiso, ‘Will Blockchain Disrupt Government Corruption?’ [5 March 2018] Stanford Social Innovation Review, https://ssir.org/articles/entry/will_blockchain_disrupt_government_corruption, accessed 19 March 2019.
44. M. Scott, ‘Blockchain Technology and the Future of Land Registries’ [6 May 2016], https://btcmanager.com/blockchain-technology-and-the-future-of-land-registries/, accessed 11 April 2019.
45. S.S. Shetty, C.A. Kamhoua, L.L. Nijilla, ‘Introduction’, in: S.S. Shetty, C.A. Kamhoua, L.L. Nijilla (eds.), ‘Blockchain for Distributed Systems Security’ (Hoboken: Wiley-IEEE Computer Society 2019).
46. L. Shin, ‘The First Government to Secure Land Titles on the Bitcoin Blockchain Expands Project’ [2017], https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/#2ae7c5184dcd, accessed 19 March 2019.
47. M. Sivart, ‘Blockchain – Security Control for Government Registers’ [2017], https://e-estonia.com/blockchain-security-control-for-government-registers/, accessed 11 April 2019.
48. J.M. Sklaroff, ‘Smart Contracts and the Cost of Inflexibility’ [2017] 166(1) University of Pennsylvania Law Review.
49. T. Stawecki, ‘Rejestry nieruchomości, księgi hipoteczne i księgi wieczyste od czasów najdawniejszych do XXI wieku’ [2002] 40 Studia Iuridica.
50. J.J. Szczerbowski, ‘Lex cryptographia. Znaczenie prawne umów i jednostek rozliczeniowych opartych na technologii blockchain’ (Warszawa: Wydawnictwo Naukowe PWN 2018).
51. J.J. Szczerbowski, ‘Transaction Costs of Blockchain Smart Contracts’ [2018] 16(2) Law and Forensic Science.
52. D. Szostek, ‘Blockchain a prawo’ (Warszawa: C.H. Beck 2018).
53. A. Third, K. Quick, M. Bachler, J. Domingue, ‘Government Services and Digital Identity’ [2018], https://www.eublockchainforum.eu/sites/default/files/research-paper/20180801_government_services_and_digital_identity.pdf, accessed 19 March 2019.
54. R. Thomas, ‘Blockchain’s Incompatibility for Use as a Land Registry: Issues of Definition, Feasibility and Risk’ [2017] 6(3) European Property Law Journal.
55. B. Verheye, ‘Real Estate Publicity in a Blockchain World: A Critical Assessment’ [2017] 6(3) European Property Law Journal.
56. J. Vos, ‘Blockchain-Based Land Registry: Panacea, Illusion or Something in Between?’ [2015] 7th ELRA Annual Publication, https://www.elra.eu/wp-content/uploads/2017/02/10.-Jacques-Vos-Blockchain-based-Land-Registry.pdf, accessed 19 March 2019.
57. A. Walch, ‘The Path of the Blockchain Lexicon (and the Law)’ [2017] 36 Review of Banking & Financial Law.
58. K. Werbach, ‘Trust, But Verify: Why the Blockchain Needs the Law’ [2018] 33 Berkeley Technology Law Journal.
59. S. Young, ‘Changing Governance Models by Applying Blockchain Computing’ [2018] 26(2) The Catholic University Journal of Law & Technology.
60. K. Zacharzewski, K. Piech (eds.), ‘Przegląd polskiego prawa w kontekście zastosowań technologii rozproszonych rejestrów oraz walut cyfrowych. Stanowisko Strumienia w sprawie kierunków ewentualnych prac legislacyjnych oraz działań regulacyjnych instytucji publicznych’ [2017], https://www.gov.pl/documents/31305/52168/przeglad_polskiego_prawa_w_kontekscie_zastosowan_technologii_rozproszonych_rejestrow_oraz_walut_cyfrowych.pdf/f6e74ce0-09e5-776d-bd3b-c21fca96cce2, accessed 19 March 2019.
61. J. Zevenbergen, ‘Systems of Land Registration: Aspects and Effects’ (Delft: Netherlands Geodetic Commission 2002).
62. A. Żuwała, ‘Możliwości wykorzystania technologii Blockchain’ [2018] 87 Studies & Proceedings of Polish Association for Knowledge Management.

A SMART APPROACH TO REGULATING THE SHARING ECONOMY SERVICES

Vija Kalniņa[1]

Abstract

The sharing economy has changed how services are being provided. It has made it possible to share with resources that the owner does not need himself at a particular moment and involved non-professionals in the provision of services. The new form of the service provision in the sharing economy has made it difficult to regulate these services either applying the existing law or issuing new rules.

Many member states of the European Union (hereinafter – the EU) have rushed to take regulatory steps regarding the sharing economy that are more of restricting and prohibiting nature. However, this might have happened because of lack of understanding and pressure from the traditional service providers. The sharing economy has many benefits therefore it is worth to consider a more open approach towards it. Also, the EU has given signals about its positive view on the sharing economy.

Although the sharing economy phenomenon is new, it has been given more and more attention and deliberation so that it is possible to evaluate most common problems, previous actions of member states, and to propose guidelines for member states that could help to get the most of the sharing economy at the same time minimalizing the risks that the sharing economy causes.

Keywords: sharing economy, services, legal framework, European Union

Introduction

Thanks to the technological achievements in the last decade the phenomenon of the sharing economy has evolved.[2] There is no consensus on how the phenomenon should be called (sharing economy, collaborative economy, gig economy, access-based economy, peer-to-peer sharing etc.)[3] or what exactly it covers (non-profit activities, financial activities, profit activities, services, sale of goods).[4] However, despite disputes mainly when speaking about the sharing economy it is understood as based on the use of under-utilised assets for extraction of economic benefits, does not involve change of ownership and thus consists of services rather than sale of goods.[5] The sharing economy business model involves three

[1] PhD student in Law, University of Latvia Faculty of Law, with a dissertation on 'Restrictions on Freedom to Provide Services in the Era of the Sharing Economy'
[2] L. Hou 'Destructive Sharing Economy: A passage from status to contract' (Beijing: Elsevier 2018) 1
[3] P. Teffer, 'Transformation that Lacks a Common Definition' [2017] Euobserver Magazine 3-7
[4] E. Zalan, 'Money Causes Shism in Sharing Economy' [2017] Euobserver Magazine 11-13, G. Petropoulos, 'An economic review of the collaborative economy', [2017] 5 Policy Contribution, 2-3
[5] G. Petropoulos, 'An economic review of the collaborative economy' [2017] 5 Policy Contribution 2-3

categories of participants – service providers that can be either non-professionals or professionals, service receivers and sharing economy platforms.[6] Accordingly in this paper only sharing economy services will be discussed in the given scope.

Sharing economy has its benefits such as effective use of resources, better prices, greater accessibility,[7] but at the same time it is also associated with may risks. Some of the concerns might be suggested by sharing economy competitors – the traditional service providers whose market share has been reduced by this new form of services, but taking a closer look there is no doubt that these concerns are well grounded, and that sharing economy is causing some serious risks. Main areas that are considered to be affected are the consumer protection, employment and taxation.[8] In addition to these also other risks are being mentioned by some authors such as fraudulent actions in the internet, discrimination issues, data protection issues,[9] housing policies, urban transportation policies etc.[10] However, some of these problems are common for all economic activities in the digital environment and some are rather reaction to changes encouraged by the sharing economy.

Although there are different views on what issues need to be addressed and what measures need to be taken, it is almost unanimously agreed that the sharing economy needs to be regulated. On the one hand the regulation is needed to address the risks that the sharing economy imposes, but on the other hand some measures (more at the EU level) should be taken to ensure the growth and development of the sharing economy.[11]

The aim of this paper is to discuss existing regulatory mechanisms and evaluate their capacity and suitability to decrease the sharing economy risks, as well as to propose guidelines for member states that could be taken into consideration when choosing a regulatory approach on sharing economy services.

1. Existing regulatory mechanisms

Sharing economy services are different from traditional services, but they are still services. Traditional services are regulated therefore it seems just reasonable to try to apply this regulation also to the sharing economy services. In addition, sharing economy platforms are aware of aspects that might deter consumers from using sharing economy services and they have their own methods to address these concerns. Both mechanisms – the existing legal framework and self-regulatory mechanisms – are already existing and dealing with sharing economy risks at some level. It is necessary to understand if these mechanisms are sufficient enough before considering new approaches on the sharing economy.

---

[6] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European agenda for the collaborative economy. COM(2016) 356 final, 3

[7] S. Ranchordás, 'The Risks and Opportunities of the Sharing Economy' [2016] 4 EJRR 650

[8] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European agenda for the collaborative economy. COM(2016) 356 final, 9, 11 and 13

[9] G. Petropoulos, 'An economic review of the collaborative economy' [2017] 5 Policy Contribution 13-14

[10] N. M. Davidson, M. Finck, J. J. Infranca, 'The Cambridge Handbook of the Law of the Sharing Economy' (New York: Cambridge University Press 2018) 261

[11] European Parliamentary Research Service, 'The Cost of Non-Europe in the Sharing Economy. Economic, Social and Legal Challenges and Opportunities' (Brussels: European Added Value Unit, 2016) 18

1.1. Application of the existing legal framework

There is an existing regulatory framework in each field where the sharing economy creates risks. There are consumer protection rules in every member state and at the EU level. The same applies to taxation, employee protection and other fields that are affected by the sharing economy such as data protection etc. However, it is difficult to apply these rules to sharing economy services thus leaving a regulatory uncertainty.[12]

The main cause for that is the fact that the sharing economy services are provided differently than it is done traditionally. These differences manifest themselves in two aspects:

1) the platforms of sharing economy are often involved in the provision of overall services;
2) non-professionals are involved in the service provision.

In the sharing economy the platforms very often are not just neutral intermediaries that provide a digital environment for service providers and receivers to meet, but they are involved in the provision of services. The Court of Justice of the European Union (hereinafter – the CJEU) in its judgment in case *Elite Taxi* acknowledged that such platform that acts as intermediary can be regarded as forming an integral part of an overall service, without the platform the provision of services would not be possible and the platform determines main aspects of the services.[13] Thus in the provision of sharing economy services two parties – the sharing platforms and service providers – are involved and that distinguishes sharing economy services form traditional services where the role and responsibilities of service provider and intermediary are clearly divided.

This aspect makes it difficult to apply the existing regulatory framework to the sharing economy services. The existing regulatory framework was made for other type of legal relationships that involve only two parties (service provider and service receiver) with clear roles, obligations and rights. The model where sharing economy platforms are involved in provision of services and are considered as the service providers even if they do not provide the overall service makes it difficult to determine who at what point should be liable for application of consumer protection, data protection and liability rules and makes it difficult to determine who and what actions should be taxed.[14]

The second aspect – involvement of non-professionals in provision of services – significantly affects consumer protection issue. Consumers are main receivers of the sharing economy services,[15] therefore consumer protection is especially significant. Consumer protection system is built on assumption that the consumer is a weaker party and therefore must be more protected.[16] However, if both parties are equal as in sharing economy when services are provided by non-professionals, consumer protection rules cannot be applied.[17] This is even more complicated by the fact that it is vague what actions

[12] S. Ranchordás, 'The Risks and Opportunities of the Sharing Economy' [2016] 4 EJRR 650
[13] Asociación Profesional Elite Taxi v Uber Systems Spain SL, Case C-434/14 [2017] electronic Reports of Cases, para. 38
[14] G. Petropoulos, 'An economic review of the collaborative economy' [2017] 5 Policy Contribution 13
[15] D. Dredge, S. Gyimóthy (eds.), 'Collaborative Economy and Tourism: Perspectives, Politics, Policies and Prospects.' (Cham: Springer 2017) 7
[16] G. van Calster, 'European Private International Law. Second Edition' (Portland: Hart Publishing 2016) 89
[17] V. Hatzopoulos, S. Roma, 'Caring for Sharing? The Collaborative Economy under EU Law' [2017] 1 (54) Common Market Law Review, 106

can be considered as economic actions by non-professionals. Some guidelines are set by the European Commission (hereinafter – the Commission) based on the Unfair Commercial Practices Directive such as frequency of service provision, aim to gain profit and turnover,[18] but it requires analysis of each separate situation. Furthermore, in the case *Kamenova* the CJEU broadened criterions that could point to an economic activity if a non-professional is selling items using internet platforms.[19]

Because of the mentioned differences the sharing economy services fall outside the existing legal framework. Furthermore, the problem is not just that the legislators could not foresee how the way services are provided could change with time, but that provision of sharing economy services creates different legal relationships between different subjects between whom the traditional responsibilities and rights should be divided. However, it is not clear what division would be fair and appropriate and the law does not provide guidelines on this issue.

1.2. Self-regulatory mechanisms

Sharing economy could not function, if the service receivers did not trust the service providers or if the quality of the services was questionable. These two issues are being solved by the sharing economy platforms by introducing self-regulatory mechanisms. Self-regulatory mechanisms can be divided in two categories – measures taken by sharing economy platforms and reputation evaluations generated by users. Both are very effective and worked as precondition for the sharing economy's success. However, there are some issues why this cannot be the only way to approach the risks of the sharing economy.

Measures taken by the sharing economy platforms consist of internal codes of practice and requirements set by the platforms for the service providers. These rules usually regulate interactions between service providers and service receivers and safety issues[20] as well as set specific requirements for service providers or their services. E.g., as it was highlighted in the case *Elite Taxi*, *Uber* platform sets requirements for drivers (driver's licence, experience) and their cars.[21] These internal regulations are effective and service providers usually comply with them, since non-compliance can be punished by banning the service provider from the platform.[22]

However, this self-regulatory mechanism has been criticized since it has potential to transforming the sharing economy platforms into purely self-regulating oligopolies.[23] Also these mechanisms lack transparency and could hide attempts to manipulate service providers. For example, it has been discovered that *Uber* is carrying out a behind-the-scenes experiment in behavioural science to manipulate drivers in the service of corporate

[18] Commission Staff Working Document. Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practies. SWD(2016) 163 final 9-10
[19] Kamenova, Case C-105/17 [2018] electronic Report of Cases, para. 38-39
[20] N. M. Davidson, M. Finck, J. J. Infranca, 'The Cambridge Handbook of the Law of the Sharing Economy' (New York: Cambridge University Press 2018) 266
[21] Asociación Profesional Elite Taxi v Uber Systems Spain SL, Case C-434/14 [2017] electronic Reports of Cases, para 39
[22] N. M. Davidson, M. Finck, J. J. Infranca, 'The Cambridge Handbook of the Law of the Sharing Economy' (New York: Cambridge University Press 2018) 266
[23] Ibid, 267

growth.[24] Thus it raises a question – in whose interests these regulatory steps actually are taken. Do they really target the sharing economy risks?

The other mechanism – user generated reputation mechanism, that have been named as one of three technology innovations that lay the foundation for success of the sharing economy[25] – strengthens mutual trust between service providers and service receivers. It is done by building one's digital reputation based on peer ratings.[26]

There are two evaluation methods – ratings and reviews. Ratings are a quantitative evaluation, where a mark is assigned to the service provider or seller, but reviews are a qualitative evaluation – they describe platform's users' grade of satisfaction evaluating in a descriptive form.[27] Both methods can be used separately and combined. Evaluations usually are public, and they can work both ways i.e. evaluation can be applied not only to service providers but also customers.[28]

However, also this method is not objective and completely fair. The reputation system can work only if the rating and reviews are made honestly and based on real facts, but in the reality, it is not always the case.[29] It is important, because the ratings significantly affect possibility to provide services – bad ratings reduce the possibility to find a customer as well as could end with an exclusion from the sharing economy platform with no way of coming back.[30]

Because of these reasons the self-regulatory mechanisms are deemed not sufficient enough and not appropriate for dealing with the sharing economy risks. These mechanisms lack balance of interests that are being protected, transparency and are also affected by human aspect. Also, self-regulatory mechanisms are not uniform and thus can vary from one platform to another not providing uniform minimal standards and protection.[31]

2. How to regulate the sharing economy services

As it was concluded previously existing regulatory mechanisms are not sufficient enough and not appropriate for dealing with the sharing economy risks. Since the risks are of serious nature it is commonly agreed that there is need for a regulatory action from member states and the EU.

It must be noted that there has been action from some states and also the EU. Approaches are different – some are rushing to regulate the sharing economy either by overregulating or banning the sharing economy services, and some are feeling more

[24] N. Scheiber, 'How Uber Uses Psychological Tricks to Push Its Drivers' Buttons' [2017] The New York Times, available: https://www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html?_r=o

[25] L. Hou 'Destructive Sharing Economy: A passage from status to contract' (Beijing: Elsevier 2018) 10

[26] Ibid, 9

[27] M. R. Redihna, M. R. Guimarães, F. L. Fernandes (eds.), 'The Sharing Economy. Legal Problems of a Permutations and combinations Society' (Newcastle: Cambridge Scholars Publishing 2019) 383-384

[28] Ibid

[29] Ibid 385

[30] Ibid

[31] N. M. Davidson, M. Finck, J. J. Infranca, 'The Cambridge Handbook of the Law of the Sharing Economy' (New York: Cambridge University Press 2018) 267

comfortable with the 'wait and see' approach. Either way the results achieved are not the best possible because they undermine the sharing economy and/or leave the risks unsolved. It is possible to do better.

2.1. Current activities in the sharing economy field

Many member states have reacted quite drastically, prohibiting the sharing economy services or imposing serious limitations on the provision of such services. For example, *Uber Pop* services have been prohibited in France, Germany, Belgium, Italy, Portugal and Spain.[32] However, attitude towards *Airbnb* has not been that hostile, although also services provided through *Airbnb* platform have faced several limitations. These limitations mainly concern rental period and housing policies. States allow short-time rentals by permanent residents and limit possibilities to rent primary residences.[33]

Latvia has also chosen to regulate the sharing economy transportation services provided by non-professionals. In 2018 the Cabinet of Ministers adopted rules on how passenger transportation with a car should be carried out.[34] These rules equalized non-professional drivers with professional taxi drivers requesting registration and licensing of non-professional drivers. But this year it was announced that the Tourism Law will be amended to apply tourist accommodation rules to rent of premises that in carried out through *Airbnb* platform.[35]

Despite the controversial opinions of member states that are very likely affected by traditional service providers, the Commission and European Parliament (hereinafter – the Parliament) have acknowledged the importance of the sharing economy and supported this type of service provision. In 2016 a Parliament study 'The Cost of Non-Europe in the Sharing Economy' was presented. This paper acknowledged the significance of the sharing economy and suggested specific steps that should be taken at the EU level to achieve the full economic potential of the sharing economy and necessity to ensure an adequate balance between creative freedom for businesses and the necessary regulatory protections.[36]

In its communication in 2016 the Commission announced that sharing economy business models can bring significant benefits to the economy, therefore Europe should be open to embracing these new opportunities. It emphasized that '*the EU should proactively support the innovation, competitiveness and growth opportunities offered by modernisation*

[32] V. Hatzopoulos, S. Roma, 'Caring for Sharing? The Collaborative Economy under EU Law' [2017] 1 (54) Common Market Law Review, 91

[33] V. Hatzopoulos, S. Roma, 'Caring for Sharing? The Collaborative Economy under EU Law' [2017] 1 (54) Common Market Law Review, 89

[34] Ministru kabineta 2018. gada 6. marta noteikumi Nr. 147 'Kārtība, kādā veicami pasažieru komercpārvadājumi ar vieglo automobili' [2018] Latvijas Vēstnesis 57 (6143)

[35] V. Anstrate, 'Regulēs dzīvokļu izīrēšanu tūristiem', lsm.lv [2017] availbale: https://www.lsm.lv/raksts/zinas/ekonomika/regules-dzivoklu-iziresanu-turistiem.a315752/

[36] European Parliamentary Research Service, 'The Cost of Non-Europe in the Sharing Economy. Economic, Social and Legal Challenges and Opportunities' (Brussels: European Added Value Unit, 2016) 6

of the economy'.[37] The Commission also emphasized the necessity to ensure fair working conditions and adequate and sustainable consumer and social protection.[38]

In reaction to the communication by the Commission the Parliament in June 2017 issue a non-binding resolution calling for clear EU guidelines regarding the sharing economy.[39] It emphasized the need to ensure consumer protection, workers' rights, tax obligations and fair competition and need for clear and balanced EU strategy.[40]

However, after these announcements no specific action from the EU has followed. On the contrary, with the judgments in the cases *Elite Taxi* and *Uber France* the CJEU left all the responsibility to deal with the sharing economy services at least in the field of transportation on the shoulders of the member states, allowing member states to chose approaches that they consider most appropriate, even if that means an imprisonment of the sharing economy platform administrators.[41]

2.2. How the sharing economy services should be approached

As described before, the sharing economy and its regulation is associated with many difficulties and challenges. Since the phenomenon has been here for several years already, it is possible to evaluate states' practices and problems that have crystalized during the time. In author's opinion there are three groups of aspects that need to be taken into consideration when states try to regulate the sharing economy services:

1) national policy;
2) substantial aspects;
3) aspects related to the EU.

Understanding of these aspects could provide guidelines for the member states on how to approach the sharing economy services, choosing the best and most sustainable solutions.

Firstly, member states have to evaluate, if the sharing economy services are important for the economy and society. The sharing economy can potentially provide many benefits in these fields and they have been acknowledged by scholars and at the EU level. States should not act short-sighted concentrating only on the risks that the sharing economy imposes, including risks to traditional service providers' business model.[42] However, that is what currently can be observed in most member states, which are being very closed towards

[37] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European agenda for the collaborative economy. COM(2016) 356 final, 16
[38] Ibid.
[39] European Parliament, 'Sharing economy: Parliament calls for clear EU guidelines' 15.06.2017. available: http://www.europarl.europa.eu/news/en/press-room/20170609IPR77014/sharing-economy-parliament-calls-for-clear-eu-guidelines (Text adopted by Parliament, single reading, available: https://oeil.secure.europarl.europa.eu/oeil/popups/printsummary.pdf?id=1494418&l=en&t=D)
[40] Ibid.
[41] Asociación Profesional Elite Taxi v Uber Systems Spain SL, Case C-434/14 [2017] electronic Reports of Cases, para. 47, Uber France, Case C-320/16 [2018] electronic Reports of Cases, para. 27
[42] V. Demary 'Competition in the Sharing Economy' (Köln: Institut der deutschen Wirtschaft Köln 2014) 21

the sharing economy ideas, except for United Kingdom, that has launched an initiative to become the 'global centre for sharing economy'.[43]

Secondly, before choosing regulatory actions member states need to understand the specific characteristics of the sharing economy as discussed in this paper. They need to be aware of the differences between traditional and sharing economy services and understand the role of sharing economy platforms. Currently some states target only the sharing economy platforms, some, such as Latvia, – the overall service providers. However, by this one-sided approach states leave legal uncertainty and ignore the specifics of the sharing economy.

Thirdly, member states need to take into consideration aspects related to the EU. These aspects could also be grouped in three categories:

1) the EU's attitude towards the sharing economy;
2) possible unification at the EU level;
3) necessity to grant freedom to provide services.

As mentioned before the EU has overall positive attitude towards the sharing economy and the Commission has encouraged an openness towards it.[44] Also announcements by the Parliament suggest that at some point some unification activities from the EU could follow.[45] Although no specific activities have followed so far, member states should abstain from activities that are contrary to the EU's position.

The last EU related aspect is freedom to provide services. These issues are not discussed broadly, but they definitely were highlighted by *Uber* cases before the CJEU, since platforms rely on this freedom.[46] And there are some authors that consider that many restrictions imposed by member states are an unjustified infringement of the freedom to provide services.[47] That means that member states need to carefully evaluate if their chosen regulation does not infringe the freedom to provide services.

Conclusions

1. The sharing economy services need to be regulated, because they cause various risks in fields that are important to the society.
2. Risks of the sharing economy cannot be eliminated only by the existing regulation and the self-regulatory mechanisms. The existing regulation is not suitable for the legal relations in the sharing economy, but the self-regulatory mechanisms are not always objective and often rather protect the interests of the sharing economy platforms not the groups that need to be protected.

[43] 'Move to make UK global centre for sharing economy' [2014] available: https://www.gov.uk/government/news/move-to-make-uk-global-centre-for-sharing-economy

[44] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European agenda for the collaborative economy. COM(2016) 356 final, 16

[45] European Parliament, 'Sharing economy: Parliament calls for clear EU guidelines' 15.06.2017. available: http://www.europarl.europa.eu/news/en/press-room/20170609IPR77014/sharing-economy-parliament-calls-for-clear-eu-guidelines (Text adopted by Parliament, single reading, available: https://oeil.secure.europarl.europa.eu/oeil/popups/printsummary.pdf?id=1494418&l=en&t=D)

[46] Ch. Busch 'The Sharing Economy at the CJEU: Does Airbnb pass the 'Uber test'?' [2018] 4 Journal of European Consumer and Market Law 173

[47] V. Hatzopoulos, 'The Collaborative Economy and EU Law' (Portland: Hart Publishing 2018) 35-38

3. Many EU member states already regulate the sharing economy services. However, mostly it is carried out in a prohibitive and limiting manner.

4. The EU has expressed a positive opinion about the sharing economy, but no further actions have followed. However, it does not mean that it will not happen.

5. The sharing economy can be regulated more effectively. It is possible to find solutions that embrace the sharing economy and at the same time minimize the risks of the sharing economy. In order to create a better regulation, member states should take into consideration the following aspects:

5.1. national policy – evaluate if the sharing economy is necessary for the economy and society;

5.2. substantial aspects – be aware of the specific attributes of the sharing economy (platforms involved in the overall service provision, non-professional service providers);

5.3. aspects related to the EU:

5.3.1. the EU's positive attitude towards the sharing economy;

5.3.2. possible unification attempts at the EU level;

5.3.3. necessity to grant freedom to provide services.

Bibliography

1. V. Anstrate, 'Regulēs dzīvokļu izīrēšanu tūristiem', lsm.lv [2017] available: https://www.lsm.lv/raksts/zinas/ekonomika/regules-dzivoklu-iziresanu-turistiem.a315752/

2. Ch. Busch 'The Sharing Economy at the CJEU: Does Airbnb pass the 'Uber test'?' [2018] 4 Journal of European Consumer and Market Law

3. G. van Calster, 'European Private International Law. Second Edition' (Portland: Hart Publishing 2016)

4. N. M. Davidson, M. Finck, J. J. Infranca, 'The Cambridge Handbook of the Law of the Sharing Economy' (New York: Cambridge University Press 2018)

5. V. Demary 'Competition in the Sharing Economy' (Köln: Institut der deutschen Wirtschaft Köln 2014)

6. D. Dredge, S. Gyimóthy (eds.), 'Collaborative Economy and Tourism: Perspectives, Politics, Policies and Prospects.' (Cham: Springer 2017)

7. V. Hatzopoulos, S. Roma, 'Caring for Sharing? The Collaborative Economy under EU Law' [2017] 1 (54) Common Market Law Review

8. V. Hatzopoulos, 'The Collaborative Economy and EU Law' (Portland: Hart Publishing 2018)

9. L. Hou 'Destructive Sharing Economy: A passage from status to contract' (Beijing: Elsevier 2018)

10. G. Petropoulos, 'An economic review of the collaborative economy', [2017] 5 Policy Contribution

11. S. Ranchordás, 'The Risks and Opportunities of the Sharing Economy' [2016] 4 EJRR

12. M. R. Redihna, M. R. Guimarães, F. L. Fernandes (eds.), 'The Sharing Economy. Legal Problems of a Permutations and combinations Society' (Newcastle: Cambridge Scholars Publishing 2019)

13. N. Scheiber, 'How Uber Uses Psychological Tricks to Push Its Drivers' Buttons' [2017] The New York Times, available:

https://www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html?_r=o
14. P. Teffer, ‘Transformation that Lacks a Common Definition’ [2017] Euobserver Magazine
15. E. Zalan, ‘Money Causes Schism in Sharing Economy’ [2017] Euobserver Magazine
16. European Parliament, ‘Sharing economy: Parliament calls for clear EU guidelines’ 15.06.2017. available: http://www.europarl.europa.eu/news/en/press-room/20170609IPR77014/sharing-economy-parliament-calls-for-clear-eu-guidelines (Text adopted by Parliament, single reading, available: https://oeil.secure.europarl.europa.eu/oeil/popups/printsummary.pdf?id=1494418&l=en&t=D)
17. ‘Move to make UK global centre for sharing economy’ [2014] available: https://www.gov.uk/government/news/move-to-make-uk-global-centre-for-sharing-economy

Cases

18. *Asociación Profesional Elite Taxi v Uber Systems Spain SL*, Case C-434/14 [2017] electronic Reports of Cases
19. *Kamenova*, Case C-105/17 [2018] electronic Report of Cases
20. *Uber France*, Case C-320/16 [2018] electronic Reports of Cases

Legislative Acts and Other Sources

21. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European agenda for the collaborative economy. COM(2016) 356 final
22. Commission Staff Working Document. Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices. SWD(2016) 163 final
23. European Parliamentary Research Service, ‘The Cost of Non-Europe in the Sharing Economy. Economic, Social and Legal Challenges and Opportunities’ (Brussels: European Added Value Unit, 2016)
24. Ministru kabineta 2018. gada 6. marta noteikumi Nr. 147 ‘Kārtība, kādā veicami pasažieru komercpārvadājumi ar vieglo automobili’ [2018] Latvijas Vēstnesis 57 (6143)

ETHICAL AND DISCRETIONARY ASPECTS OF DECISION-MAKING IN THE CONTEXT OF DIGITAL RATIONALIZATION

Lijana Kanarskiene, Egle Ruzgyte[1]

Abstract

While the most important point of using algorithms in judicial systems is named fairness, it is necessary to search for measures on how to map out regulatory frameworks for decision-making based on algorithms. This suggests that purely normative legal instruments might lose their power, thus authors in the perspective of future judicial power analyze some legal and ethical implications. As a point of bridging the gap between human and algorithmic decision-making is the identification of emerging issues in legal reasoning. Authors submit decomposition of using logical methods in the light of possible dissonance between artificial and human legal reasoning. The attention is paid not only on rational-logical methods of legal reasoning but, conversely, discretionary and ethical dimensions. Furthermore, authors distinguish the importance of judicial power in legal reasoning, especially because of the so-called "hard cases". Taking into account the rationalism, introduced by the rapid change of technology in legal discourse, authors seek for a counterweight to the moral justice side. Also, the distinction between a judge and mechanical reasoning indicates a demand for deploying new ethical requirements in this sphere. According to a rapidly growing role of technologies in the judicial work, the forecast is a grave decrease of judicial discretion. The latter aspect indicates introducing high legal ethics skills with frameworks of exercising abilities to reflect technological changes in judicial systems.

Keywords: rationalization, judicial decision-making, judicial discretion, ethical skills

Introduction

AI-powered legal automation is not yet occupied judicial work, but still, the concern between judges about the influence of AI to judicial systems is clearly visible. Discussions about this impact have reached the peak when The European Commission for the Efficiency of Justice (CEPEJ) in December 2018 declared European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment. Not surprisingly, rapid deployment of technologies in judicial work creates favourable conditions to broaden rationalization of legal reasoning.

Through technological development, we see how AI is already altering the way "justice is done".[2] In this period of development so-called "increasingly capable machines" draw on and analyze massive complex data sets to make or predict decisions, educate themselves so that they itself increase their own capacity.[3] For instance, digital rationalization of the decision-making, based on a model called "bag-of-words", show incredible results. This model is a simplifying representation used in natural language processing and informal retrieval, then a text is represented as the "bag" of its words

[1] Second year PhD candidates in Vilnius University, Faculty of Law. Fields of interests: legal theory, legal ethics, legal professions.
[2] D. Hazel Genn, 'Online Courts and the Future of Justice' [2017], Birkenhead Lecture, p. 1.
[3] R. Susskind and D. Susskind, 'The Future of Professions' (Oxford: 2015) p. 272.

disregarding grammar and word order but keeping multiplicity.[4] Scientists from University College London, who develop systems to predict the outcome of real-life human rights cases, trained an algorithm on a set of court decisions, viewing each document with a before mentioned method. Not surprisingly, their experiment shows that with using enough data, machines can quite accurately predict legal decisions.[5] Some widespread examples already had shown intriguing AI abilities (e. g. "CaseCruncher Alpha") to predict the outcome of litigation.[6]

Further commonly cited examples confirm the advantages of machine-made thinking. For example, abilities of IBM's Watson computer, which in 10 minutes, identified and recommended treatment for leukemia in a patient whose case had been confounding many doctors being baffled by this situation. Another example of JP Morgan's programme ("Contract Intelligence") shows abilities to scan contracts in seconds to interpret credit agreements thus replacing thousands of lawyers working hours.[7] It is no more questions about the capabilities of those machines to think, still, there is left space to ask whether those machines are able to outperform humanity.

1. Advantages and imperfections of "intelligence assistance"

Courts are being significantly transformed by digitization and it is progressing unstoppable, which means AI can do more than carrying out tasks, depended before now on human reasoning. Machines are able to learn from new information, evaluate data. AI can support courts systems by acting as "assistants" to judges. "Intelligence assistance" manifests simply doing the same as judges: analyzing cases, applying legal norms and predicting possible resolutions. Support like the latter leads to a judge only review the work, which was done by the machine.

Professor D. Hazel Genn names how technologies at this moment can benefit the judiciary. According to him, technologies can help to reach out information; speed up and simplify processes (e. g. online procedures, document handling, embedding procedural rules within online forms and processes, preparing contracts, correcting errors); allow people to gather information without the necessity for physical presence; ease online resolution. Professor says, technologies ultimately can support or even replace "human-decision-making through automated processes and databases of the subject matter, duration, and outcome of disputes could help dispute prevention and early resolution".[8]

All this means less time and money consuming, but one of the most frequently repeated advantages of AI in the judiciary is emotional neutrality: in other words, technology doesn't get tired, nervous, hungry, etc. Minimizing the influence of such extraneous factors as "weariness and emotional instability" is the key aspect of AI welcoming in courts systems.[9] Human keeping up with technologies is quite shocking

[4] R. Balamurugan, S. Pushpa, 'A Study on Sentiment Analysis on Social Media Using Machine Learning Techniques' [2017], International Journal of Recent Advances in Engineering Technology, Vol. 5, p. 29.
[5] N. Aletras, et al, 'Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective', PerJ Computer Science, [2016], pp. 1-19.
[6] N. Aletras, 'Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective', PerJ Computer Science, [2016], p. 1-19.
[7] D. Hazel Genn, 'Online Courts and the Future of Justice' [2017], Birkenhead Lecture, pp. 2-3.
[8] Ibidem, p. 3.
[9] T. J. Buocz, 'Artificial Intelligence in Court Legitimacy Problems of AI Assistance in the Judiciary' [2018] 2, 44.

thus the usage of AI in the judiciary requires safeguards in the legal discourse in order that predictive justice would not change the essence of justice.

This "intelligence assistance" leads to raising several important questions. One of the essential dangers of judge's decision-making is distinguished the loss of discretionary power. To this problem attention in this text will be paid on later. The second issue of this discourse is changes of models of human thought processes. This indicates a major alteration of the methods commonly used in legal reasoning and, consequently, the dominance of logical argumentation.

1.1. Decision-making based on logic

The role of logic in legal reasoning at all times was indisputable, but in the Fourth Industrial Revolution, it has become of exceptional importance.[10] Taking a flashback to the past, when the talks about the synthesis of legal reasoning and AI have just begun to raise, an exploration of computer's potential in law started with the logic. Efforts in exploring this conjunction have given consideration opportunity that computers can function with the legal database in the way lawyers do – foremost apply logic.

The justification for legal authority or legal validity is sought through rational argumentation. In a general sense "rationalism" means that cognition is a consequence of logical thinking and cannot be separated from logic, therefore rationality is defined as logically based, theoretically thought out and systematically covered by the perception of some phenomenon's purpose. However, the "purification" of legal science in the perspective of AI, created the preconditions for the development of an internal definition of the legal logic necessary for legal certainty. Regarding the connection between law and logic, it should be noted that logic is often correlated with legal formalism,[11] which is generally associated with situations when decisions are made logically by drawing conclusions from certain assumptions without taking into account the social aspects or values. In this case, the norms of law are not evaluated, they are correct or incorrect, applied almost mathematically.[12] The application of clear rules to obvious facts is primarily characterized as a legal formalism by the process of applying the law of syllogistic nature, which is understood as a logical operation, i. e. deduction (relationship of law, facts, and conclusion). Deductive reasoning is considered to be an internal legal justification, which, if logically concluded from the assumptions of law and facts, provides rationality for argumentation.[13]

Nowadays legal reasoning is based on many different artificial tools that can automate this process. Legal formalism using AI is also considered to be an approach where decisions are taken and the law is interpreted on the basis of rules and system established usually by the legislature and legal practices. So, in this case, legal discourse is roughly based on algorithms, formed on the basis of formal logic. This means the legal conclusions as a rational consequence of legal discourse become logically justified. Even making the outcome of legal discourse rational, the rationality of the reasoning activity is primarily based on the search for reasonable explanations, assertions, but not values itself, internal motives.

---

[10] E. Feteris, H. Kloosterhuis, 'The analysis and evaluation of legal argumentation: approaches from legal theory and argumentation theory' [2009] Studies in Logic, Grammar and Rhetoric, Vol. 16 (29), p. 311.

[11] R. Latvelė, 'Teisėjo vaidmuo aiškinant teisę: daktaro disertacija [The role of the judge in interpreting law]' (Vilnius: Vilnius University 2010) p. 35.

[12] R. A. Posner 'Legal Formalism, Legal Realism, and the Interpretation of Statutes and Constitution' [1986] Case Western Reserve Law Review, Vol. 37, p. 180.

[13] Deductive system's consisting of basic and deductively derived statements, is considered to be the ideal form of knowledge according to the classical concept of rationality.

In this sense, rationality is not idealized – it is not a requirement for justice, as a principle, as a value category.

It should be recognized that digital decision-making allows to abstract rationality as a sign of reasonableness, consistency, clarity, logic, actual certainty, and sufficiency. Either digital decision-making systems are clearly evolving: from proofing rationality of arguments towards reintroducing elements of rhetoric, context, procedure. Also, the link between rationality and logic in the legal discourse is directed at efficiency, which manifests itself as ”justification of law” and persuasion in the authority of law. Even so, scientists acknowledge, interpreting the logic of reasoning systems is still a big deal and note that it should be raised new requirements for judges in chasing the logic of such decision-making.

1.2. Imperfections of rationalism

Definitely, AI legal reasoning is a time-saver in general, but without human intervention, digital tools give the impression that all situations can be solved by rational application of the rule, it also commands a formalistic model of legitimacy. In this context, it is also worth mentioning the replica that “syllogism is not a useful template for legal thinking”. According to R. A. Posner, the formalism that is used uncritically leads to a contradiction between formal and fundamental justice,[14] so only legal normative instruments in AI-based decision-making are not sufficient.[15] Therefore, several reasons justifying such an approach are distinguished.

Firstly, a dynamic of social behavior regulators is still one of the core minuses of AI rooted logic. Even though technologies forecast not only statically understandable law, it is hard to bypass social human life (peculiarities of changing values, social norms, policies, etc.). The distance between an abstract norm and a specific situation can be considered as a weighty defect of digital making decisions. In this context, it should also be noted that the inappropriateness of reasoning based on logic is most closely related to the staggering variety of language usage, the division of concepts into abstract and specific, their multiple meaning.[16] Even if the current technological means are capable of delivering good results in decision-making, linguistic meaning is not enough, – in the words of A. Barak, one should strive to establish the relation between the word and the context or “verba” and its “spirit”. Formal legal interpretation is considered to be opposed to the creative, which gives priority to the spirit, not to the letter of the law. The purpose of such an interpretation is to identify (verify) the legal provisions in a broader sense by obtaining additional information that is not directly related to the system of sign characters. The purpose of creative interpretation of the law is the harmony of form and content: incorporation of rationality and intelligence and other legal values into the interpretation of the law; not just the text of the rule of law, but also reliance on what goes beyond the norm.[17]

Another problem of digital decision-making is real communication with the parties: it is predicted that an ethically trained judge will have to spend more time

[14] R. A. Posner recognizes that many legal issues are addressed through the syllogism and believes that ”<...> critical logic is a method of pursuing consistency. Consistency, like logic, is appreciated because it allows the tools to fit into the goal. Such adaptation is the core of rationality, and logic and rationality are closely related.” R. A. Posner, ‘Jurisprudencijos problemos [The Problems of Jurisprudence]’ (Vilnius: Eugrimas 2004) p. 43, 45, 54, 97.

[15] H. Prakken ‘AI and Law, Logic and Argument Schemes’ [2005] Argumentation, Vol. 19 (3), p. 12.

[16] C. Cohen, C. M. Irving, ‘Introduction to Logic. Twelfth edition’ (New Jersey: Upper Saddle River 2005) p. 69; A. Marmor, ‘Interpretation and Legal Theory’ (Oxford: Clarendon Press 1994) pp. 125-126.

[17] A, Barak, ‘The Judge in a Democracy’ (Princeton: Princeton University Press 2006) pp. 123-125.

communicating with people in the process. Compliance with procedural rules will, therefore, be of great importance. According to R. Alexy, the rationality of legal argumentation should not be linked to the certainty of the results obtained but especially to the observance of the rules laid down. A big part of those normative rules is procedural. Only If these requirements were met during the discourse, it can be described as "correct". From this point of view, it is emphasized that legal discourse should always take place under restrictions such as a distribution of roles, obligation to tell truth, set time for reasoning, other regulated procedural norms. In legal discourses, there is a claim of justice, which is related to whether it can be rationally justified not even by logic, but by the existing law.[18]

It is also worth mentioning another imperfection of digital reasoning, which is a disregard of plurality of non-legal arguments.[19] As a value-neutral, AI is directed towards the logical justification of law, it does not analyse or analyse incompletely the axiological aspects. The law requires a moral judgment – so keeping this position much more space should be left to values, which cannot be explained logically but come from experience, different cultures, legal principles. However, the role of them may change unrecognizably.

The principles of law, as standards of conduct, are considered to be the fundamental provisions of general nature, in addition to shaping binding standards of behaviour, they always reflect a moral dimension, which inevitably implies their intrinsic nature and, at the same time, their abstract nature. Even principles seem to be at a "high-level of subjectivity", and also can be associated with many phenomena that everyone may think differently[20], the problem of digital decision-making is how to deal with all above-mentioned aspects.

Some examples of dealing with above-mentioned problems were submitted still in 2001. These are computational models for practical ethical, rather than legal, reasoning. Scientist B. McLaren created a program ("Sirocco"), which, given a problematic situation, retrieves past ethics cases, also ethics codes provisions, which are relevant to the analysis of the problem. The main issue, which was trying to solve by the program, was that in ethics, as in law, principles cannot be simply defined as an applied deductively. So, it was meant to answer, how to bridge the gap between particularly abstract principles and the factual scenarios? Results of using the program had shown great abilities to decide cases as judges do.[21]

Notwithstanding, norms with the elements to be evaluated will always have an internal or high-level subjectivity and will not be universally endorsed. Among other things, the application of syllogism is complicated in cases where the conflict of laws is not resolved by the usual collision rules and when so-called "hard cases" are encountered. Justice in the sense of the legal form, besides the rich elements of law – the values of law, the principles of law, still seems to be impossible in today's law.

The importance of logic revealed the category of rationality as a rationalization of everything (not just the argumentation process, but also of justice) by operating concepts and dogmatic truths. Rational decision-making is not just a matter of form but also of content. This means that the rationality of legal reasoning in the sense of fairness of its form is insufficient: it is necessary (most important) to seek justice in content. Though the

[18] R. Alexy, 'Teisinio argumentavimo teorija [Theory of Legal Argumentation]' (Vilnius: Teisinės informacijos centras 2005) pp. 230-239.
[19] T. Bench-Capon 'Argument in Artificial Intelligence and Law' [1997] Artificial Intelligence and Law, Vol. 5, p. 256.
[20] N. MacCormick, 'Reasonableness and Objectivity' [1999], Notre Dame Law review, Vol. 74, pp. 576-578.
[21] K. Ashley, et al, 'Legal Reasoning and Artificial Intelligence: How Computers 'Think' Like Lawyers' [2001], The University of Chicago Law School Roundtable, Vol. 8, pp. 9-12.

automation of justice has several visible measures: training judicial ethics and developing judicial discretion.

2. Discretionary and ethical dimensions

In order to properly implement the rule of law and the independence of judiciary, it is necessary to ensure judicial discretion (lat. *discretio*). The latter is the right of the instance of an officer or a public instance to decide some issue on their own. The term discretion is used in law with a different, special meaning: as discretion of a judge, that is an officer of the state who executes justice. The discretion of the judge is a certain freedom of actions (choice) to solve some issue at its own authority to adopt, or not to adopt, whatever rule he deems fit.[22]

It goes without saying that it is impossible for the legislator to prepare legislation covering all the situations dealt with in courts or the situations, the solutions of which become part of the legal system. Therefore, since judges are involved in the process of court and receive testimony (evidence) at first hand, they must have some discretion to not only apply law in the procedure of hearing and the factual circumstances of the dispute, but also to interpret the legal text in order to determine the idea expressed by the text[23], to reveal the legislator's intentions, in other words, to perceive the spirit of the law; whereas the latter depends on the distinctive factors under the influence of “the general spirit” of a historically matured particular nation.[24]

The very requirement to reason a judgement of the Court silently demonstrates that in principle several opinions are possible when interpreting the same law norm[25], but it also shows a certain discretion of the judge to choose the appropriate interpretation with regard not only to the legislator's intentions, but also to the social and moral values of the current period, through making use of favourable social provisions[26]. The judges contemplate (consider) not only the origin of the norm; they also take into account the feeling of expediency / appropriateness prevalent in the society and the profession during the time, which recognizes certain moral principles to a proper resolution of the legal dispute[27].

Such legal interpretation is not only the explanation of law, it is interpretation of law by creatively constructing it[28]; Interpretation is a morally (by way of morality) "charged" activity.[29] When being aware of the trends and needs determined by the overall legal regulation, the judge has a degree of freedom and the power to make

[22] G. C. Christie, ‘An Essay on Discretion’ [1986] Duke Law Journal, Vol. 5, p. 748.
[23] G. Lastauskienė, ‘Teismų “interpretacinis žaismas” ir jo doktrininės prielaidos [Judicial "interpretative play" and its doctrinal assumptions]’ [2012] Jurisprudencija, T. 19 (4), p. 1345.
[24] A. Valantiejus, ‘Charles Montesquieu ir ankstyvoji sociologinė tapyba [Charles Montesquieu and Early Sociological Painting]’ [2005] Sociologija. Mintis ir veiksmas, p. 150.
[25] R. Latvelė, ‘Teisėjo vaidmuo aiškinant teisę: daktaro disertacija [The role of the judge in interpreting law]’ (Vilnius: Vilnius University 2010) p. 171.
[26] R. Bakševičienė, D. Beinoravičius, ‘Teisės ir moralės santykis remiantis teisės požymiais. Jo naudojimas formuoti teigiamas Lietuvos teisės sistemos atžvilgiu visuomenės nuostatas [The Role of Morality in a Legal System in the Context of the Western Legal Tradition]’ [2004] Teisė, 51, p. 21.
[27] S. R. Suumers, ‘Essays and Legal Philosophy’ (University of California Press: Berkeley and Los Angeles 1968), p. 54.
[28] E. Spruogis, ‘Teisės aiškinimo probleminiai aspektai [Problematic Aspects of Interpretation of Law]’ [2006] Jurisprudencija, T. 8 (86), p. 59.
[29] B. W. Wendel, ‘The Limits of Positivist Legal Ethics: A Brief History, A Critique, and a Return to Foundation’ [2017] Canadian Journal of Law & Jurisprudence, p. 458.

decisions at his or her discretion and at his or her choice on what interpretation and application of legislation meets those needs and (or) the regulatory objectives best: it becomes a creative law enforcer[30] who fulfils the method of substantive application and interpretation of law. Some examples from legal practices confirm that in difficult cases, a formalistic approach is not sufficient – to view the meaning of the words superficially, without holding it dependent on any reasonably foreseeable circumstances. [31]

The legal competence is not sufficient to reach decisions in difficult cases, because in such cases the legal experience is not usually associated with the appropriate decisions. Then a substantive interpretation (application) of law serves for the proper resolution of the dispute; the creative construction of law is determined and promoted by two key factors: 1) the concept of rights (what sources of law will be used to rely on by the judge); 2) uncertainty of the law norm or its formal failure (ambiguity of the legal language, conflicts, gaps, etc.), which implies the possibility and need to make a decision not in accordance with a verbal expression of the norm, but on the basis of the principles, values, objectives and so on.[32] In cases like these, legal discretion is necessary. Because absence of the judge's discretion makes legal interpretation, which corresponds to the epoch and defends the values, impossible and the absence of a legal interpretation makes the rule of law itself impossible. The role of the judge is precisely to implement the rule of law[33].

It should also be noted that choices by the judge, if they are made as a part of a normal life of the public, are always determined by the criteria of values or culture and consciousness prevailing in the society. It is recognized that one of the major general (public) aspects of welfare is what is known as the moral clarity/intelligibility of our lives.[34] Therefore, in principle, the judge is delegated with the power to implement the conceptions of the political morality of his or her own, in other words,

[30] R. Latvelė, 'Teisėjo vaidmuo aiškinant teisę: daktaro disertacija [The role of the judge in interpreting law]' (Vilnius: Vilnius University 2010) pp. 168-169.

[31] One of the most interesting practical cases of Lithuania, in which the substantive application of law has manifested, is the Judgement made by the Supreme Administrative Court of Lithuania in 2010. Having regard to the then economic crisis of the country and its consequences for small business, the Court on its own initiative appointed to the offender (an entity of a small business) a significantly lower penalty than the statutory minimum penalty. It is an evident example of an active, free and creative gesture of the Court, and accordingly, an expression of empathy in judges (in the presence of a crisis to the situation of the offender, a small business entity), emotional intelligence and legal ethics. Ruling of 5 October 2010 of the Supreme Administrative Court of Lithuania in administrative case No A-143-972/2010.

Another practical example is related to the well-known Riggs v. Palmer case, which dealt with the issue on the interpretation of the law on the right of succession, when a successor killed the testator. The Court recognised that the testament was legal under the applicable law, which has set certain formal requirements of testaments, but the Court denied the successor's (who killed the testator) right to the bequests, on the ground that all the laws are limited to certain fundamental maxims. R. A. Posner, 'Jurisprudencijos problemos [The Problems of Jurisprudence]' (Vilnius: Eugrimas 2004) p. 221. H. W. Simon, 'Role Differentiation and Lawyers' Ethics: A Critique of Some Academic Perspectives' [2010] Georgtown Journal of Legal Ethics, p. 15.

[32] R. Latvelė, 'Teisėjo vaidmuo aiškinant teisę: daktaro disertacija [The role of the judge in interpreting law]' (Vilnius: Vilnius University 2010) p. 175.

[33] A. Barak, 'Purposive interpretation in Law' (Princeton: University Press 2005). In R. Latvelė, 'Teisėjo vaidmuo aiškinant teisę: daktaro disertacija [The role of the judge in interpreting law]' (Vilnius: Vilnius University 2010) p. 180.

[34] D. A. Selbst, S. Barocas, 'The Intuitive Appeal of Explainable Machines' [2018] Fordham Law Review, Vol. 87, p. 1118.

to use morality (ethics), an additional non-legislative measure for his right to interpret.[35]

An unambiguous definition of ethics is impossible, simply because it lies within the difficulties (drawbacks) of actions (conducts). The term “ethics” has a connection with the interoperability between themselves and normative environment. The ethical dilemma is a decision on what it is - to do as to "met and right”. The “met and right” indicates proper, intelligent, wise, smart and prudent. It is a need for a reflective, caring, wilful, insightful, wise (edified) behaviour in difficult situations. [36] It is important to mention that ethics analyses not just any (not all of the) behaviour, but the kind that is only morally significant, requiring valuable incentives; appropriate situations (severe, unclear, undefined) are necessary for such behaviour to manifest. That is why there is no way to predict (define) in advance what "met and right" is in specific cases.[37]

So, the court's independence and discretion are a legal and ethical principle. When a decision lacks legal principles, the ethical ones come to supplement, which allows the legal mind of the judge to assign a "justifiable" reason to take some decision in full spirit.[38] Each judge in the exercise of discretion and pursuing this "spirit", is exposed to the inner subjective factors, and at the same time, limited by the overall social context and its regularities[39], but in any case, an essential element of discretion remains, which is the judge’s ethical choice. It is precisely the judicial discretion that allows the manifestation of the ethical thinking of the judge, which has been formed by the customs over centuries and is related to the choices that are crucial to the public (its welfare).

3. In the conjunction of AI and ethics

While a few decades ago the scientists of AI of the legal field (judicial activity) used to consistently reject any attempts to "appropriate" the judicial discretion, by replacing it with a stiff computer model[40], today it is obvious that the AI has already successfully entered the modern world of the system of Courts: AI already changes the decision making process in the USA and other jurisdictions; the models of the forecasted legal analytics already allow to make assumptions on the results of legal disputes; online dispute resolution which uses decision-making by AI is already conducted.[41]

AI research aims to develop practical measures to support judicial activities as well as new analytical tools to help understand and model judicial decision-making. However, as already mentioned in the previous section, there are many factors that affect judicial decision-making. Such factors include induction and intuition, as well

[35] E. Spruogis, ‘Teisės aiškinimo probleminiai aspektai [Problematic Aspects of Interpretation of Law]’ [2006] Jurisprudencija, T. 8 (86), p. 59, 61.
[36] C. G. Hazard, ‘The Legal and Ethical Position of the Code of Professional Ethics. Social Responsibility: Journalism, Law, Medicine’ [1979] Wash. & Lee Univ., pp. 10-11.
[37] Ibid.
[38] B. Sullivan, ‘Law and Discretion in Supreme Court Recusals: A Response to Professor Lubet’ [2013] Valparaiso University Law Review, Vol. 47, p. 909.
[39] J. Gumbis, ‘Teisinė diskrecija: socialinis požiūris [Discretion: Social Approach]’ [2004] Teisė, 52. In R. Latvelė, ‘Teisėjo vaidmuo aiškinant teisę: daktaro disertacija [The role of the judge in interpreting law]’ (Vilnius: Vilnius University 2010) p. 198.
[40] G. Sartor, K. L. Branting, ‘Introduction: Judicial Applications of Artificial Intelligence’ [1998] Artificial Intelligence and Law, pp. 105-106.
[41] 2018, p. 1121.

as the ability to take the moral values into account and to assess the social impact of decisions[42]. There still is a problem that ethics implies more frequently something that people feel over what they intellectualize.

Meanwhile, AI cannot learn this sense, it has no empathy nor emotional intelligence, so it will never be able to match a person. The operation of software operation programmes is based on logic, wherein the input information is processed by the algorithms programmed in order to receive the results laid down. Digital technologies have the ability to process and manipulate abstract symbols (zeros and units), but they do not understand this information nor the sense of the processes of its treatment. This may be contrary to the human mind that can understand what information it processes[43].

Prudence, as the ability to choose between the alternatives of different value, is an essential condition of ethics. The task of legal ethics is to understand what is right and what is wrong[44]; there is a need for practical wisdom of the judge[45]. Meanwhile, on the one hand, by using algorithms to analyze the issues that have no correct answer, we do not even have a simple way to calibrate them (to compare them with the correct answer) or to correct them. Therefore, we should not expect that the algorithm takes some moral decisions that we have yet to make. On the other hand, our ethical and moral criteria are so nuanced and culturally dependent, that it is questionable whether the automated logical process will ever be able to properly weigh and evaluate them.[46] On the one hand, even if we are able to give some examples of ethical behaviour of the AI, we would inevitably miss some of them. On the other hand, ethics is most frequently associated with not previously investigated (backlog) situations.

It is acknowledged that a number of challenges is brought about by the bias of the current decisions of the court; it can be affected by a number of factors that would not be present in the presence of AI: the time of the day; what and when the judge had as a meal; the number of decisions made by him or her on that date; on what conscious beliefs and unconscious assumptions he or she relied on; how much he or she trusted his or her intuition; how the attractiveness of the participants influenced him or her; by what emotions he or she was affected. It is true that the scope and scale of the influence of these factors is not known, but even if the judge "recognises" these factors, it is likely he or she [the judge] would undervalue (or, more generally devalue) their impact.[47] This goes to say that the ultimate "black box" is our minds.[48]

Therefore, the overall consistency of judicial decisions is never achieved: it is more a posteriori reasoning used in the explanation of the judge, with the purpose of

[42] T. Sourdin, 'Judge v Robot? Artificial Intelligence and Judicial Decision-Making' [2018] UNSW Law Journal, Vol. 41 (4), p. 1123.
[43] T. Sourdin, 'Judge v Robot? Artificial Intelligence and Judicial Decision-Making' [2018] UNSW Law Journal, Vol. 41 (4), p. 1128, 1132.
[44] B. W. Wendel, 'Legal Ethics Is About Law, Not Morality or Justice: A Reply to Critics' [2012] Texas Law Review, Vol. 90:727, p. 731.
[45] B. L. Solum, 'The Virtues and Vices of a Judge: An Aristotelian Guide to Judicial Selection' [1988] Southern California Law Review, Vol. 61, p. 1753.
[46] O. Tene, J. Polonetsky, 'Taming The Golem: Challenges of Ethical Algorithmic Decision Making' [2017] North Carolina Journal of Law and Technology, p. 33.
[47] T. Sourdin, 'Judge v Robot? Artificial Intelligence and Judicial Decision-Making' [2018] UNSW Law Journal, Vol. 41(4), p. 1129.
[48] O. Tene, J. Polonetsky, 'Taming The Golem: Challenges of Ethical Algorithmic Decision Making' [2017] North Carolina Journal of Law and Technology, p. 28.

the making sure of the validity of a specific decision rather than a strict and objective description of all of the decision-making processes that have led to this outcome [49].

Meanwhile, AI would eventually determine the standardization of judicial decisions, which would be based not on the assessment by the court (the judge) in each specific case, but only on purely statistical calculations associated with the averages of other previously made decisions (inner beliefs of judges). It is obvious that such rigidity of the AI is not compatible with the discretionary and (or) ethical decisions by judges. However, of course, as the information needed for the human decision-making becomes increasingly complex (because there are a lot of complex data sources), judges will eventually have no other choice but to rely on the AI. However, instead of imposing the obligation of making ethical decisions on AI, a better choice would be to teach it to establish examples of ethical and unethical behaviour and leave the possibility for people (judges) to take decisions deriving from this differentiation.

Summarising the above information, we can conclude that in spite of the fact that AI is a very powerful tool, there still are a few areas where it is superior to a human being, mainly those related to rapid information processing, therefore even having fulfilled (completed) all of the principles and requirements posed in the European Charter (on the ethical principles when using AI in the judiciary system), still, the AI "judge" should not replace the human judge, but only to complement his or her human intellect, by giving a further opportunity for the judge to use the "smart" advice of the AI. Therefore, the application of AI in the court system (in the judicial decision-making activity) is a continuity of the trust in the rule of law. However, in this respect, the opportunity of the human decision-maker to review and object to a decision made by the AI is a required component of any automated decision-making system.[50] Justice is and should remain human because it relates primarily to people[51]. AI can process information, whereas a human being can decide what to do with it. As we can see, in this analysis one thing is certainly clear – AI cannot act in place of the judge, and we cannot act against the AI – we have to work together with it.

Conclusions

In view of the worrying debate in the judiciary on the power of AI, particular attention should be paid to the legal justification of decision-making. Although the benefits of using algorithms in decision-making are staggering, there are still fundamental problems that are being encountered: a change of law and other social behavior regulators; limits of the linguistic approach, including a vacuum between “word” and “sense”; value-neutrality and compliance with procedural requirements.

[49] European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment, adopted at the 31st plenary meeting of the European Commission for the Efficiency of Justice (CEPEJ), Strasbourg, 3-4 December 2018 Available at: <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>.

[50] T. Sourdin, ‘Judge v Robot? Artificial Intelligence and Judicial Decision-Making’ [2018] UNSW Law Journal, Vol. 41(4), p. 1119, 1124.

[51] A. Gutauskas, Lithuanian courts website. Rubric: Judicial system news. Available at: <https://www.teismai.lt/lt/naujienos/teismu-sistemos-naujienos/aurelijus-gutauskas-teisingumas-yra-ir-turetu-likti-zmogiskas/6388>.

The use of “intelligence assistance” in judicial decision-making manifests itself as a threatening rationalization of justice processes, therefore should be introduced new interdisciplinary requirements for judicial systems in order to reduce the distance between human and machine decision-making.

While the benefits of mechanical decision-making in the judiciary are not disputed, there are reasonable doubts as to whether judges will be able to grasp and manage decision-making processes. In this case, the most important problems are indicated as legitimacy and social acceptance of such decisions. To address these problems it is proposed to develop new ethical requirements, as well as strengthen the discretion of judges.

Bibliography

1. N. Aletras, et al, ‘Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective’, PerJ Computer Science, [2016].
2. R. Alexy, ‘Teisinio argumentavimo teorija [Theory of Legal Argumentation]’ (Vilnius: Teisinės informacijos centras 2005).
3. K. Ashley, et al, ‘Legal Reasoning and Artificial Intelligence: How Computers ‘Think’ Like Lawyers’ [2001], The University of Chicago Law School Roundtable, Vol. 8.
4. R. Bakševičienė, D. Beinoravičius, ‘Teisės ir moralės santykis remiantis teisės požymiais. Jo naudojimas formuoti teigiamas Lietuvos teisės sistemos atžvilgiu visuomenės nuostatas [The Role of Morality in a Legal System in the Context of the Western Legal Tradition]’ [2004] Teisė, 51.
5. R. Balamurugan, S. Pushpa, ‘A Study on Sentiment Analysis on Social Media Using Machine Learning Techniques’ [2017], International Journal of Recent Advances in Engineering Technology, Vol. 5.
6. A. Barak, ‘The Judge in a Democracy’ (Princeton: Princeton University Press 2006).
7. T. Bench-Capon ‘Argument in Artificial Intelligence and Law’ [1997] Artificial Intelligence and Law, Vol. 5.
8. T. J. Buocz, ‘Artificial Intelligence in Court Legitimacy Problems of AI Assistance in the Judiciary’ [2018].
9. G. C. Christie, ‘An Essay on Discretion’ [1986] Duke Law Journal, Vol. 5.
10. C. Cohen, C. M. Irving, ‘Introduction to Logic. Twelfth edition’ (New Jersey: Upper Saddle River 2005) 69.
11. Feteris, H. Kloosterhuis, ‘The analysis and evaluation of legal argumentation: approaches from legal theory and argumentation theory’ [2009] Studies in Logic, Grammar and Rhetoric, Vol. 16 (29).
12. A. Gutauskas, Lithuanian courts website. Rubric: Judicial system news. Available at: <https://www.teismai.lt/lt/naujienos/teismu-sistemos-naujienos/aurelijus-gutauskas-teisingumas-yra-ir-turetu-likti-zmogiskas/6388>.
13. C. G. Hazard, ‘The Legal and Ethical Position of the Code of Professional Ethics. Social Responsibility: Journalism, Law, Medicine’ [1979] Wash. & Lee Univ.
14. D. Hazel Genn, ‘Online Courts and the Future of Justice‘ [2017], Birkenhead Lecture.

15. G. Lastauskienė, ‘Teismų “interpretacinis žaismas” ir jo doktrininės prielaidos [Judicial "interpretative play" and its doctrinal assumptions]’ [2012] Jurisprudencija, T. 19 (4).
16. R. Latvelė, ‘Teisėjo vaidmuo aiškinant teisę: daktaro disertacija [The role of the judge in interpreting law]’ (Vilnius: Vilnius University 2010).
17. N. MacCormick, ‘Reasonableness and Objectivity’ [1999], Notre Dame Law review, Vol. 74.
18. A. Marmor, ‘Interpretation and Legal Theory’ (Oxford: Clarendon Press 1994).
19. R. A. Posner ‘Legal Formalism, Legal Realism, and the Interpretation of Statutes and Constitution’ [1986] Case Western Reserve Law Review, Vol. 37.
20. R. A. Posner, ‘Jurisprudencijos problemos [The Problems of Jurisprudence]’ (Vilnius: Eugrimas 2004).
21. H. Prakken ‘AI and Law, Logic and Argument Schemes’ [2005] Argumentation, Vol. 19 (3).
22. Ruling of 5 October 2010 of the Supreme Administrative Court of Lithuania in administrative case No A-143-972/2010.
23. G. Sartor, K. L. Branting, ‘Introduction: Judicial Applications of Artificial Intelligence’ [1998] Artificial Intelligence and Law.
24. H. W. Simon, ‘Role Differentiation and Lawyers’ Ethics: A Critique of Some Academic Perspectives’ [2010] Georgtown Journal of Legal Ethics.
25. B. L. Solum, ‘The Virtues and Vices of a Judge: An Aristotelian Guide to Judicial Selection’ [1988] Southern California Law Review, Vol. 61.
26. T. Sourdin, ‘Judge v Robot? Artificial Intelligence and Judicial Decision-Making’ [2018] UNSW Law Journal, Vol. 41 (4).
27. E. Spruogis, ‘Teisės aiškinimo probleminiai aspektai [Problematic Aspects of Interpretation of Law]’ [2006] Jurisprudencija, T. 8 (86).
28. S. R. Suumers, ‘Essays and Legal Philosophy’ (University of California Press: Berkeley and Los Angeles 1968).
29. R. Susskind and D. Susskind, ‘The Future of Professions’ (Oxford: 2015).
30. B. Sullivan, ‘Law and Discretion in Supreme Court Recusals: A Response to Professor Lubet’ [2013] Valparaiso University Law Review, Vol. 47.
31. O. Tene, J. Polonetsky, ‘Taming The Golem: Challenges of Ethical Algorithmic Decision Making’ [2017] North Carolina Journal of Law and Technology.
32. A. Valantiejus, ‘Charles Montesquieu ir ankstyvoji sociologinė tapyba [Charles Montesquieu and Early Sociological Painting]’ [2005] Sociologija. Mintis ir veiksmas.
33. B. W. Wendel, ‘Legal Ethics Is About Law, Not Morality or Justice: A Reply to Critics’ [2012] Texas Law Review, Vol. 90:72.
34. European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment, adopted at the 31st plenary meeting of the European Commission for the Efficiency of Justice (CEPEJ), Strasbourg, 3-4 December 2018 Available at: <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>.

THE GRAMMAR OF THE CONSTITUTIONAL COUNCIL: A NEW PERSPECTIVE IN INQUIRING OF JUDICIAL DECISION-MAKING PROTOCOL

Michael Koskas[1]

Abstract

This paper seeks to bring an approach 2.0 to the judicial process. It departs from the classical theories and tries to grasp the decision-making process through a micro-approach. Indeed, classical analysis of constitutional decisions are based on a macro-analysis that strives to find « types of behaviors » (using conceptual frameworks from political science and game theory, for example economic analysis of law). Facts are thus tapped for drawing up hypotheses to support them, instead of being used to analyze unique behaviors in a particular context. Far from such a deterministic perspective, the present research is built on an empirical internal analysis of decisions drafting and justification. Based on pragmatism, one of the analytical frameworks could result from the assessment of concrete situations, in order to best determine the reasons that lead judges to prefer one behavior to another (these theorizations could include the last outcomes of the action theory and theory of justification in particular, as well as the analysis of literary styles).

Keywords: Judicial decision making protocol, Constitutional Council, Pragmatic approach, Theory of law, decision making process.

Introduction

How do the judges decide? What factors influence their decisions? These questions are recurrent in academic work all over the world. Attempts to obtain answers are many. It has to be recognized that these questions remain, still today. In France, for example, the study of the supreme courts case law (Cour de cassation, Conseil d'État, Conseil constitutionnel) petered out. While opposing, two attitudes coexist among jurists for more than twenty years. A first, traditional and somewhat idealized, considers that the decisions of the judge meet his mission to build a unified, coherent legal order and overlooking ; another, more realistic, apprehends the jurisprudence of these institutions through large theoretical models such as the "strategic analysis", the "theory of legal constraints"[2] or the "economic analysis of law"[3]. These classic behavior assessment models, based on conceptual

[1] Phd student, Université Paris Nanterre, Centre de Théorie et Analyse du Droit. Teaching assistant in Administrative Law and Constitutional Law. Subject of the thesis: The Grammar Of The Constitutional Council: Micro approach Of The Judicial Decision Protocol Making. Former trainee in the French Constitutional Council (July to November 2017).

[2] M. Troper, C. Grzegorczyk, V. Champeil-Desplats (dir.) Théorie des contraintes juridiques, Paris, LGDJ et Bruylant, coll. « La pensée juridique moderne », 2005.

[3] E. Mackaay, S. Rousseau, L'analyse économique du droit, Paris, Dalloz, Méthode du droit, 2e éd., 2008.

frameworks from political science and game theory are now limited and reveal the need to appeal to new « micro » analytical frameworks to examine judges' behaviors. According to these models, judges have rational behavior in all circumstances. This paper aims to depart from this point of view with a micro approach which takes into account the existence of a plurality of rationality for each actor.

This approach I am suggesting here, approach 2.0 of the judicial decision making protocol, strives to overcome these two ways to understand how the judges decide. This contribution tries to expose a more contextual approach, which could be described as "micro": the idea is questioning the activity of the constitutional judge through the study of his social environment, more precisely the internal jurisdictional process. In the same way that the grammar constitutes the set of rules to be followed in order to express oneself correctly in a language, the aim of this contribution is to give an account of all the structural rules that judges (and their assistants) tend to respect in their practice, as we are able to observe them; this is what I call the grammar of the Constitutional Council[4].

It is clear from my point of view, that it is only through the application of an adequate theoretical framework and a rigorous methodology that this grammar will be able to provide precise and relevant lessons on the jurisdictional process. In this regard, the proposed approach draws its inspiration from several schools of thought such as the young school of pragmatic sociology developed by Luc Boltanski and Laurent Thévenot[5], or, little known yet, the American anthropology of law, with authors like Annelise Riles[6] or Marina Valverde[7]. Both of these perspectives provide valuable insights into the "follow-up of professionals". Inspired by such theoretical and methodological approaches, my perceptive is armed with tools that favor the development of a legal study that is both non-essentialist and non-reductionist; or, in other words, an approach which is interested in constitutional litigation as it really exists, or "still in process of making", to use the words of the pragmatist philosopher William James[8].

Aiming at understand the decision-making protocol, this methodology suggests an attitude that is not widespread among French and international lawyers, by approaching the jurisdictional process as closely as possible. Still, it must be recognized that this approach is often difficult for lawyers, but *in situ* observation is not the only way to adopt an internalist approach: conducting interviews with judges and assistants (litigation staff within jurisdictions) is also useful to teach us a lot about the rules of an institution.

The cross-checking and exploitation of these data make possible to identify the presence of typical material and organizational processes within the jurisdictions: the legal devices ("dispositifs juridiques" in French). The latter aim to guide the behavior of individuals by conveying a certain conception of law - the editorial style of the decisions, the internal organization of the different services, the form of the documents made available to judges,

[4] For more informations about the concept of "grammar" see C. Lemieux, La sociologie pragmatique, Paris, La Découverte, Repères, 2018, p. 58-60.
[5] L. Boltanski, L. Thévenot, De la justification. Les économies de la grandeur, Paris, Gallimard, 1991 ; Y. Barthe, et al. « Sociologie pragmatique : mode d'emploi », Politix, vol. 103, n° 3, 2013, p. 175-204, p. 176 ; C. Lemieux, op. cit.
[6] A. Riles, « Models and Documents: Artefacts of International Legal Knowledge », International and Comparative Law Quarterly, 48, 4, 1999, p. 805-825 ; also The Network Inside Out, Ann Arbor, The University of Michigan Press, 2000.
[7] M. Valverde, v. Law's dream of a common knowledge, Princeton, Princeton University Press, Cultural lives of law, 2003 ; also « The Sociology of Law as a 'Means against Struggle Itself ' », Social & Legal Studies, 2006, vol. 15, n°4, p. 591-597.
[8] W. James, The Meaning of Truth, New York, Longmans, Green & Co Editor, 1909.

the deliberative process are examples. In the same way, and contrary to what the great theoretical models claim, the exploitation of the deliberative reports reveals a plurality of rational behaviors at a given instant that can be modeled through a typification of observed behaviors[9].

The contribution for the legal studies of this microapproach is indeed very important. It helps to better understand certain legal constructions, such as the application of the principle of proportionality. It also helps to understand the rise of some unwritten rules such as the adoption of an internal procedural ruling applicable before the Constitutional Council for the control of the constitutionality of ordinary laws, treaties, and regulations of the houses of the Parliament.

To illustrate this approach, I choose to focus on the French Constitutional Council, which is the subject of my doctoral thesis. For five months, I carried out an internship within the documentation department (from July to November 2017) where I was able to contribute to the preparation of the decisions. For the moment, I also make twenty-three interviews with the people in charge of litigation. These resources are valuable in the development of a micro approach of the judicial process.

To expose it, I will try to show how the grammar was instituted within the Constitutional Council. That is to say, how the operating rules within this institution were established. In a second part, I will show that this grammar should be understood as dynamic and evolutionary. My ambition here is modest : in this brief contribution, I wish to expose my approach by taking a telling example which characterizes the singularity of the Constitutional Council : the presence of a single legal service and the absence of individual assistants for judges. This example is, in my opinion, very revealing of the specificity of the grammar of the Constitutional Council.

1. The adoption of the constitutional grammar

How was constitutional grammar adopted? This question implies to ask oneself about how were adopted rules that judges and their assistants tend to respect in their practice, as we are able to observe them. Observing the practices of judges, by means of a rigorous methodology will allow a better understanding of the law; our tools is in-situ observation ("follow-up of professionals") and the interviews, the reading of testimonies and secondary documents annexed to the Constitutional council decisions.

The study of all these empirical sources reveals the contextual constraints. By borrowing from Michel Foucault the concept of “device”, the sociologist Bruno Latour[10] has notably tried to reveal the pragmatic constraints (human and material) experienced by the actors in their daily lives[11]. An example of a device is represented by Michel Foucault by the architectural structure of the panoptic: by allowing, in a penitentiary establishment, to

[9] M. Xifaras, « Théorie des personnages juridiques », RFDA, 2007, p. 275-287.
[10] B. Latour, Pasteur : guerre et paix des microbes Suivi de Irréduction, Paris, La Découverte, 2011 [1re éd. 1984] ; see also : M. Callon, B. Latour, La science telle qu'elle se fait. Anthologie de la sociologie des sciences de langue anglaise, Paris, La Découverte, 1991
[11] For more informations about judicial device, see M. Koskas « Le dynamisme de la proportionnalité : enjeux de la fragmentation tripartite du principe dans le processus juridictionnel », La Revue des droits de l’homme, n°15, 2019.

monitor prisoners without being seen, it encourages prisoners to adopt a certain type of behavior, "the good" behavior[12].

According to Bruno Latour's reasoning, and if we transpose it, the courts would not be spared by the deployment of devices that encourages judges and assistants to follow a certain attitude; the ambition to uncover such devices obviously contributes to a better understanding of the judicial process. So, as in other jurisdictions, legal provisions rule the functionning of the Constitutional Council. These legal devices influence behaviors, so that they are constitutive of the grammar of the Constitutional Council.

But what is interesting is that was not initially a jurisdiction. To say it quickly, the Constitutional Council was created in 1958 to frame the prerogatives of the Parliament which was causing government's instability during the French Fourth Republic ; it was a regulating chamber of the public authorities, more than a jurisdiction[13]. Thus, at the Constitutional Council, the legal devices for their majority come from Parliament. For example, the legal service includes two administrators from parliamentary assemblies.

The study of the testimonies tends to show that these administrators put forward similarities between their functions in the Parliament and the Constitutional Council. For example, a judge (a former deputy or senatory) drew a parallels between the reports made by the administrators of the assemblies and the reports of the legal service in the Constitutional Council.

The report from the general secretary [i.e. document made by the jurists] looks like what I knew in Parliament. It is a very well done document that perfectly summarizes the parliamentary debates and the issues that come up during the meetings. I rely a lot on this work of the jurists. [...] Their work here [at the Constitutional Council] looks like to what they did as an administrator of the assemblies in Parliament: before they made reports for parliamentarians and now they make reports [legal notes] for us, the members of the Constitutional Council[14]

Such a representation of work is also found in the testimonies from a jurist who is also an administrator in Parliament:

There are many similarities between the task I do in the Constitutional Council and the work I do in Parliament. The administrator follows the rapporteur [ie the rapporteur in the Parliament]; the administrator will write a draft report to the rapporteur who may say "it suits me". As the administrator of the Parliament, I was not disoriented by the working methods of the Constitutional Council, there is always, as in the Parliament, a legitimacy that must be respected [i.e. the judge at the Constitutional Council and the legislator in the Parliament][15].

Thus, these testimonies reveal that the legal devices do exist in the Constitutional Council. This institution chooses to use the services of the administrators and encourages them to use their working methods, so that the grammar of the Constitutional Council has progressively been constituted and affirmed distinct from that of a court.

---

[12] M. Foucault, Dits et écrits 1954-1988. Tome III: 1976-1979, Paris, Gallimard, 1994; see also field « le dispositif entre usage et concept », in Hermès La revue, 1999-3, n° 25, p. 9-242. See also, H. Dumez « Qu'est-ce qu'un dispositif ? Agamben, Foucault et Irénée de Lyon dans leurs rapports avec la gestion », Le Libellio d'Aegis, volume 5, n° 3, 2009, p. 34-39.

[13] H. Roussillon, P. Espuglas, Le Conseil constitutionnel, Dalloz, Connaissances du droit, 8e éd., p. 7-13.

[14] Interview with a judge

[15] Interview with a jurist

However, in some ways, the grammar of the Constitutional Council tends to get closer to a third room. Indeed, some established devices are sometimes borrowed from a jurisdiction such as the Council of State. It the case of the drafting style of the decisions structured with the “visas” and the “considerants”, reminds us the construction of the decisions of the supreme administrative court. Thus appear all the specificities of the grammar of the Constitutional Council, which integrates both behaviors of a parliamentary chamber and at the same time those of a jurisdiction.

The testimony of a member of the Council of State, comparing the drafting methods to the Constitutional Council is, in this respect, enlightening. The person interviewed was an administrative judge who worked, during five years, at the Constitutional Council.

The Constitutional Council shares the same culture as the Council of State regarding the drafting of decisions. There is a lot of reviews and everyone re-reads everyone. The decision is made by several hands and, at each stage, there is a review phase.

There would be many other examples to highlight this constitutional grammar, such as the fact that there is only a single legal service or the specific deliberative process.

The grammar of the Constitutional Council borrows from various institutions such as the Parliament or the Council of State, but at the same time it is different from a court or of a parliamentary chamber. This is precisely all these loans that constitute the specificities of the constitutional grammar.

I do not presuppose, on the one hand, that the grammar exists outside any human organization. On the other hand, I do not deny the existence of this grammar: that is to say I do not think that there are only individual behaviors without links between them (this concept is close to methodological holism[16]). So, I have to think about the determination of this grammar of action. That is the purpose of the second part of this paper.

2. The dynamism of the grammar

Where do the functioning rules of an institution come from? Does the Constitutional Council present some specific features when it dispenses constitutional justice? How are such rules reformed? Referring to a set of behaviors mobilizable by the constitutional judge, the grammatical structure is seen as a possibility to carry out many actions, as well as a limit to what can be done. It is at the same time a bound and a source of initiative for the constitutional judge.

2.1. Reforming the legal devices to influence the behaviors

The behavioral rules that can be observed within an institution are not frozen but can evolve through the time, with the evolution of the social environment. Such an evolution often undergoes through reforms of the legal devices, more precisely of the processes which tend to influence the behaviors in a particular space. Indeed, as I demonstrate previously, when choosing to institute certain devices rather than others, one decides to direct the behaviors towards a determined line. In France, the Constitutional Council has chosen not to

[16] C. Lemieux, op. cit., p. 59.

use all the legal devices which would go towards a juridictionalisation, such as the choice not to adopt a procedural ruling for the *a priori* litigation. Such a refusal is obvious when reading the testimonies of the former members of the institution, as well as when reading of the former deliberation reports. As a matter of fact, the former members considered that the presence of such a text was not necessary because of the need to treat the litigation within a short time[17].

Nevertheless, a desire to accentuate the jurisdictional nature of the institution appeared in 2010 in the Constitutional Council. There was a desire expressed by former President Jean-Louis Debré to accentuate the jurisdictional nature of the institution[18]. This has resulted in the recent introduction of the Regulation of 4 February 2010 on the procedure applicable before the Constitutional Council for priority matters of constitutionality.

In revealing words, the former Secretary General of the Constitutional Council Marc Guillaume explains the issues involved in the creation of this regulation.

The creation of such *a posteriori* control implies the definition of a new procedure radically different from that in force for the *a priori* control. The two judicial devices will coexist, each responding to different natures. The new procedure will be of a jurisdictional nature, the intervention of the Council itself is part of a jurisdictional procedure[19].

The implementation of these Regulation on procedure, and establishes a legal devices. It leads to a change in the behavior of the actors of the Constitutional Council. With the entry into force of the “priority preliminary ruling on the issue of constitutionality” (QPC in French)[20], there was also the establishment of a real Registry and a calendar for the investigation of cases (deadlines for the receipt of the written submissions of the parties, ten minutes for the pleadings of the lawyers). All these reforms of legal devices tend to institute a jurisdictional grammar. There are other examples, witnesses of an accentuation of the jurisdictional grammar such as the setting up of a courtroom.

Setting up of the priority preliminary ruling on the issue of constitutionality show that legal devices can evolve, and therefore the grammar is not fixed and for all. With their dynamism, the legal devices, influencing the behaviors in a jurisdiction. They constitute instruments to influence the grammar of the Constitutional Council.

2.2. Influencing the behaviors through the use of legal devices

[17] B. Genevois, « La jurisprudence du Conseil constitutionnel en 1986 », Annuaire international de justice constitutionnelle, p. 411-464, p. 416 ; La jurisprudence du Conseil constitutionnel : principes directeurs, Paris, Sth, 1991. O. Schrameck, « Les aspects procéduraux de la saisine », in "20 ans de saisine parlementaire" » Economica, 1994 ; J.-É. Schoettl, « ma cinquantaine rue de Montpensier, Cahiers du Conseil constitutionnel », Les Nouveaux cahiers du Conseil constitutionnel, 2009 https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/ma-cinquantaine-rue-de-montpensier ; M. Guillaume, « La procédure au Conseil constitutionnel, permanence et innovations », p. 519-532, p. 530.

[18] J.-L. Debré, Audience de rentrée solennel de la Cour administrative d’appel de Versailles et du tribunal administratif de Versailles , Versailles, in Mélanges Genevois, Paris, Dalloz,17 octobre 2011.

[19] M. Guillaume, op. cit., p. 530.

[20] An "application for a priority preliminary ruling on the issue of constitutionality" is the right for any person who is involved in legal proceedings before a court to argue that a statutory provision infringes rights and freedoms guaranteed by the Constitution. For more information about this procedure, see https://www.conseil-constitutionnel.fr/en/selection-of-qpc-decisions

Of course, the legal measures limit the possibilities of action of the constitutional judge : by choosing to guide behaviors by the implementation of certain devices, it also limits the possibilities of action of the person to other behaviors. Establishing a legal device is therefore, in a way, binding on the constitutional judge.

To illustrate this idea, I'll take the revealing case of the presence of a single legal service at the constitutional council. Unlike their German or Italian neighbors, French constitutional judges, as we know, do not have personal assistants or, to use Belgian terminology, referendaries. It is a unique legal service that assists members and contributes, often to a considerable degree, to the preparation of decisions. In addition to the Secretary-General and the part-time officers, this structure is made up of four full-time, non-statutory staff members seconded from their original administration (the judiciary, the two assemblies of the Parliament[21]).

This organizational originality thus constitutes a device in the Foucaldian sense of the term. Indeed, it encourages the constitutional judge to act in a certain way, to produce a certain type of determined behavior. The legal device "single legal service" incites for example, to encourages the search for a form of consensus among members[22]. It carries out an important work of synthesis of the principal legal arguments exchanged by the parts and a selection of the case law relating to each case.

The legal service therefore, in a way, controls the choice of solutions offered to the College of judges at the time of the deliberations with an horizon of possibilities – the legal service proposes a limited number of solutions. And it is most often only within this horizon of possibilities that the judges opposed to the orientation finally chosen by the rapporteur, are able to propose counter-draft decisions - in addition to themselves written by the single legal service and not by the member himself. This legal device, single judicial service, thus limits the possibilities of action of the judge, it is thus binding for the constitutional judge.

But this pragmatic constraint is not absolute. Of course, it is often easier for the judge to follow the solutions proposed by the legal service. But there is nothing to stop him from doing a job himself to persuade its colleagues that the solution proposed by the legal service is not the most convincing.

To resume the testimony of an other judge of the Constitutional council:

I have already gone against the solution proposed by the legal service. It was not easy, I did a lot of work about the case and I managed to convince the College of the merits of my solution[23].

We can see, with this example, that the legal devices established in a jurisdiction are not absolutely binding. Indeed, the judge can go against the legal service solution.

Conclusions

[21] More specifically, the legal service consists of two judges (one administrative and the other judicial) and two adinistrators of the assemblies (one of the National Assembly and the other of the Senate).
[22] J.É. Schoettl, « Les coulisses du contrôle de constitutionnalité en France », Justice & Cassation, 2007, p. 157-169.
[23] Interview with a judge.

Drawing the outline of a study which will be larger and much more detailed, the approach developed in this paper seems nevertheless suitable to suggest a new “micro” analysis (to use the terms borrowed from the economic and sociological analysis) of the decisions ruled by an institution (or a jurisdiction) as the Constitutional council. Furthermore, it constitutes a preliminary study that would precede a critical analysis dealing with the reform of material and environmental devices within these institutions. These are the various tasks that might fall to young legal studies.

Bibliography

1. M. Troper, C. Grzegorczyk, V. Champeil-Desplats (dir.) *Théorie des contraintes juridiques*, Paris, LGDJ et Bruylant, coll. « La pensée juridique moderne », 2005.
2. E. Mackaay, S. Rousseau, *L’analyse économique du droit*, Paris, Dalloz, Méthode du droit, 2e éd., 2008
3. C. Lemieux, *La sociologie pragmatique*, Paris, La Découverte, « Repères », 2018.
4. L. Boltanski, L. Thévenot, *De la justification. Les économies de la grandeur*, Paris, Gallimard, 1991.
5. Y. Barthe, et al. « Sociologie pragmatique : mode d’emploi », *Politix*, vol. 103, n° 3, 2013, p. 175-204, p. 176.
6. A. Riles, « Models and Documents: Artefacts of International Legal Knowledge », *International and Comparative Law Quarterly*, 48, 4, 1999, p. 805-825.
7. A. Riles, *The Network Inside Out*, Ann Arbor, The University of Michigan Press, 2000.
8. M. Valverde, v. *Law’s dream of a common knowledge*, Princeton, Princeton University Press, coll. « Cultural lives of law », 2003.
9. M. Valverde, « The Sociology of Law as a ‘Means against Struggle Itself ’ », *Social & Legal Studies*, 2006, vol. 15, n°4, p. 591-597.
10. W. James, *The Meaning of Truth*, New York, Longmans, Green & Co Editor, 1909.
11. M. Koskas « Le dynamisme de la proportionnalité : enjeux de la fragmentation tripartite du principe dans le processus juridictionnel », *La Revue des droits de l’homme*, n°15, 2019.
12. M. Xifaras, « Théorie des personnages juridiques », *RFDA*, 2007, p. 275-287.
13. B. Latour, *Pasteur : guerre et paix des microbes* Suivi de *Irréduction*, Paris, La Découverte, 2011 [1re éd. 1984].
14. M. Callon, B. Latour, *La science telle qu'elle se fait. Anthologie de la sociologie des sciences de langue anglaise*, Paris, La Découverte, 1991.
15. M. Foucault, *Dits et écrits 1954-1988. Tome III*: 1976-1979, Paris, Gallimard, 1994.
16. H. Dumez « Qu'est-ce qu'un dispositif ? Agamben, Foucault et Irénée de Lyon dans leurs rapports avec la gestion », *Le Libellio d'Aegis*, volume 5, n° 3, 2009, p. 34-39.
17. H. Roussillon, P. Espuglas, *Le Conseil constitutionnel*, Dalloz, Connaissances du droit, 8e éd., p. 7-13
18. B. Genevois, « La jurisprudence du Conseil constitutionnel en 1986 », *Annuaire international de justice constitutionnelle*, p. 411-464.
19. B. Genevois*, La jurisprudence du Conseil constitutionnel : principes directeurs*, Paris, Sth, 1991

20. O. Schrameck, « Les aspects procéduraux de la saisine », *in "20 ans de saisine parlementaire"* » Economica, 1994.
21. J.-É. Schoettl, « ma cinquantaine rue de Montpensier, Cahiers du Conseil constitutionnel », Les Nouveaux cahiers du Conseil constitutionnel, 2009.
22. M. Guillaume, « La procédure au Conseil constitutionnel, permanence et innovations », in *Mélanges Genevois*, Paris, Dalloz, 2009 p. 519-532
23. J.-L. Debré, Audience de rentrée solennel de la Cour administrative d'appel de Versailles et du tribunal administratif de Versailles , Versailles, 17 octobre 2011.
24. J. É. Schoettl, « Les coulisses du contrôle de constitutionnalité en France », *Justice & Cassation*, 2007, p. 157-169.

REGULATORY STRATEGIES FOR ACCOUNT INFORMATION SERVICE PROVIDERS (AISPs) AND PAYMENT INITIATION SERVICE PROVIDERS (PISPs) UNDER PSD2

Marcin Krzemień[1]

Abstract

The Payment Services Directive 2 (PSD2) introduced third-party players (TPPs) to the EU regulatory landscape. Those players – Account Information Services Providers (AISPs) and Payment Initiation Services Providers (PISPs) are peculiar types of payment institutions which do not themselves hold any funds on behalf of their customers, but instead heavily rely on the existing infrastructure of entities which do so (primarily - of universal banks). At the same time, their core function requires them to access some very sensitive consumer data (so far – mostly reserved for banks) and communicate with other players in the financial space (again – mostly banks) in a swift, secure and accurate manner. As such, they pose a unique challenge for the EU regulator. This article looks at the regulatory strategies used in the PSD2 uses in order to assure security of operations of AISPs and PISPs for their end customers.

Keywords: PSD2, electronic payments, fintechs, open banking, financial regulation

Introduction

The Payment Services Directive 2 Directive (Directive (EU) 2015/2366 - PSD2) which entered into force in January 2018 "provides the legal foundation for the further development of a better integrated internal market for electronic payments within the EU"[2]. In essence, it updates the regulatory regime for the so-called 'payment institutions' operating in the EU. Within the meaning of PSD2, a payment institution is an entity which performs payment services as described in the Annex 1 to PSD2. Those services encompass operations such as: depositing, withdrawing and transferring funds to and from user's (electronic) payment account[3].

Discussing the full scope of PSD2 is of course well beyond the scope of this article. I will focus on one aspect of the directive – the rules concerning the so-called "access to account". Those rules allow certain types of third-party actors (third party providers – TPPs) to access the customer's primary bank account information if he or she authorizes them to do so in order to provide services for said customer.

The article will proceed as follows: First, the author will briefly characterize some of the features of payment institutions in general which cause them to fall within the scope of

[1] The author is a PhD student at the Chair of European Law of the Faculty of Law of the University of Warsaw,
[2] Summary of the PSD2: https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32015L2366
[3] Directive 2015/2366 (PSD2) – Annex 1

regulatory umbrella. Second, I will describe types of third party providers introduced in PSD2, their role and unique characteristics. Third, I will analyze the regulatory strategies used by the EU regulator with respect to those entities. Finally, I will conclude.

Why payment institutions should be regulated

Historically, the payment system had been operated by universal banks. However, in the last decade many new players – mostly from the technological or fintech space – have entered the playing field and have been trying to provide some of the same services that banks have been providing for so many years.

The payment system has 3 common features of the utmost importance for the end customer. It provides him or her with storage – i.e. a place where money can be safely stored and where its value will always be correctly accounted for; liquidity – meaning that the customer may generally withdraw the funds from the system on his or her demand in order to enter into a transaction; and transfer – meaning that the customer can transfer his funds from his or her possession to another participant of the financial system in an organized manner[4].

Banks have been uniquely positioned to perform those functions because of the regulatory regime they have been historically subject to (and underlying this regime – financial guarantees of sovereign states). Even under heavy institutional stress banks have generally been able to provide their customers with liquidity, storage and transfer functions. New entrants - while they might be able to perform those functions as well as universal banks under normal conditions – have largely been outside the regulatory umbrella[5].

The European Union has been trying to mitigate this issue by way of creating the category of 'payment institution' (described in the introduction to this article) and creating a regulatory regime tailored specifically for those institutions. The main regulatory strategy used by the PSD2 in order to mitigate the risk of payment institutions is a mixture of capital requirements and various portfolio restrictions imposed on those institutions. Article 9 of PSD2 provides that payment institutions shall at all times hold their own funds of a certain amount (calculated e.g. based on the total volume of payments serviced in the past) – [minimum capital requirements], while article 10 of PSD2 stipulates that the funds stored with them by their customers must be properly safeguarded [portfolio restrictions].

Discussing the pros and cons of the above strategies is well beyond the scope of this article. These strategies are tailored for payment institutions which actually hold funds on behalf of their customers (which in itself is a large potential source of risk). However, the PSD2 introduces a new category of payment institutions – the third party providers – which do not hold funds on behalf of their customers and as such must be subject to a different regulatory regime. They are the main focus of this short article.

Third party providers under PSD2

[4] J. Armour et al – Principles of Financial Regulation, Oxford 2016, p. 391

[5] D. Awrey, K. van Zweiten – "The Shadow Payment System", 2018 - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2843772&fbclid=IwAR2Mk7mBJB3LlAFgJIrCYs6GJSRytCawpdUqnZ5eEFTNbLGyHkUWjWyXOkg, p. 10

PSD2 introduces a new type of payment institution – the so-called third party provider (TPP). In order to better understand this concept, it is best to think about TPPs in terms of practical services they are envisaged to perform under PSD2. PSD2 divides TPPs into 2 groups – Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs).

AISPs provide the customer with information from one or more of his or her bank accounts. In basic terms, they can access the same information that you could see in your bank account(s), aggregate and/or repackage it and then subsequently display it to the customer (perhaps in a clearer or more robust manner) to his or her benefit. Sample uses of such a services may include budgeting apps or price comparison websites[6].

PISPs on the other hand are used to initiate a transaction between the customer and a third party merchant (say: an e-commerce store) while the actual transaction is to be cleared with the merchant via the customer's bank. A standard use-case of a PISP (for a single, debit transaction) could go like this: A user buys a product from a third-party merchant. In order to pay for that product, he or she initiates payment via the PISP, authorizing it to initiate the transaction. The PISP then informs the customer and the merchant that the said transaction has been initiated. Subsequently, it instructs the customer's bank that it has been authorized to initiate the transaction and that the merchant should be paid a specified amount. The bank itself then clears the transaction with the merchant[7]. As it has been pointed out by the FCA, in doing so, PISPs allow the customer to conveniently pay the merchant using his or her bank and thus may provide an alternative to using a credit or debit card and the card-issuing company (Visa or Mastercard) infrastructure in the process[8].

Following this brief characterization of the functions performed by AISPs and PISPs, one can point out several distinct features of those two peculiar types of payment institutions.

First, at no point do they hold funds of the customer. AISPs aim in essence to give the customer an image of what is going on in his or her bank account(s), thus performing mainly an information function. PISPs on the other hand – as their name indicates – merely initiate the transaction which is technically executed via the customer's bank. They assist the customer in performing the transfer function (as characterized in point 2 of this article) but they do not perform the storage one. In performing their services, both AISPs and PISPs rely fully on existing infrastructure of PSPs (mainly – universal banks) and thus 'piggyback' on it.

Second, both AISPs and PISPs require explicit user consent in order to provide their services. The data that they handle is quite sensitive – for AISPs it is information concerning detailed account (transaction) information from one or more accounts of the customer . PISPs on the other hand request the PSP (bank) to execute a transaction to a third party on customer's behalf. Therefore, robust mechanisms of user authorization, monitoring and registering his or her consent to provide such service must be in place.

[6] https://www.fca.org.uk/account-information-service-ais-payment-initiation-service-pis

[7] EY – The Revised Payment Services Directive (PSD2) – What you need to know, https://www.ey.com/Publication/vwLUAssets/Regulatory_agenda_updates_PSDII_Luxembourg/$FILE/Regulatory%20agenda%20updates_PSDII_Lux.pdf p. 3

[8] https://www.fca.org.uk/account-information-service-ais-payment-initiation-service-pis

Third, in the same vein, both AISPs and PISPs rely heavily on communication between themselves and the customer's bank (PSP). In order for the AISPs and PISPs to do their job properly, this communication must be precise (accurate), quick and secure. This need was recognized by EU legislators in article 98 of PSD2. Article 98.1(d) stipulates that EBA should publish requirements for common and secure open standards of communication for the purpose of identification, notification information and implementation of security measures between banks, PISPs and AISPs[9].

Fourth, the relation between banks and AISPs / PISPs and banks is not a contractual one. The PSD states quite clearly that both types of third party players operate solely on the basis of customer's authorization and consent. If the customer authorizes either an AISP to access his or her account(s) information or a PISP to initiate a transaction on his or her behalf, the PSP (bank) must oblige and enable the third party players to communicate with itself in order for them to be able to perform their service.

Following this brief analysis, we can see that the AISPs and PISPs are a peculiar type of payment institution characterized by their heavy reliance on communication with PSPs (banks) and their technical infrastructure, which do not hold customer funds, but in performing their service necessarily have access to sensitive user data (account information for AISPs, requests to execute transactions for PISPs). We will now analyze the regulatory strategies used by the EU legislators in order to tackle those particular characteristics.

Regulatory strategies for AISPs

As it has already been hinted at, the main risk associated with the activities of AISPs is associated with the extremely sensitive type of information they may potentially gain access to (bank account history of a particular customer) and is one of fraud.

The scope of the regulatory regime that the AISPs are subject to is presented in article 33 of PSD2. The first thing to note is that AISPs are exempt from most regulatory duties that 'standard' payment institutions are subject to by virtue of the fact that they do not at any point hold customer's funds.

The core characteristic of AISPs (and likewise – of PISPs) is that they rely or 'piggyback' on existing infrastructure of the PSP (bank). An AISP merely analyzes – slices, dices and presents – information from customer's account or accounts. What happens in that account – the safety of funds therein, security, speed and accuracy of operations – is the worry of the PSP – usually a universal bank or a different 'standard' payment institution subject to a much more robust prudential regime. Such a regulatory strategy has been described as "piggybanking"[10].

As such, AISPs are exempt from the minimum capital requirements provided for in article 7 of PSD2. They are also exempt from the duty of article 11 of PSD2 – that is, the need to receive authorization in order to commence payments. They have to merely register with the competent authority of the host Member State per article 14 of PSD2 (and are later evidenced in the EBA register per article 15). Furthermore and more importantly – they are

[9] PSD, article 98.1(d)
[10] D. Awrey, K. van Zweiten, op. cit., p. 31

exempt from the two main mechanisms that PSD2 uses in order regulate 'standard' payment institutions which do perform the storage function (unlike AISPs and PISPs), which were briefly described in point 2 of this article. They do not to hold their own funds against any potential claims of their customers in the event of institutional stress (since they do not have on their bosk any funds of their customers as liabilities – again they merely perform an information function) and they do not have to safeguard the funds in any way (since they do not hold them – that obligation will be faced by the PSP).

AISPs are, however, still subject to normal supervision from the competent prudential authorities in the host Member State. Per article 23 they may be e.g. requested to provide all necessary information to the said authorities or be subject to an on-site inspection. In the course of commencing its operations, they must also present the supervisors with certain documentation specified in article 5 of the PSD2 – namely business and operational plan, operational structure and last but not lease – measures in place that ensure robustness of security mechanisms. That is especially important in the context of the particular mode of operations of AISPs and risks associated with it as indicated above.

However, the one crucial measure that the AISPs are subject to is the specified in article 5.3 of PSD2. That provision stipulates that all AISPs shall hold an indemnity – that is third party insurance – which will be able to protect both the customer and the PSP (bank) in case of customer data being accessed fraudulently. As it has already been indicated, provision of services by the AISP relies heavily on communication with the bank and obtaining clear and explicit user consent and fraud or unauthorized access to this information is the biggest risk associated with AISPs operations. In the author's view the EU regulator has correctly identified the largest risk factor for the customer associated with the existence of AISPs (fraud) and targeted it with an appropriate regulatory measure. One may think of the third party insurance (indemnity) as a secondary 'guarantee' being placed on the customer's bank account due to the fact that he or she decided to use an AISP's services and grant it access therein. Should anything happen with the customer's account due to AISP's operations (i.e. a fraudulent third party will access the account and cause loss to the customer), he or she will be indemnified for the damage by an independent third party insurer.

Regulatory strategies for PISPs

The PISPs are somewhat similar to the AISPs in the sense that they as well do not hold the funds of their customers at any point during the provision of the payment initiation service. Likewise, they rely – or piggyback – on the existing architecture of other players in the payment space – the PSPs. As it has been described in point 3 of this article, a PISP merely instructs the PSP (usually bank) to execute a transaction on the customer's behalf. The security, speed and correctness of the transaction is assured by the bank itself.

Therefore, it should come as no surprise that - like the AISPs - PISPs are not required to hold their own funds (against potential claims of the customers – their customers have no open balance with them and therefore, there is no liability on the side of the PISP) or safeguard the (non-existent) consumer funds.

Like the AISPs, the most pervasive risk associated with the operations of a PISP is one of fraud. In the opinion of this author, due to how a PISP operates relatively to an AISP,

this risk is even more prevalent and that is visible in the stricter regulatory regime applied to PISPs relatively to AISPs by the EU regulator.

PISPs at its core function may not only access some very sensitive information while communicating with the customer's bank (PSP). More importantly, they instruct the said bank/PSP to execute a transaction to a third party on user's behalf. This 'active' function performed by the PISPs first of all – increases the risk of fraud already existing in the case of AISPs (because of how PISPs operate there is potential for a fraudulent third party to try and initiate an unauthorized transaction) and secondly – creates a different risk – one associated with a late or faulty execution of the transaction (which may in effect result in a loss on the side of the consumer).

Those differences – and more potent risks – associated with PISPs due to the peculiarities of their business model – are visible in how PISPs are regulated under PSD2. Unlike the AISPs, there is no mirror provision such as article 33 for PISPs which would exempt those institutions from much of the scope of PSD2 regulatory regime. As such, PISPs are subject to full filing duties under article 5 of PSD2, they are required to become authorized in order to commence operations under article 11 and are faced with minimum capital requirements under article 7 (albeit the requirement of EUR 50 000 minimum capital is significantly lower than EUR 125 000 for 'standard' payment institutions). Specifically, article 11.5 of PSD2 stipulates that competent authorities may require structural separation of payment vs. non-payment function for an entity engaging in payment initiation services provision – there is no similar provision for AISPs.

Similar to AISPs however, the main regulatory strategy used by the EU legislators to mitigate the risk associated with operations of PISPs is indemnity / third party insurance. Article 5.2 of PSD provides that PISPs should hold an indemnity insurance that could cover specific liabilities specified in articles 73, 89, 90 and 92 of PSD2. Those liabilities correspond to the risks already described above – one of fraud (fraudulently initiating and subsequently executing – via bank – a transaction unauthorized by the consumer) and late or faulty execution of the transaction. The crucial point here is that - according to PSD2 – in the event that the customer suffers a loss due to either fraud or faulty executed transaction, the burden of proof lies on the PISP (to prove that they were not at fault).

Conclusion

Both AISPs and PISPs are a peculiar type of payment institutions in a sense that they do not at any point hold funds on behalf of their customers. As such, they must be subjected to a specific mix of regulatory strategies which correspond with their characteristics. Normally, payment institutions perform all or some of the functions historically performed by banks – namely provide their customers storage, liquidity and transfer functions. AISPs perform none of those functions (they perform a crucial information function but do not themselves participate in the transfer or storage of money), while PISPs merely assist in the transfer function. None of them perform liquidity or storage function.

As such, the usual mechanisms used to provide security of payment institutions (portfolio restrictions or capital requirements) are useless in regulating AISPs or PISPs. That is not to say however, that they are fully safe and subject to no risk. The major risk stemming from the operations of both AISPs and PISPs is one of fraud (and for PISPs – of wrongly initiating and executing a transaction). The instrument used by the EU legislators - third

party insurance – seems to be the correct one to tackle such risk type, however we have yet to see how successful it will be in reigning in those risks. We have yet to see how big the appetite of private third-party insurers will be for actually insuring those kind of risks. Secondly, it has been indicated that third-party insurance does very little to tackle systemic risks (however, risks that we are discussing in relation to AISPs and PISPs do not on face value seem to be systemic in their nature)[11].

Finally, a diligent reader may ask – what all the fuss is about? The PSD2 has been in force for over a year and many have been hailing the arrival of PSD2, AISPs and PISPs as revolutionary. Meanwhile, most people – even well-versed in the world of finance – would probably find it difficult to name even a few PISPs or AISPs. The EBA register shows only a couple dozen of each of those entities registered in total so far in the EU[12]. The reason for that is the regulatory and technical standards – necessary to ensure crucial communication between banks and AISPs and PISPs (in other words official instructions on how banks should allow access to its systems for PISPs and AISPs by way of API and what security mechanisms both banks and AISPs and PISPs should have in place) have not yet entered into force and will do so only in September 2019[13].

Bibliography:

1. Payment Services Directive 2 - Directive (EU) 2015/2366
2. Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication
3. J. Armour, D. Awrey, P. Davies, L. Enriques, J. Gordon, C. Mayer, J. Payne – Principles of Financial Regulation (Oxford 2016)
4. D. Awrey, K. van Zweiten – "The Shadow Payment System", 2018 - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2843772&fbclid=IwAR2Mk7mBJB3LlAFgJIrCYs6GJSRytCawpdUqnZ5eEFTNbLGyHkUWjWyXOkg
5. https://www.fca.org.uk/account-information-service-ais-payment-initiation-service-pis
6. EY – The Revised Payment Services Directive (PSD2) – What you need to know, https://www.ey.com/Publication/vwLUAssets/Regulatory_agenda_updates_PSDII_Luxembourg/$FILE/Regulatory%20agenda%20updates_PSDII_Lux.pdf
7. PwC guide – PSD2 in a nutshell: https://www.pwc.com/it/en/industries/banking/assets/docs/psd2-nutshell-n03.pdf
8. EBA Register of payment and e-money institutions under PSD2: https://eba.europa.eu/risk-analysis-and-data/register-of-payment-and-e-money-institutions-under-psd2

11 D.Awrey, K. van Zweiten, op. cit., p. 47.

12 EBA Register of payment and e-money institutions under PSD2: https://eba.europa.eu/risk-analysis-and-data/register-of-payment-and-e-money-institutions-under-psd2

13 Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (OJEU, L 69, 13.3.2018).

TFEU 346: CHALLENGES AND POSSIBILITIES

Vilius Kuzminskas[1]

Abstract

Public procurement currently is one of the main tools of various public policy implementation - starting from the green environmental friendly compulsory requirements and finishing with a significant share of public procurement reservation for socially exposed groups of society. In general, the idea of implementation of public policy through the public procurement is not new and neither is shocking or amazing. But the legal possibilities to implement policy through the procurement in recent decades changed dramatically, because of the legal regulation changes due to European Union public procurement directives. While some of these changes, that are done in common (civil) public procurement area, might be considered as justifiable and written off to the permanent efforts of European Commission to deepen internal market integration, some other changes are just too exceptional and not compatible with commission goals or EU purposes overall. Further more, here comes really important side effect of commission efforts to deepen integration of internal market through the regulation of procurement - European Union regulations of the procurement in defence area. It must be noted, that first directive of procurement in defence area come into the power only in 2009 - and 2019 is the year, which might be considered as tenth anniversary of first viable commission effort to impose European regulations to the defence procurement area. Nevertheless, effectiveness and legality of the EU defence procurement regulations in general is still questionable due to the treaty of European Union and the exception stated in article 346 (ex 296). Irrespective of this, EU commission keeps putting efforts to limit the usage of the exception not only through the soft-law regulations, but from time to time challenging the usage of the exception in the ECJ. But is the EU defence procurement directive the only legal way to move forward with defence area procurement - or is there another way, fixed in TFEU 346? Of course it is, but before taking this side road, comprehensive evaluation of the exception application clauses, fixed in the Treaty of Function of European Union article 346 must be done, ECJ cases, concerning this issue must be revealed and other member states lessons learned studied. Moreover, public procurement in defence area doctrine different approaches and current practices in national regulations must be disclosed and evaluated, advantages and disadvantages of the possible solutions must be revealed. Lastly, the question if public procurement in defence area regulation viability, started by the EU commission 10 years ago - and might be called a version of public procurement in defence area 1.0 - must be reevaluated and ideas of moving towards public procurement in defence area for version of 2.0 must be proposed.

Keywords: public procurement, defence, TFEU 346

Introduction

[1] PhD student of Department of Private Law, Faculty of Law, Vilnius University, LL.M, MBA. Subject of the PhD studies research – public procurement. Head of Procurement Policy Division Ministry of National Defence Republic of Lithuania.

As states Hoeffler, military sovereignty, defined as the state's capacity to possess arms and maintain security of supply in defence acquisition, is one of the fundamental features of modern nation-states[2]. This idea is nor new nor unexpected, this is a reality of every modern state, including those, who are members of European Union. That is the reason and main cause why in the Treaty of European Function (hereinafter - TFEU) clause 346 (ex 296) was included into the treaty of European communities since the beginning of the first treaty. Moreover, as states Butler[3], wording of this clause remain the same in treaties since 1957. Neither the less, the wording might stay the same, but the interpretation of the clause changed significantly, due to European Commission incentives. But this was not an easy way for European Commission - many obstacles, including significant unwillingness of member states to give up discretion in national security, had to be mitigated. The main problem was and actually still persists and will persist in foreseeable future - European union never was a real military union. Due to his, as states Hoeffler, the Commission's initiatives to limit this practice and to regulate defence procurement through EU secondary legislation constantly failed throughout the late 1990s and 2000s. In contrast, Directive 2009/81/EC constitutes the EU's first supranational legal act which integrates the trade and the production of military goods and services[4].

The first Commission incentives to establish European wide rules for defence procurement might be associated with communications of 1996[5] and 1997[6]. But these incentives were not a game changer, more or less it was just declaration of Commissions point of view. The real change was the case of European Court of Justice (hereinafter - ECJ) case against Spain[7], where ECJ ruled in an infringement case against Spain that ex-Article 296 TEC did not justify a quasi-automatic exemption of arms procurement from single market rules, but it had to be interpreted narrowly as well as other exemptions of the TFEU - the only articles in which the Treaty provides for derogations applicable in situations which may involve public safety are Articles 36, 48, 56, 223 and 224 of the EC Treaty (now, after amendment, Articles 30 EC, 39 EC, 46 EC, 296 EC and 297 EC), which deal with exceptional and clearly defined cases. Because of their limited character, those articles do not lend themselves to a wide interpretation. Due to this significant rule, more attentive consideration to the application of TFEU 346 clauses must be applied and “exceptional and clearly defined cases” meaning must be revealed.

1. TFEU 346: the regulation itself and primary requirements

TFEU 346 (ex 296) states, that:

1. The provisions of the Treaties shall not preclude the application of the following rules:

[2] C. Hoeffler, ‘European armament co-operation and the renewal of industrial policy motives’ (Journal of European Public Policy 2012), Volume 19, Issue 3.
[3] L.R.A Butler, ‘EU and US defence procurement regulation in the transatlantic defence market’, Cambridge university press 2017, 79.
[4] C. Hoeffler, ‘European armament co-operation and the renewal of industrial policy motives’ (Journal of European Public Policy 2012), Volume 19, Issue 3.
[5] European Commission. The challenges facing the European defence-related industry: a contribution for action at European level. COM(1996)10 [1996].
[6] European Commission. Implementing European Union strategy on defence-related industries. COM(1997)583, [1997].
[7] Commission of the European Communities v. Kingdom of Spain, C-414/97 [1999], European Union Court of Justice.

(a) no Member State shall be obliged to supply information the disclosure of which it considers contrary to the essential interests of its security;

(b) any Member State may take such measures as it considers necessary for the protection of the essential interests of its security which are connected with the production of or trade in arms, munitions and war material; such measures shall not adversely affect the conditions of competition in the internal market regarding products which are not intended for specifically military purposes.

In order to follow stated regulations first of all arises fundamental question: which security interests should be considered as essential. Firstly, due to the nature of security interests it is very hard, o even impossible, to determine which security interests may be considered as "secondary", because even insignificant devaluation of any security interest may result in unpredictable result and unacceptable damages of overall state security. Secondly, even more important question arise: who is responsible for these essential security interests definition? Notably, ECJ rules, that definition of essential security interests is the responsibility of member states[8] but as stated ECJ, although Article 296(1)(b) EC refers to measures which a Member State may consider necessary for the protection of the essential interests of its security, that article cannot, however, be read in such a way as to confer on Member States a power to depart from the provisions of the EC Treaty based on no more than reliance on those interests. This point of of view complied with Commission's point of view, because Commission considers that it is the Member States' responsibility to define and protect their security interests, and that it is not for the Commission to assess Member States' essential security interests, nor which military equipment they procure to protect those interests[9].Also, ECJ rules, that consequently it is for the Member State which seeks to take advantage of Article 296 EC to prove that it is necessary to have recourse to that derogation in order to protect its essential security interests[10]. So the most important point should be not the definition of essential security interest, but the test of taken measures are necessary for the protection of the essential security interests and do not go beyond the limits. This means the test of proportionality is mandatory requirement in every case.

As states Trybus[11], the test of proportionality has three elements: first, the measure in question has to be suitable to promote the objective of public security. Second, the measure has to be adequate. This means that there is 'no other measure, less restrictive from the point of view of the free movement of goods, capable of achieving the same objective'. The measure must 'not restrict intra-Community trade more than is absolutely necessary'. Third, the measure needs to be proportionate in the strict sense. The positive effect of the measure on the objective of public security has to be balanced with the negative effect on the internal market. This strict test will be applied to all free movement exclusions. If the test is not satisfied the European Court of Justice will rule against the use of the exemption.

But all of mentioned above is just a part of judicial challenges, EU member states faces in case of attempt to comply unexpectedly high requirement of current TFEU interpretation stated in Commission *soft law* documents and ongoing ECJ practice.

[8] European Commission v. Republic of Finland, C-615/10 [2012], European Union court of Justice.
[9] 8.Interpretative communication on the application of Article 296 of the Treaty in the field of defence procurement [2006] COM(2006) 779 final.
[10] European Commission v. Republic of Finland, C-615/10 [2012], European Union court of Justice.
[11] M. Trybus, 'The Limits of European Community Competence for Defence'. (journal of European Foreign Affairs Review 2004), vol. 9.

2. Later challenges to overcome

In order to apply TFEU 346 part 1, first of all an essential security interest, which must be protected, should be revealed. Taking into consideration the above mentioned transparency requirements and nature of EU Treaties, firstly it would be necessary to consolidate essential security interests of a particular Member State in national law. Moreover, the definition of essential security interest should be officially defined in generally applicable terms (not for each procurement process individually) - otherwise it may infringe principle of transparency. This requirement is also recognized in defence area procurement doctrine, f.e. Heuninckx[12]. Moreover, it must be noted, that discretion of defining essential security interests have some limitations - essential security interest must be essential and of the highest importance, because solely economic and protectionist measures might not be considered as essential security interest[13]. Taking all of above into consideration, essential national security interest must be named and then it is possible to continue further.

In order to comply with TFEU 346 (1) (a) procurement must be related with secret information, that cannot be revealed and in case of disclosure of this information irreparable damage to national security is done. As already mentioned above, when the essential national security interest is named, further must be disclosed how that interest will be secured in case of application of TFEU 346 (1) (a). Disclosure should be not just a formal act or insignificant declaration, but a direct link between the invoke of the exemption and the protection on essential security interest, caused by above stated exemption, must be reasoned. Lastly, but must importantly, reasons why less restrictive measures cannot by applied must be revealed. And the last part of exemption application is the most challenging. The main problem, from the legal point of view is directly connected with the procurement directive. The legal rules, stated in the directive allows procurement authority to exercise procurement, which involves secret information, in accordance with the rules, who are already included in the directive itself. So this makes justification quite difficult challenge, because sufficient efforts and specific knowledge must be empowered to justify use of exemption. All of this means extensive use of administrative resources, which not always are available.

In order to comply TFEU 346 (1) (b), procurement must be related to necessity of the protection of the essential interests which are connected to the production or trade in arms, munitions and war material. The firs question, that needs to be answered is whether the intended to procure goods are included into 1958 the Council list of products to which this provision applies according to Article 346 EC Treaty[14]. As states Aalto[15], this list has made been public through a reply to written a question in the European Parliament, but the original list has not been officially published in official journal. This could be considered as shortage of legal certainty, but the list it self is not detailed and because of that almost all munitions and war material should be considered as items that fall in the scope of the list. However, question related to dual purpose materials still exists, because TFEU (1) (b) literally requires that such measures shall not adversely affect the conditions of competition in the internal

[12] B. Heuninckx, '346, the Number of the Beast?' [2017] Public Procurement Research Group. Public Procurement: Global Revolution. VIII. 2017.
[13] European Commission v Federal Republic of Germany, C-372/05 [2009]. European Union court of Justice.
[14] Council of the European Union. Legislative acts and other instruments. Extract of the Council decision of 255/58 1958 April 15. REV4 14538/4/08.
[15] E. Aalto, 'Towads a European defence market' [2008]. (European Union Institute for Security studies Chaillot paper) No. 113.

market regarding products which are not intended for specifically military purposes. Must be noted, that European Commission narrow interpretation of list application only to solely military purpose goods was rejected by ECJ in InsTiimi Oy[16] case. ECJ ruled, that it must, indeed, be noted that the word 'military' used in that list and the words 'insofar as they have a specifically military nature. Moreover, ECJ stated, that it is necessary to reiterate that, recently, in recital 10 in the preamble to Directive 2009/81, the EU legislature stated that the term 'military equipment', as used in that directive, should cover products which, although initially designed for civilian use, are later adapted to military purposes to be used as arms, munitions or war material. According to this, dual purpose goods also might be considered as items that fall in the scope of the list if these goods, even though designed for civilian purpose, but contains substantial modifications. The most important aspect in the evaluation of dual purpose materials and the procurement of these item does not adversely affect the conditions of competition in the common market is evaluation particular materials "intrinsic characteristics", that may be regarded as having been specially designed and developed for military use. All of this inevitably requires even more administrative resources and decent technical expert knowledge, which usually is not at the disposal of procurement authorities, but rather specific know-how only available to private market entities.

Further application of TFEU 346 (1) (b) is related to to disclosure of following conditions - particular essential security interest naming, direct link between that particular essential security interest and intended application of exemption. Lastly, reasonable circumstances must be disclosed, why the only possible way to secure essential security interest is possible only by inclusion of TFEU 346 (1) (b) and less restrictive measures, stated in procurement in defence area directive, are not sufficient.

Taking into consideration all above analyzed requirements to justify application of the exemption, it becomes rather clear, that application of the exemption became really complicated and demanding administrative resources and specific technical knowledge, that is not at the disposal of procurement authorities. This leads to obvious danger to significant damage to national security of particular member state and aspiration to devalue national security interest in order not to get involved into long and costly dispute procedure with European Commission.

3. Security of supply: the ultimate sacrifice of narrow interpretation

As already expressed above, legal application of TFEU 346, according to current interpretations of the Treaty, is not an easy way forward, but still a viable option in some cases. Security of supply is unilaterally recognized[17] (in ECJ cases, Commission soft law documents and procurement in defence area doctrine) as important justification for exemption application, however, current legal regulation complicates possibilities for pursuing it. As states Heuninckx[18] security of supply is still a valid concern for EU Member States: embargoes by foreign countries remain a possible threat. Indeed, some Member States from the borders of the continent, such as Cyprus, Malta, Finland or the Baltic States,

[16] European Commission v. Republic of Finland, C-615/10 [2012], European Union court of Justice.
[17] F.e. M. Trybus, 'The Limits of European Community Competence for Defence'. (Journal of European Foreign Affairs Review 2004), vol. 9 or Interpretative communication on the application of Article 296 of the Treaty in the field of defence procurement [2006] COM(2006) 779 final.
[18] B. Heuninckx, '346, the Number of the Beast?' [2017] Public Procurement Research Group. Public Procurement: Global Revolution. VIII. 2017.

are located in a geographical area that does not make them immune from foreign embargoes. The problem of too narrow interpretation of TFEU 346 exemption application leads to decline of the most important aspect of defence procurement - devaluation of security off supply. Modern military equipment tends to be very sophisticated, complex and expensive items, designated to ensure essential security interests and frequently requires arrangement between various types of armed forces. Inappropriate security of supply of maintenance items (or even a delay of delivery) for this equipment makes this expensive equipment impossible to operate and due to that ensure security of essential interest. According to all of mentioned above - application of the exemption is not an easy way forward, but the only possible way in particular cases. In foreseeable future, member states pursuing security of essential security interest, should be cautious and apply in TFEU 346 fixed exemption in accordance with above given insights, ECJ practice and constantly changing point of view of European Commission.

Conclusions

Application of TFEU 346 stated exemption is not an easy nor legally secure way to ensure essential security interest of the particular state, but it is inevitable in modern military acquisitions. Essential security interest are the ones of the highest importance and none compromises in securing them could be done. However, TFEU and commitments for other European memberstates requires to take into consideration all legal aspects stated above in order to adopt a legally secure way to move forward with this exemption.

Challenges of interpretation of possibility to apply this exemption as well as European institutions continuous will to equalize rules (but not to take into account reality of differences in geography and actual situation of national security) of this exemption application, leads to wrong imaginary illusion, in which southern European countries (f.e. Spain) faces same security challenges as Baltic states. If some of the member states may discuss and spent countless amount of time to justify application of exemption, Baltic states do not have such luxury and time is critical in decision making process in order to secure essential security interests, because postponement of solutions may lead to situation, when it is too late for search for peaceful decisions.

Bibliography

1. C. Hoeffler, ‘European armament co-operation and the renewal of industrial policy motives’ (Journal of European Public Policy 2012), Volume 19, Issue 3.
2. L.R.A Butler, ‘EU and US defence procurement regulation in the transatlantic defence market’, Cambridge university press 2017, 79.
3. European Commission. The challenges facing the European defence-related industry: a contribution for action at European level. COM(1996)10 [1996].
4. European Commission. Implementing European Union strategy on defence-related industries. COM(1997)583, [1997].
5. Commission of the European Communities v. Kingdom of Spain, C-414/97 [1999], European Union court of Justice.

6. European Commission v. Republic of Finland, C-615/10 [2012], European Union court of Justice.
7. M. Trybus, 'The Limits of European Community Competence for Defence'. (Journal of European Foreign Affairs Review 2004), vol. 9.
8. Interpretative communication on the application of Article 296 of the Treaty in the field of defence procurement [2006] COM(2006) 779 final.
9. B. Heuninckx, '346, the Number of the Beast?' [2017] Public Procurement Research Group. Public Procurement: Global Revolution. VIII. 2017.
10. European Commission v Federal Republic of Germany, C-372/05 [2009]. European Union court of Justice.
11. Council of the European Union. Legislative acts and other instruments. Extract of the Council decision of 255/58 1958 April 15. REV4 14538/4/08.
12. E. Aalto, 'Towads a European defence market' [2008]. (European Union Institute for Security studies Chaillot paper) No. 113.

LEGAL TECHNOLOGY AND EMERGING NEW FORMS OF ENTREPRENEURSHIP: THE CASE OF SOCIAL BUSINESS

Tomas Lavišius[1]

Abstract

The European Commission declares that social economy gives a lot to the European Union. The Council of the European Union defines the social economy as a key driver of economic and social development in Europe. Therefore, this paper attempts to look at the case of regulating social business through the legal technology.

Usually legal technology refers to the use of technology and software to provide legal services. The scientists raise the question whether we need technology for the practice of law. If so, is the risk of using unproven or challenging legal technology products worth it? The scientists think that it is worth. They suggest that the approach should be to stop searching for what makes the law different and special, and instead focus on what makes it the same as other professional services. Moreover, the promotion of the rule of law by permitting ordinary citizens to actually make use of the powers granted to them by the legal system can be implemented also by using some legal technology.

In this light, we can speak about social entrepreneurship as an innovative way to tackle social problems. The legal status and recognition of social enterprise varies from state to state. It seems that no common agreement is found on the EU level as well. Therefore, we can ask whether the legal technology could catalyse development of legal preconditions for social entrepreneurship.

So far it is up to the particular country to decide whether the social enterprise is supposed to obtain special legal form or not. The connection of the legal technology with regulation of incorporation and maintenance of social enterprise also varies from state to state. The correlation between the above mentioned aspects is yet quite insignificant. Therefore, much more needs to be done at all levels of public policy to optimize the framework conditions for social enterprises.

Keywords: Legal technology, Social enterprise, Social business, Soft law

Introduction

[1] Tomas Lavišius is a PhD student at Mykolas Romeris Law School of Mykolas Romeris University. He is also a member of Mykolas Romeris University Justice Laboratory. His research field is the legal regulation and legal status of social enterprise (or social business) in the European Union. With respect to the novelty of the social entrepreneurship as the legal category and the lack of legal certainty, his research focuses on thorough examination of legal preconditions for social entrepreneurship in the European Union.

The hybridity of the legal status of social enterprise determines its coexistence somewhere between private company and NGO. Different methods, definitions and procedures are used in different countries to obtain the legal status of social enterprise. The European Commission defines a social enterprise as an operator in the social economy whose main objective is to have a social impact rather than make a profit for its owners or shareholders. It operates by providing goods and services for the market in an entrepreneurial and innovative fashion and uses its profits primarily to achieve social objectives. It is managed in an open and responsible manner and, in particular, involves employees, consumers and stakeholders affected by its commercial activities.[2] It should be noted that the Communication of the Commission doesn't emphasize any specific form of legal entity as a social enterprise.

This paper raises the question, could possibly the legal technology contribute to the area of social entrepreneurship or is already contributing in some countries? This is the main question of this research.

Digitalization, the adoption of advanced technologies or the incorporation of artificial intelligence are leading to the emergence of new ways of working, producing and providing services. Because social economy companies do not completely fit into the European concepts of 'for-profit' or 'not-for-profit', this concept of 'limited profitability' should be recognized. In addition, for that reason some aspects of legal technology could be useful talking about the fostering of the concept of social entrepreneurship.

Therefore, the general purpose of this paper is to find out whether the legal technology could catalyse development of legal preconditions for social entrepreneurship. The convergence of legal technology and emerging new forms of business is quite new and original approach to research legal preconditions of social entrepreneurship. It can be relevant for researchers, policy makers and social businesses all around the EU.

Methodologically this research focuses on the legislation of European Union and some recent initiatives that were undertaken by several EU Member States in order to foster development of social business with help of legal technology. This research utilizes the qualitative research methods. The textual analysis method has been used to examine the content and meaning of legal texts and other documents, as well as their structure. The scope of the research covers the examination of the EU legislation regulating this area. It also covers the comparative analysis of social entrepreneurship legal regulation in several particular countries of the EU.

1. Theoretical preconditions and evolution of social economy

The European Economic and Social Committee highlights the figures that in 2016 there were 2.8 million social economy enterprises and organizations in the European Union that employed 13.6 million people and represented 8% of the EU's GDP. Therefore, the social economy is a crucial part of the EU socio-economic landscape.[3]

[2] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Social Business Initiative. COM (2011) 682 final.

[3] 'Recent evolutions of the Social Economy in the European Union' European Economic and Social Committee [2016],

Despite the social entrepreneurship has become a source of hope, people still know little about its origin. By their origin social entrepreneurs usually do not rely on business and government for the realisation of their ideas and aiming systematic change. Social entrepreneurs are usually promoted by the non-governmental organizations, the media, policy-makers, etc. They become branded and politicised actors.[4] Researchers argue that the danger of an uncritical and exclusive promotion of a free and market based (social) system is obvious. However, there are areas where the state has a duty to act and to ensure the basic security of its citizens.[5] Therefore, the question is, if the legal circumstances is a crucial factor for development of social entrepreneurship not only as a business form that aims to tackle social problems using business methods and applying social innovation but also as a societal phenomenon *per se*.

How can legal technology serve to development of this phenomenon as such? The legal technology industry is still growing, but the industry has quietly built up a number of new categories over the last few years such as electronic discovery, law practice management, and online legal services. However, there is still a lot of opportunity to improve processes within a legal industry still attached to manual and paper-based processes. Since the most of social enterprises innovate a lot, they need and sufficient innovative legal services. Here can be mentioned the concept of the Economy for the Common Good (ECG). It is a socioeconomic and political movement founded by Austrian economist Christian Felber in 2010. The ECG model's central proposition is that the economy should be at the service of people, i.e., of the common good. The ECG model is cross-disciplinary and applicable to all kinds of companies and organisations.[6]

The other question is whether the legal preconditions for social entrepreneurship can be evaluated separately from other factors. We must stress that beside the legal preconditions there are cultural, social, and economic preconditions of social entrepreneurship. We think that in this case a successful social entrepreneurship requires organization and participation. Therefore, in order to become a part of some organization, a legal status is usually required.

The social economy refers to a wide diversity of enterprises and organisations that share common values and features such as the primacy of the individual and the social objective over capital, a democratic governance, and the reinvestment of most of the profits (surpluses) to carry out sustainable development objectives and services of general interest.[7]

Different stakeholder groups, such as Social Economy Europe (SEE),[8] propose to introduce a European commission recommendation establishing the main principles and

---

https://www.eesc.europa.eu/en/our-work/publications-other-work/publications/recent-evolutions-social-economy-study

[4] Ibid, 1.

[5] R. Ziegler, 'Introduction: voices, preconditions, contexts', in Rafael Ziegler et all, An Introduction to Social Entrepreneurship: Voices, Preconditions, Contexts (Cheltenham, UK: Edward Elgar, 2009) 1.

[6] Ibid, 104.

[7] 'The Future of EU policies for the Social Economy: towards a European Action Plan' Social Economy Europe, http://www.cecop.coop/The-Future-of-EU-policies-for-the-Social-Economy-towards-a-European-Action-Plan

[8] Social Economy Europe (SEE) was created in November 2000 under the name of CEP-CMAF – the European Standing Conference of Cooperatives, Mutuals, Associations and Foundations with the purpose of establishing a permanent dialogue between the social economy and the European Institutions. In 2008, CEP-CMAF changed its name and officially became the "Social Economy Europe". More about SEE: http://www.socialeconomy.eu.org/.

characteristics of the social economy, as well as its main legal forms: cooperatives, mutual organizations, associations, foundations, and social enterprises.[9]

Therefore, the common legal framework in the EU would serve fostering convergence and coherence between the different social economy legislations. Improving recognition and removing the existing barriers could help social economy enterprises to take full advantage of the single market of the EU through cross-border operations. So, such stakeholders as the SEE think that social economy can flourish only if a legal framework with suitable political, legislative and operational conditions is introduced at EU level. As mentioned above, the most of social enterprises innovate a lot and therefore they need sufficient innovative legal services. On the other hand, the social enterprise sector can use the opportunity to step in as the innovators in the field of legal technology start-ups, e.g. advocating different social and societal challenges. However, at this moment we don't have much of data on social enterprises or social enterprise start-ups that possibly work in the field of legal technology, therefore this could be the subject of future research.

2. Practical implications at the EU level

There is variety of social economy operators across the EU. They can be separated in two main groups – market producers and non-market producers. The group of market producers consists of non-financial corporations (e.g. cooperatives, social enterprises, other association-based enterprises, other private market producers), financial corporations (e.g. credit cooperatives, mutual insurance companies, insurance cooperatives), and general government. The group of non-market producers, on the other hand, consists of households and non-profit institutions serving households (e.g. social action associations, social action foundations, other non-profit organizations serving households: cultural, sports, etc.).

The third sector has become a meeting point for different concepts, fundamentally the 'non-profit' sector and the 'social economy', which, despite describing spheres with large overlapping areas, do not coincide exactly. Moreover, the theoretical approaches that have been developed from these concepts assign different functions to the third sector in the economies of today. We can briefly look at the main differences of the concept of social entrepreneurship in two continents. The main differences between the North American and European approaches to social enterprises have much to do with the different contexts in which they arose. In the United States, social enterprises have been a business response to social challenges traditionally served by social action non-profit organizations, which responded to cuts in public subsidies and private donations in the 1980s by developing business strategies to generate revenue to fund their philanthropic activities. In Western Europe, on the other hand, social enterprises arose to help solve structural problems of unemployment and groups with employability difficulties, as well as providing other social services targeting groups at risk of social exclusion. In other words, generally they were not set up to fund social action non-profit organizations but to solve problems of unemployment and social care for vulnerable social groups by means of a variety of productive activities.[10]

The other relevant definition is a 'collaborative economy'. We'll that in the context of the EU legislation it goes hand in hand with the 'social economy'. In its Communication

[9] 'The Future of EU policies for the Social Economy: towards a European Action Plan' Social Economy Europe, http://www.cecop.coop/The-Future-of-EU-policies-for-the-Social-Economy-towards-a-European-Action-Plan

[10] Ibid, 17-24.

called “A European agenda for the collaborative economy” (COM/2016/0356 final - 02/06/2016), the European Commission defines the collaborative economy as “business models where activities are facilitated by collaborative platforms that create an open marketplace for the temporary usage of goods or services often provided by private individuals”. Moreover, the Communication identifies three categories of actors involved in the collaborative economy: a) service providers — private individuals or professionals; b) the users of these services, and c) intermediaries — via an online platform — that connect providers with users and that facilitate transactions between them (“collaborative platforms”). The Communication also emphasizes that collaborative-economy transactions do not involve a change of ownership and can be carried out for profit or not for profit.[11]

Not only political but also financial institutions are involved in development of social entrepreneurship. The Social Impact Accelerator is a fund of funds created in 2015 by the European Investment Bank group and European Investment Fund (EIF) that targets social enterprises. It invests funds in social enterprises based on a new framework for quantifying and reporting on social impact metrics developed by EIF.[12] Although the sphere of financing of social entrepreneurship is not directly related with use of legal technology but we see that it hugely relies on the technological aspects, such as social impact metrics, etc.

3. Correlation between the soft law and legal technology

Usually legal technology refers to the use of technology and software to provide legal services. It is commonly associated with technology start-ups disrupting the practice of law by giving people access to online software that reduces or in some cases eliminates the need to consult a lawyer. The legal industry is widely seen to be conservative and traditional. However, the saturation of the market leads many lawyers to look for cutting-edge ways to compete accelerating the adoption of technology in law.

In this light we usually can speak not only about hard law, but also about the soft law measures. These soft law measures could be considered as tools to facilitate the self-regulation of particular business sectors. Self-regulation tools implemented with help of legal technology can be a significant step forward in order to promote social entrepreneurship and to facilitate unifying legal conditions for social enterprises in the EU. In the strict sense of the definition, legal technology may not be directly related with the soft law, however access to online software reduces or in some cases eliminates the need to consult a lawyer, can promote a simplified development of social entrepreneurship. In such case arrangement of private standards, guidelines, codes of conduct and forums for transnational dialogue can minimize the use of legal consultants, including legal technology as such.

In 2011, European Commission created a document: “Buying social: a Guide to taking account of social considerations in public procurement”. The Guide was a tool to help public authorities to buy goods and services in a socially responsible way in line with EU rules. It also highlighted the contribution public procurement can make to stimulate greater social inclusion. The Guide explained the wide range of possibilities offered by the EU public procurement rules to take social aspects on board in the various stages of the procurement

[11] Ibid, 26.
[12] ‘The Social Impact Accelerator‘ European Investment Fund, http://www.eif.europa.eu/what_we_do/equity/sia/index.htm

process.[13] It can be considered as a step towards more active use of soft-law measures in the regulation of social entrepreneurship. However, considering that the European Parliament and the Council in 2014 adopted a new Directive on public procurement[14], the above-mentioned Guide should be revised as well in order to keep it up to date.

In this context we can raise the question on what level law can be separated from politics if it can be separated at all. Some scholars argue that the turn from law's myths to its facts, from the falsehood of law's neutrality to the truth of its politics, could only be accomplished by turning away from traditional jurisprudence to society and history (reality). Also they claim that their social and historical analysis had revealed law to be politics pure and simple, both past and present, law would no longer be able to resist politics on the spurious grounds that politics was something other than law. The result would be law opened to explicit political reimagination and change.[15] It is quite controversial idea having in mind that the legislature creates a new legal regulation not accidentally, but with a specific purpose to meet a need of society, which requires such new legal regulation. Also there can be a lack of legal regulation, which occurs in society during the formation of new social phenomenon. Such lack of regulation also should be timely defined.

The future of applying soft law elements to the governance of social enterprise is still in the early phase of development. One can argue that one could measure intermediate results, such as the farmers' crop yields, but determining quality of life is more challenging. The absence of effective pay instruments for aligning managerial and stakeholder interests adds greatly to the costs of contracting for the production of charitable goods.[16] Soft law elements can be compared with development of corporate social responsibility (CSR). Researchers argue that more than a decade ago corporate governance and CSR started as soft law initiatives, but later on have developed beyond being pure soft law instruments. Now their hard law elements are concerned with disclosure requirements. Corporate governance issues are often addressed in CSR reports, and CSR is becoming part of the corporate governance system. According to Directive 2003/51, companies have to disclose non-financial key performance indicators in their annual reports, including environmental and employee matters, to the extent necessary for an understanding of the company's development, performance or position.[17] Of course, so far it is applicable to certain types of large listed companies. But it's plausible that at some level it could become a common practice in entities that act like social enterprise.

4. New regulatory approaches in the EU countries

Different EU countries undertake different regulatory initiatives regarding regulation of social business. We will see that some of the initiatives correlate with the legal technology and some not. However there is a clear tendency of movement towards the domain of the

[13] 'Buying social: a Guide to taking account of social considerations in public procurement' European Commission, http://europa.eu/rapid/press-release_IP-11-105_en.htm

[14] Directive 2014/24/EU of the European Parliament and of the Council on public procurement and repealing Directive 2004/18/EC [2014], OJ L 94.

[15] Ch. Tomlins, 'Law 'And', Law 'In', Law 'As': The Definition, Rejection and Recuperation of the Socio-Legal Enterprise' [2013] Law in Context 29, no. 2, 138.

[16] B. Galle, 'Social Enterprise: Who Needs It?' [2013] Boston College Law Review 54, no. 5, 2028, 2045.

[17] D. Szabó, K.E. Sørensen, 'Integrating Corporate Social Responsibility in Corporate Governance Codes in the EU' [2013] European Business Law Review, no. 6, 789.

soft law and digital social innovation. Digital solutions to social challenges range from social networks for those living with chronic health conditions, to online platforms for citizen participation in policymaking, to using open data to create more transparency about public spending. This movement is frequently called a phenomenon of digital social innovation.[18]

Some experts emphasize that digital social innovation a lot in common with other terms like “tech for good”, “civic tech” and “social tech”. We can see that they all heading in the same direction and share similar aims: to reorient technology to social ends; to use collective knowledge and skills to positive effect; to make government more accountable and transparent; to foster and promote alternatives to the dominant technological and business models — alternatives which are open and collaborative rather than closed and competitive.[19] Digital social innovation uses a huge range of technologies - open hardware, peer-to-peer platforms, open data etc. And it is being used to tackle challenges in almost all areas, including education, healthcare, democracy, transparency and accountability, justice and many others.[20] Several examples in the EU countries show the tendency of the movement towards this direction.

In Denmark, a social enterprise must be defined as a company that has a social aim, sales products or services, reinvests any profits back in the company, and is democratic and citizen-oriented - it is legitimate in relation to its surroundings.[21] Speaking about the use of legal technology, it should be stressed that Denmark is one of the easiest places in the world to fill out the formalities for starting a business. It is all done online and takes several minutes. When a person registers a venture online he or she instantly receives a company registration number and must choose which type of company he or she wants to register under. Despite the type of company, they are not defined as a social enterprise unless they follow the above mentioned characteristics.[22]

In Denmark, the purpose of the Act on Registered Social Economic Companies is to create the basis for a common identity for social economy enterprises. It does not give any immediate financial or legal benefits after registering as a social economy company. Currently, the advantage is that it becomes easier to communicate to the outside world that one works from social economy principles.[23]

E.g., Danish and British sector of social enterprise developed differently and the assigned role of social enterprises in each country is mostly different. Much of the UK activity in social enterprise and social investments has revolved around an outsourcing or acquisition of public sector services. In Denmark, the role of social enterprise has so far been more or less disconnected from the issue of gaps in public sector service. Instead, social enterprises have almost entirely been used as means of including people with some

[18] ‘Digital Social Innovation’ Social Innovation Community, https://www.siceurope.eu/network/digital-social-innovation

[19] ‘Digital social innovation is intimately related to all other areas of social innovation: an interview with our DSI network facilitator’ Social Innovation Community, https://www.siceurope.eu/network/digital-social-innovation/digital-social-innovation-intimately-related-all-other-areas?conical=true

[20] Ibid.

[21] ‘What is a social enterprise’ Startupsvar.dk, https://www.startupsvar.dk/social-enterprise

[22] Ibid.

[23] ‘Registreret socialøkonomisk virksomhed – RSV’ Startupsvar.dk, https://www.startupsvar.dk/registreret-social-virksomhed

form of disadvantage or disability into the ordinary labor market – in businesses or projects with no attachment to public service delivery.[24]

We see that it's modern and innovative approach letting the social enterprises use legal technology is quite well developed and gaining its popularity with every year. Is it the case also in other countries?

In Sweden, social enterprises are generally understood as companies with the aim to reduce social exclusion and to provide efficient welfare services in a not-for-profit setting. Additionally, Sweden has had a long history of not-for-profit organizations with societal aims. Despite the level of institutionalisation of the different existing forms of social enterprises in Sweden remains low, social innovations are visible and take place in collaboration between the public sector, the private sector and civil society. It can be viewed as a new form of welfare ideas and as social innovation for the twenty-first century. When it comes to legal frameworks, two Swedish laws have come to influence the sector - The Public Procurement Act and The Law on Freedom of Choice that ensures the right of citizens to choose their own welfare service provider amongst the possible actors from the public, the private and the not-for-profit sector.[25] From the point of view of the legal technology, the Swedish private and not-for-profit sector provides a variety of soft tools for social entrepreneurs to create a legal status, come up with a business idea and develop it in several social innovation incubators or to use a national knowledge platform for social innovation and societal entrepreneurship.[26]

In Finland, social enterprises are no different from other companies, as companies. They produce goods and services for the market and try to make a profit, the same as any other business. However, social enterprises have they separate legal framework – Act on Social Enterprises. According to the Act, the purpose of social enterprises is to create jobs in particular for the disabled and long-term unemployed. A social enterprise is a registered trader who is entered in the register of social enterprises.[27]

Moreover, social entrepreneurs get the mark of certification (the Finnish Social Enterprise Mark) if they promote well-being, limit their distribution of profits and offer transparency of their business operations.[28] It's an innovative approach, based on a principle of self-regulation, which allows obtaining the social enterprise the additional status (label) besides the one that is described in the Law.

Estonia is one of two Baltic countries (besides Lithuania) that haven't developed a concrete legal framework for social entrepreneurship. However, it has to be mentioned that the sector has been actively developing for several decades. Most recently, the social enterprise concept and practical support measures were included into two national development plans as well as the new Public Procurement Law. Since there is no special legal structure for social enterprises in Estonia, registering as a "non-profit" is a default

[24] M. Bruhn Lohmann, 'What's the future of social enterprise in Denmark and the UK?' Social Innovation Community, https://www.siceurope.eu/network/social-economy/whats-future-social-enterprise-denmark-and-uk

[25] H. Thomas, R. Persson, N. Hafen, 'Social Enterprise, Social Innovation and Social Entrepreneurship in Sweden: A National Report' 24-25, 37, https://sofisam.se/download/18.72b312e7163120a87495d6d6/1525433671511/EFESEIIS%20National%20Report%20Sweden.pdf

[26] Ibid, 42.

[27] 'Act No. 1351/2003 on Social Enterprises' finlex.fi, http://www.finlex.fi/en/laki/kaannokset/2003/en20031351.pdf

[28] 'Social Entrepreneurship Rising in Finland' Business and Innovation. This is Finland, https://finland.fi/business-innovation/social-entrepreneurship-rising-in-finland/

option for social purpose initiatives there. More specifically, most of them are registered as so-called civil society organizations: either non-profit associations (governed by its members) or foundations (governed by a board). There are also a few limited liability companies identifying themselves as social enterprises.[29] Despite the limited legal recognition, on the level of self-regulation, social enterprise community of Estonia enjoys quite active advocacy from the association – Estonian Social Enterprise Network. Also several soft-law tools, such as "Social Impact Measurement Tools for Young Social Entrepreneurs", are available.[30]

Latvia is the only Baltic state so far, which has developed a concrete legal framework for social entrepreneurship. In 2017, the Latvian Parliament adopted new Law on Social Business, which foresees that a social enterprise is a limited liability company that has received the status of social enterprise pursuant to this law and that performs operations with a positive social impact.[31] The status of social enterprise can be obtained online.

The Lithuanian Government so far adopted the Draft Law on the Social Business.[32] This way the Government seeks to define the criteria and forms of social business, as well as the support measures in order to boost social economy. However, the Draft Law hasn't reached the step of the reading in the Parliament. So far, it is difficult to say whether some legal innovations will be introduced in the process of establishing and maintaining social business entity.

In comparison, United Kingdom has perhaps longest tradition in developing and promoting social entrepreneurship in the EU (regardless the ongoing process of Brexit). UK in 2005 established dedicated form of social enterprise – Community Interest Company.[33] The Community interest company is a structure specifically created for social enterprises. Legal technology is frequently used in creating (e-registration), supporting (online funding platforms) and maintaining (ethical standards and other soft law instruments) social enterprises. The Community interest companies enjoy a dedicated online incorporation process.[34]

The examples from several countries show that the connection of the legal technology with regulation of incorporation and maintenance of social enterprise varies from state to state. The correlation between the use of legal technology and soft law is yet quite insignificant in the countries where the general legal preconditions for social entrepreneurship are underdeveloped and vice versa – where the legal environment for social entrepreneurship is advanced it correlates more frequently with the elements of legal technology and soft law.

---

[29] 'Social Impact Measurement Tools for Young Social Entrepreneurs: Needs Analysis' sev.ee, https://sev.ee/wp-content/uploads/2017/06/kusif-needanalysis-26-10-16.pdf

[30] 'Know your Impact' Social Impact Measurement tools for Young Social Entrepreneurs, https://knowyourimpact.ku.edu.tr/the-project/

[31] 'Saeima establishes legal framework for activities of social enterprises' Latvijas Republikas Saeima [2017], http://www.saeima.lv/en/news/saeima-news/26238-saeima-establishes-legal-framework-for-activities-of-social-enterprises

[32] 'Lietuvos Respublikos socialinio verslo plėtros įstatymo projektas' e-seimas, https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/f6ed4d30ff9f11e89b04a534c5aaf5ce?positionInSearchResults=0&searchModelUUID=f56e3d9a-46cf-44e0-b119-c423ff4a6c5c

[33] The Community Interest Company Regulations [2005], http://www.legislation.gov.uk/uksi/2005/1788/pdfs/uksi_20051788_en.pdf

[34] 'Community Interest Companies' Office of the Regulator of Community Interest Companies, https://www.gov.uk/government/organisations/office-of-the-regulator-of-community-interest-companies

Despite some examples of the use of legal technology, the greatest potential of the synergy between legal technology and soft law in the field of social entrepreneurship is still untapped. The community of legal technology start-ups is familiar with such new areal of legal service as legal research, notarization tools, intellectual property/trademark services, etc.,[35] which could be used by the social enterprises to lower the costs of their goods or services. On the other hand, the social enterprises can become start-ups providing above mentioned legal technology services tackling social problems. One from the up-to-date legal technology start-up databases[36] provides information that none of the above mentioned countries have a specialized legal technology start-up working exceptionally with social businesses, or operating as social business itself. However, there are several examples that are worth to mention despite they were out of the scope of this research. To everyone's surprise, the main examples of the legal technology start-ups that work with the goal of social mission can be found in India. Such start-ups like 'Ruly'[37], 'Law for Me'[38], or 'Lawtoons'[39] offer range of legal services and educational materials dedicated to people who can't afford traditional legal services. Some examples can be found also in Europe, e.g. German legal technology start-up 'Helpcheck'[40] defends consumers against big corporations and insurance companies, for those who might otherwise be deterred from pursuing their rights due to high legal fees.

Authors who research development of legal technology notice that in recent years clients have been more thorough with their billing and spending on legal services, resulting in a need to be more transparent and efficient.[41] It seems that there is a good opportunity for social enterprise sector to step in with the affordable legal services based on legal technology.

Conclusions

Answering the question whether the legal technology could catalyse development of legal preconditions for social entrepreneurship highlights three tendencies.

The first, so far it is up to the particular country to decide whether the social enterprise is supposed to obtain special legal form or not. Therefore connection of the legal technology with regulation of incorporation and maintenance of social enterprise also varies from state to state. We can argue that the correlation between the above mentioned aspects is yet quite insignificant.

The second, the legal technology is already contributing to the area of social entrepreneurship in particular circumstances. We see that sphere of financing of social

[35] 'Legal Tech Market Map: 50 Startups Disrupting The Legal Industry' [2016], https://www.cbinsights.com/research/legal-tech-market-map-company-list/

[36] 'Legal Tech Startups' [2019], https://airtable.com/shr74dsY3wZMwLMBg/tble1gLbY7XwrlSQD/viwp8mj6JmaFoqZVK?backgroundColor=blue&layout=card&blocks=hide

[37] 'Ruly', http://www.ruly.in/index

[38] 'Law for Me', http://lawforme.in/

[39] 'Lawtoons', http://www.lawtoons.in/

[40] 'Helpcheck', https://www.helpcheck.de/

[41] G. Miranda 'How Legaltech Startups are Revolutionizing the Legal Services Industry' LAWAHEAD, https://lawahead.ie.edu/how-legaltech-is-revolutionizing-the-legal-services-industry/

entrepreneurship hugely relies on the technological aspects, such as social impact metrics, etc.

The third, soft law measures could be considered as tools to facilitate the self-regulation of particular business sectors. Self-regulation tools implemented with help of legal technology can be a significant step forward in order to promote social entrepreneurship and to facilitate unifying legal conditions for social enterprises in the EU. Giving social enterprise access to online software that reduces or in some cases eliminates the need to consult a lawyer, can promote a simplified development of social entrepreneurship. Moreover, arrangement of private standards, guidelines, codes of conduct, and forums for transnational dialogue can minimize the use of legal consultants, including legal technology as such. And additionally, CSR principles applicable to certain types of companies with help of soft law measures could become a common practice in entities that act like social enterprise.

Overall, there is a clear tendency of movement towards the domain of the soft law and digital social innovation. Therefore, much more needs to be done at all levels of public policy to optimize the framework conditions for social enterprises.

Bibliography

1. 'Act No. 1351/2003 on Social Enterprises' finlex.fi, http://www.finlex.fi/en/laki/kaannokset/2003/en20031351.pdf.
2. M. Bruhn Lohmann, 'What's the future of social enterprise in Denmark and the UK?' Social Innovation Community, https://www.siceurope.eu/network/social-economy/whats-future-social-enterprise-denmark-and-uk.
3. 'Buying social: a Guide to taking account of social considerations in public procurement' European Commission, http://europa.eu/rapid/press-release_IP-11-105_en.htm.
4. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Social Business Initiative. COM (2011) 682 final.
5. 'Community Interest Companies' Office of the Regulator of Community Interest Companies, https://www.gov.uk/government/organisations/office-of-the-regulator-of-community-interest-companies.
6. The Community Interest Company Regulations [2005], http://www.legislation.gov.uk/uksi/2005/1788/pdfs/uksi_20051788_en.pdf.
7. 'Digital social innovation is intimately related to all other areas of social innovation: an interview with our DSI network facilitator' Social Innovation Community, https://www.siceurope.eu/network/digital-social-innovation/digital-social-innovation-intimately-related-all-other-areas?conical=true.
8. 'Digital Social Innovation' Social Innovation Community, https://www.siceurope.eu/network/digital-social-innovation.
9. Directive 2014/24/EU of the European Parliament and of the Council on public procurement and repealing Directive 2004/18/EC [2014], OJ L 94.
10. 'The Future of EU policies for the Social Economy: towards a European Action Plan' Social Economy Europe, http://www.cecop.coop/The-Future-of-EU-policies-for-the-Social-Economy-towards-a-European-Action-Plan.

11. B. Galle, ‘Social Enterprise: Who Needs It?’ [2013] Boston College Law Review 54, no. 5, 2025-2045.
12. ‘Helpcheck’, https://www.helpcheck.de/.
13. ‘Know your Impact’ Social Impact Measurement tools for Young Social Entrepreneurs, https://knowyourimpact.ku.edu.tr/the-project/.
14. ‘Law for Me’, http://lawforme.in/.
15. ‘Lawtoons’, http://www.lawtoons.in/.
16. ‘Legal Tech Market Map: 50 Startups Disrupting The Legal Industry’ [2016], https://www.cbinsights.com/research/legal-tech-market-map-company-list/.
17. ‘Legal Tech Startups’ [2019], https://airtable.com/shr74dsY3wZMwLMBg/tble1gLbY7XwrlSQD/viwp8mj6JmaFoqZVK?backgroundColor=blue&layout=card&blocks=hide.
18. ‘Lietuvos Respublikos socialinio verslo plėtros įstatymo projektas’ e-seimas [2018], https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/f6ed4d30ff9f11e89b04a534c5aaf5ce?positionInSearchResults=0&searchModelUUID=f56e3d9a-46cf-44e0-b119-c423ff4a6c5c.
19. G. Miranda ‘How Legaltech Startups are Revolutionizing the Legal Services Industry’ LAWAHEAD, https://lawahead.ie.edu/how-legaltech-is-revolutionizing-the-legal-services-industry/.
20. ‘Recent evolutions of the Social Economy in the European Union’ European Economic and Social Committee [2016], https://www.eesc.europa.eu/en/our-work/publications-other-work/publications/recent-evolutions-social-economy-study.
21. ‘Registreret socialøkonomisk virksomhed – RSV’ Startupsvar.dk, https://www.startupsvar.dk/registreret-social-virksomhed.
22. ‘Ruly’, http://www.ruly.in/index.
23. ‘Saeima establishes legal framework for activities of social enterprises’ Latvijas Republikas Saeima [2017], http://www.saeima.lv/en/news/saeima-news/26238-saeima-establishes-legal-framework-for-activities-of-social-enterprises.
24. ‘Social Entrepreneurship Rising in Finland’ Business and Innovation. This is Finland, https://finland.fi/business-innovation/social-entrepreneurship-rising-in-finland/.
25. ‘The Social Impact Accelerator‘ European Investment Fund, http://www.eif.europa.eu/what_we_do/equity/sia/index.htm.
26. ‘Social Impact Measurement Tools for Young Social Entrepreneurs: Needs Analysis’ sev.ee, https://sev.ee/wp-content/uploads/2017/06/kusif-needanalysis-26-10-16.pdf.
27. D. Szabó, K.E. Sørensen, ‘Integrating Corporate Social Responsibility in Corporate Governance Codes in the EU’ [2013] European Business Law Review, no. 6, 781-828.
28. H. Thomas, R. Persson, N. Hafen, ‘Social Enterprise, Social Innovation and Social Entrepreneurship in Sweden: A National Report’, https://sofisam.se/download/18.72b312e7163120a87495d6d6/1525433671511/EFESEIIS%20National%20Report%20Sweden.pdf.
29. Ch. Tomlins, ‘Law ’And’, Law ’In’, Law ‘As’: The Definition, Rejection and Recuperation of the Socio-Legal Enterprise’ [2013] Law in Context 29, no. 2, 137-163.
30. ‘What is a social enterprise’ Startupsvar.dk, https://www.startupsvar.dk/social-enterprise.

31. R. Ziegler, ‘Introduction: voices, preconditions, contexts’, in *Rafael Ziegler et all, An Introduction to Social Entrepreneurship: Voices, Preconditions, Contexts* (Cheltenham, UK: Edward Elgar, 2009) 1-20.

CRYPTOCURRENCIES: A CHALLENGE FOR TAX REGULATION

Alessandro Liotta[1]

Abstract

The aim of this paper is to highlight the main problems deriving from cryptocurrencies in the field of taxation. First, the paper will give a glimpse at the key features of cryptocurrencies and Blockchain. Secondly, the paper will deal with the definition of this phenomenon and it will focus on the difficulties faced by different Institutions and entities, at European and International level, to provide a convincing and homogeneous definition of cryptocurrencies. The paper will provide a comparative overview of some different definitions to give an idea of how difficult it is to identify what cryptocurrencies are. Finding out the correct definition is not important as such, but it represents the first step to understand how to tax revenue deriving from cryptocurrencies. In fact, various economically relevant activities are involved in the world of cryptocurrencies, such as mining or exchanging, and such activities need to be taxed. In this scenario, the current legislative framework is not up to date and obsolete and requires robust amendments. How should revenue deriving from cryptocurrencies be taxed? An answer has been given by the Italian Tax Administration, which has issued two responses, following the judgment of the ECJ which, however, do not seem to be conclusive. In fact, the Italian Tax Code does not set forth any provisions regarding cryptocurrencies and the Tax Administration had to interpret the existing provisions. In addition, the paper will explore the approach of a Notice issued by the US Internal Revenue Service (IRS Notice 2014-21, March 25, 2014) and the one adopted by the Virtual Currency Tax Reform Act, which is supposed to give a definitive solution to the problem of taxation in the US. In conclusion, the paper will pose some questions regarding the ability of the tax systems to deal with issues related to cryptocurrencies.

Keywords: Tax Blockchain, Bitcoin Regulation

1. Introduction: the essentials of Blockchain and cryptocurrencies

The law systems are not usually able to keep up with technological developments and struggle to acknowledge and regulate their most innovative elements. The inadequacy of such systems is evident when it comes to deal with cryptocurrencies[2]. Despite Blockchain –

[1] Master of Laws at Università degli Studi di Palermo, LL.M. in International Tax Law at King's College London, PhD candidate in "Law and Business", LUISS Guido Carli (Rome), Faculty of Law, with a dissertation in Tax Law on the application of anti-avoidance provisions to IP Holding Companies. Visiting Researcher at UNIL and Visiting Scholar at UC Berkeley, Boalt Hall Law School. Member of the Science Center of Public Finances and Tax Law at Vilnius University. Main interests: Tax Law, both from a domestic and an international perspective, and EU Law issues, especially those related to Tax Law. Email address: aliotta@luiss.it

[2] For a thorough introduction of the concept of currency and its relationship with bitcoin, see KIEN-MENG LY M., 'Coining Bitcoin's "Legal Bits": Examining the Regulatory Framework for Bitcoin and Virtual Currencies, in Harvard Journal of Law & Technology, [2014], 27, 587.

the technology cryptocurrencies are based on – was ideally born in 1991[3] and Bitcoin was theorized in 2008[4] by some authors under the pseudonym of Satoshi Nakamoto, lawmakers and regulators have been caught by surprise[5].

The impact Blockchain and cryptocurrencies may have on transactions is still unpredictable, considering the speed of evolution of these technologies and the difficult task of creating an acceptable and shared definition of these phenomena[6]. Although the Financial Action Task Force (FATF) has created a sort of dictionary[7] that sums up and classifies cryptocurrencies, the uncertainties wafting around virtual currencies are considerable.

In any case, it is nowadays impossible to deny the potential of the Blockchain technology and the very existence of a *real virtual world*[8] cannot be put aside or considered as a marginal phenomenon, especially if we consider its impact and its ability to affect the "real world". This paper is not deemed to focus on the various, albeit interesting, aspects of Blockchain, but it is rather going to deepen some issues regarding the regulation of cryptocurrencies. However, it is necessary to identify the key elements that characterize the technology at issue, in order to better address the topic of this paper.

---

[3] For a deeper study of the history of cryptocurrencies, see FRANKLIN M., 'A Profile of Bitcoin Currency: An Explanatory Study', in International Journal of Business and Economic Perspectives, [2016], 1, 80.

[4] NAKAMOTO S., 'Bitcoin: A Peer-to-Peer Electronic Cash System', [2008].

[5] It is possible to spot the uncertainties regarding the concept of cryptocurrencies by mentioning the guidelines issued by some American States. In this respect see. HUGHES S.J. – MIDDLEBROOK S.T., 'Are These Game Changers? Developments in the Law Affecting Virtual Currencies, Prepaid Payroll Cards, Online Tribal Lending, and Payday Lenders', in The Business Lawyer, [2014], 70, 261. The Authors point out that "At state level, regulators in California, Connecticut, Indiana, Nevada, New Mexico and Texas all issued statements or guidance related to virtual currency activities in their respective states. In addition, New York announced that it would consider formal applications from entities wishing to establish and operate regulated virtual currency exchanges within the state".

[6] It is worth noting that few Authorities have issue various, and often divergent, definitions of cryptocurrencies, which makes it even harder to deal with this topic. For instance, according to the European Bank Authority virtual currencies are "digital representation of value that is neither issued by a central bank or a public authority nor necessarily attached to a fiat currency (FC), but is accepted by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically". See Opinion on Virtual Currencies, EBA/op/2014/08, 10 (2014). Cryptocurrencies might be deemed as categories of virtual currencies that use cryptography to create new currencies and the control of transactions, allowing a decentralized system of transactions. See. VIGNA P. – CASEY M.J., 'Cryptocurrency: The Future of Money?', Random House, [2016], 42. In addition, the National Payment System (NPS) Department of the South African Reserve Bank (SARB) stated "A virtual currency (VC) is a digital representation of value that can be digitally traded and functions as a medium of exchange, a unit of account and/or a store of value, but does not have legal tender status". In this respect, see the Position Paper on Virtual Currencies, December 3rd, 2014, SARB 2014 https://goo.gl/2nX9Tv.

[7] Cryptocurrencies can be divided into several categories: centralized (that is to say linked to an administrative authority, like Webmoney or Perfect Money), decentralized (like Bitcoin, LitCoin and Ripple), non-convertible (which means that they do not have an equivalent in real currencies and they cannot be exchanged with any other currency, like Q Coins, World of Warcraft Gold and Project Entropia Dollars). See NIEMAN A., 'A Few South African Cents' Worth on Bitcoin', in PER, [2015], 18, 1979. Depending on how virtual currencies are used to ease transactions, they can belong to one or another category. See also ANAND J., 'Virtual Economies Virtually Unregulated: How Clear Taxpayer Guidance Can Mitigate Tax Compliance Risks', in Hofstra Law Review, [2014], 43, 253.

[8] The existence of the real virtual world is highlighted by the so called Bitnation, where it is claimed that sovereignty is shifting from the State to the citizens, In this respect, see TARKOWSKI TEMPELHOF S., 'Bitnation, Pangea Jurisdiction and Pangea Arbitration Token (PAT), The Internet Sovereignty', https://tse.bitnation.co/. This sovereignty shift is said to be due to the lack of regulatory entities or of central authorities that have the power to issue currency or to control its movements.

Bitcoin and other similar virtual currencies are based on a consensus network, that allows an unprecedented payment system. It consists in a decentralized peer-to-peer payment network, powered by its users, with no intermediaries or central authorities. As a matter of facts, the Bitcoin network is not owned by anyone and it shares a public ledger known as Blockchain[9], where it is possible to find information regarding all the transactions occurred, allowing, thus, the users to verify the validity of such transactions.

The authenticity of each transaction is protected by cryptography and digital signatures, allowing all the users to have full control over the bitcoins sent from their "Bitcoin account".

In addition, each user can process the transactions using the computing power of hardware systems and receive, in exchange, a sum in bitcoin for this type of service (so-called mining activity). More specifically, such an activity consists in the use of advanced computing power to process transactions, keep the network safe and synchronized all the members of the system[10].

A transaction regarding bitcoin usually involves the following entities: a subject sending bitcoins who starts a transaction in the network; a subject who receives and accepts these bitcoins; the miners, who check the validity of the transaction; the Bitcoin development team, that update the system, if required; and the Bitcoin currency exchange team, that make the exchange of cryptocurrencies easier.

As it is possible to understand from the previous description, the main features of the Blockchain technology can be enlisted as follows: it can act as a public ledger; it is a global, transparent and shared system, that allows its users to monitor the activities taking place therein; it does not need any intermediaries or regulatory authorities. Consequently, in the current legal framework it is hard to identify an economical or juridical category which cryptocurrencies may belong to[11].

Although Bitcoin was initially meant to be used only as a tool for financial transactions, it has turned out to be a reliable currency and, since 2013, it has been increasingly used also in other contexts[12].

It is thus surprising that such a widespread phenomenon has not been efficiently ruled and is still surrounded by an aura of uncertainty.

2. Definition(s) of cryptocurrencies

[9] Literally, the term "blockchain" stems from the idea that transactions must be treated as parts (blocks) of a chain. A new block is added to the chain roughly every ten to twelve minutes, despite part of the process implies the solution of complex algorithms. In this respect, see ALLEN K, 'A Bitcoin Primer', Arizona Daily Star, 2014 https://tucson.com/business/local/a-bitcoin-primer/article_aff0568e-bf71-5c88-b821-38c1b9c4e277.html. The Blockchain technology is used in the area of transfer pricing. See BILANEY S. K., 'From Value Chain to Blockchain – Transfer Pricing 2.0', in International Transfer Pricing Journal, [2018], 294.

[10] In this respect, see BRYANS D., 'Bitcoin and Money Laundering: Mining for an Effective Solution', in Indiana Law Journal, [2014], 441

[11] As it will be further highlighted in the following section, cryptocurrencies have been alternatively deemed as goods, securities or financial instruments. In this respect, see TU V.K. – MEREDITH M.W., 'Rethinking Virtual Currency Regulation in the Bitcoin Age', in Washington Law Review, [2015], 271.

[12] See SMALL S., 'Bitcoin: The Napster of Currency', in House Journal of International Law, [2015], 581.

The concept of cryptocurrency is not so hard to imagine but tailoring a juridically incontrovertible convincing definition around it is not as easy. In fact, if we put the stress on any of its characteristics and consider any of them predominant over the others may give rise to different results.

For instance, cryptocurrencies might be analysed considering their purpose, that is to say, their ability to act as medium of exchange and store of value. According to the District Court of Texas, when it comes to defining cryptocurrencies it is necessary to stress their functions. In fact, since "*[…] it is clear that Bitcoin can be used as money*" as "*[Bitcoin] can be used to purchase goods or services, and […] used to pay for individual living expenses, […] Bitcoin is a currency or a form of money*"[13].

However, if we look at the elements that traditionally belong to the concept of "money", it might be claimed cryptocurrencies cannot be included in that category because they are not legal tender as they are not issued by any central authority[14].

To make it clear, cryptocurrencies like Bitcoin are the result of an Internet protocol and, since they leave no physical sign (so-called paper trail), they may disappear by the very nature of Internet[15]. Based on this type of reasoning, on July 22nd, 2015, the District Court of Florida held Bitcoin was not money[16]. In fact, Judge Pooler dismissed the case of money laundering involving Bitcoin, stating that Bitcoin did not qualify as money, since it lacks any banks or governmental authorities and it cannot – to quote the Judge – "*be hidden under a mattress like cash and gold bars*"[17].

According to the European Central Bank, cryptocurrencies may not be regarded as foreign currencies. In a recent Opinion, the ECB stated that the only recognized currency in the Monetary Union and pointed out that cryptocurrencies should be considered as means of exchange, rather than proper currencies[18].

[13] SEC v Shavers, 2013, U.S. District. LEXIS 110018 (E.D. Texas August 6, 2013).

[14] In this respect, see CIRILLO A. – ATZENI C., 'Aspetti operative, giuridici e fiscali delle criptovalute, in Amministrazione e Finanza, [2018], 8, 27.

[15] An example of alternative and more structured and reliable cryptocurrency is the Unified System for Regional Compensation (SUCRE). The SUCRE was initially a cryptocurrency used for transactions between Ecuador and Venezuela and it as meant to replace the US dollar as a mean of exchange and to limit the control of US over South American trades and, simultaneously, to increase the level of stability of these markets. In this respect, see ALVARO M. – LEWIS J.T., 'Who Needs Bitcoin? Venezuela has its "Sucre", [2014], http://www.wsj.com/articles. See also HURTADO C.R., 'Fiscal Policies as Decisive Solutions for Troubled Economics: Differing Legislative Enactments in Argentina Ecuador, in Loyola L.A. International & Comparative Law Review, [2014], 24, 391.

[16] Florida v Espinoza F14-2923, 6 (Florida District Court 2015).

[17] The case at issue regarded a web designer, Michell Espinoza, who was accused of money laundering because he had previously sold bitcoin to under-cover agents to buy stolen credit cards. For a deeper analysis of the case, see PIAZZA F., 'Bitcoin in the Dark Web: A Shadow over Banking Secrecy and a Call for Global Response', in Southern California Interdisciplinary Law Journal, [2017], 26, 521.

[18] See the Opinion of the European Central Bank (October 12th, 2016), § 1.1.3: "First, 'virtual currencies' do not qualify as currencies from a Union perspective. In accordance with the EU Treaties and the provisions of Council Regulation (EC) n. 974/98, the euro is the single currency of the Union's economic and monetary union, i.e., of those Member States which have adopted the euro as their currency. […] Second, given that virtual currencies are not in fact currencies, it would be more accurate to regard them as a means of exchange, rather than a means of payment".

It has also been argued Bitcoins might be defined as a type of financial instrument[19]. From an economic point of view, a financial instrument is a type of investment. However, the juridical definition of financial instrument changes, sometimes radically, from State to State. In the USA, according to Section 77 (b) of the 1933 Securities Act "*any note, stock, treasury, security future, security-based swap, bond […] investment contract […] or, in general, any interest or instrument commonly known as 'security'*"[20]. The US Courts usually determine if an interest can be treated as a financial instrument with the Howey test. Briefly, in the SEC v W.J. Howey Co. Case[21], the Court stated that it is first necessary to find out what an investment contract is, in order to determine what can be included in the definition of financial instrument[22].

However, if we applied said test to Bitcoin, it would be impossible to consider it as a financial instrument.

As an alternative, Bitcoin may be defined as raw materials. A peculiarity of such goods is that their quality remains average among the various producers. Every raw material must satisfy three conditions to identify as such: they must be standardized; they are ready use once delivered; their price must vary enough to justify the creation of a market. Typical examples of raw materials are those related to energy (gas, coal, oil), precious metals (gold, silver, copper) and agricultural goods (wheat, oil, coffee).

In September 2015, the U.S. Commodity and Futures Trading Commission (CFTC) issued its first action against a non-registered platform that traded options on Bitcoins, holding that Bitcoin, like the other cryptocurrencies, qualified as raw material for the purposes of the Commodity Exchange Act (CEA)[23]. Indeed, defining cryptocurrencies as raw goods gives rise to two doubts: first, raw materials are commonly used to satisfy primary needs; second, unlike traditional raw materials, the quantity of cryptocurrencies is potentially unlimited.

Conversely, it has been stated that the currencies of those countries that have a large availability of raw materials or natural resources have long been accepted as raw materials themselves[24].

Despite the opinion of the CFTC, it may be argued that cryptocurrencies and raw materials satisfy, in principle, different needs and, thus, do not have the same functions.

Considering how difficult it is to define cryptocurrencies, the solution could be including them in the more general category of the intangibles[25].

---

[19] See SONDEREGGER D., 'A Regulatory and Economic Perplexity: Bitcoin Needs Just a Bit of Regulation', in Washington University Journal of Law & Policy, [2015], 47, 175.
[20] 15 U.S.C.S. § 77b.
[21] SEC v W. J. Howey Co., 328 U.S. 293 [1946].
[22] The Howey Test establishes if an investment contract and, consequently, a financial instrument, is "a contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party, it being immaterial whether the shares in the enterprise are evidenced by formal certificate or by nominal interests in the physical assets employed in the enterprise".
[23] See in Re Coinflip Inc. et al., CFTC Docket n. 15-29 (CFTC Filed September 17, 2015) https://www.irs.gov/pub/irs-drop/n-14-21.pdf.
[24] See PERRY B., Forex Currencies: Commodity Pairs (USD/CAD, USD/AUD, USD/NZD), INVESTOPEDIA.
[25] In this respect, see FERRARI E., 'Bitcoin e criptovalute: la moneta virtuale tra Fisco e antiriciclaggio', in Il Fisco, [2018], 9, 861.

To sum up, none of the previous definitions seems to be suitable for the concept of Blockchain. Given this situation of uncertainty, it might be necessary to create statutory tools that may be useful to effectively rule the phenomenon of cryptocurrencies[26].

3. Regulating cryptocurrencies from a Tax Law perspective

3.1. The U.S. approach

As it often happens, the U.S. play a pivotal role when it comes to deal with new phenomena like new technologies. Therefore, it is not surprising that the U.S. have recently introduced a statutory definition of the concept of cryptocurrency and cleared out the tax treatment of the profits deriving from them, at least for the purpose of federal taxes[27]. Before this long awaited and desired result was finally reached, the IRS (Internal Revenue Service) and the U.S. Courts had to face huge difficulties in coping with the hideous problem of cryptocurrencies. In particular, in 2014 the IRS issued a note aimed at outlining some general principles regarding such currencies[28].

For the purpose of the federal taxes, virtual currencies are to be treated as "property". According to the IRS, the general tax principles applicable to transactions regarding properties shall apply also to transactions involving virtual currencies.

Also, the taxpayer who receives cryptocurrencies in exchange for goods or services, when filing in their tax return, must include the fair market value of such currencies measured in US dollars, at the time the taxpayer received them.

According to the IRS, if the taxpayer holds bitcoins for a certain amount of time, they would be subject to the tax treatment applied to capital gains[29]. The problem with the interpretation of the US Tax Administration is that Bitcoins are not just "property" but also currencies, and this gives rise to uncertainties[30].

---

[26] See HARASIC V., 'It's Not Just About the Money: A Comparative Analysis of the Regulatory Status of Bitcoin Under Various Domestic Securities Laws', in American University Business Law Review, [2014], 3, 487. The Author points out that "if not properly regulated, Bitcoin has the potential to create a disruptive and risky new global monetary system. Bitcoin not only poses grave money-laundering dangers, but also, it has the tendency to result in drastic price fluctuations, which may create various risks for users and investors in bitcoin-based financial products. Notably, regulators should seek a solution that will provide proper oversight and investor protection, without discouraging economic growth and investment".

[27] Virtual Currency Tax Reform Act, H.R. 4602, May 7th, 2014. Curiously, this statute was proposed by MP Steve Stockman (Texas), who was the first member of the U.S. Congress who accepted funds in Bitcoin for his election campaign.

[28] See IRS Notice 2014-21. 2014-16, I.R.B. 938 March 25th, 2014.

[29] In this respect, see PRENTIS M., 'Digital Metal Regulating Bitcoin as a Commodity', in Case Western Law Review, [2015], 66, 609. The Author underlines that "[…] to qualify a bitcoin as a capital asset, the taxpayer would have to not be holding the bitcoin as 'stock in trade' or be a 'dealer of bitcoins'. Any gain from a bitcoin transferred after being held for more than a year would be considered a capital gain. Conversely, if a taxpayer holds bitcoins as inventory in his business, the disposition of the bitcoins would be treated as ordinary gain or loss". See also ROMAN J.A., 'Bitcoin: Assessing the Tax Implications Associated with the IRS's Notice Deeming Virtual Currencies Property', in Review of Banking & Financial Law, [2018], 34. 451.

[30] See MIRJANICH N., 'Digital Money: Bitcoin's Financial and Tax Future Despite Regulatory Uncertainty', in De Paul Law Review, [2014], 64, 237.

To start with, Bitcoin gives birth to a high risk of tax evasion[31]. According to certain commentators, Bitcoin may become a new offshore bank system, which might be used to avoid the application of taxes on capital gains[32]. Chances are that cryptocurrencies at issue may be used as a tax haven, since, for instance, they would guarantee total anonymity to their owners, which would make it hard for the IRS to verify if the taxpayer had obtained any gains or incurred losses.

Secondly, there might be some administrative problems: determining the tax base[33] (and, consequently, the capital gains) could be particularly tough for the taxpayers, considering that virtual currencies can be purchased at different prices, from different sellers and at different times[34]. Also, the IRS Note does not give any hints on the tax treatment of Bitcoin loans[35].

Finally, defining cryptocurrencies as property could not be the best approach, from a U.S. point of view, since the definition of the rights concerning property are defined by States' law (not by Federal law) and the ways these rights can be exercised significantly change from currency to currency[36].

Despite the principles enshrined in the I.R.S. Note, the Virtual Currency Tax Reform Act classifies Bitcoins as foreign currencies, because adopting the definition of the I.R.S. would imply that transactions involving cryptocurrencies would be subject to capital gain tax. Pursuant to the statute at issue, the I.R.S. cannot apply the capital gain tax until five years have passed since it enters into force.

The Virtual Currency Tax Reform Act justifies the equivalence between bitcoin and foreign currencies exclusively with the following statement: bitcoins play the same role as foreign currencies. For the purpose of the statute at issue, a virtual currency is defined as a digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value.

3.2. The EU approach

[31] In this respect, it is necessary to point out that the U.S. Treasury's Financial Crimes Enforcement Network ("FinCEN") held exchanges in cybercurrencies are to be meant as business activities consisting in "money service businesses" (MSB).

[32] See MARIAN O., 'Are Cryptocurrencies Super Tax Havens?', in Michigan Law Review First Impressions, [2013], 38, 38; SLATTERY T., 'Taking a Bit out of Crime: Bitcoin and Cross-Border Tax Evasion', in Brooklin Journal of International Law, [2014], 39, 829.

[33] See ELLIOTT A., 'Collection of Cryptocurrency Customer-Information: Tax Enforcement or Invasion of Privacy?', in Duke Law & Technology Review, [2017], 1, 1. According to the Author "[…] the Notice leaves taxpayers wondering how they are supposed to maintain sufficient records to calculate the tax due. Especially for users who conduce numerous transaction a day, as well as for those that consistently use Bitcoin as a method of payment for everyday consumption, keeping track of the basis for every Bitcoin is unduly burdensome and arguably impossible". See also CHODOROW A., 'Rethink Basis in the Age of Virtual Currencies', in Virginia Tax Review, [2017], 36, 371.

[34] LAMBERT E.E., 'The Internal Revenue Service and Bitcoin: A Taxing Relationship', in Virginia Tax Review, [2015], 35, 88. The Author highlights that "[…] taxpayers lack an authoritative resource to determine the value of their bitcoins since unlike stocks, bitcoins are not actively traded on a regulated market".

[35] See SHAPIRO D.C., 'Bitcoin Loans and Other Cryptocurrency Tax Problems', in Journal of Taxation of Investments, [2017], 33.

[36] See ANTONIKOVA N., 'Real Taxes on Virtual Currencies: What Does the I.R.S. Say, in Virginia Tax Review, [2015], 34, 433.

As it is well-known, the EU does not have a full competence in the area of direct tax law, but it does have a direct competence in the field of VAT. It is no surprise, then, that the first judgment of the ECJ regarding cryptocurrencies involves the application of the VAT Directive[37].

In the case at issue[38], the ECJ had to establish if the activity carried out by Mr. Hedqvist, consisting in the exchange of traditional currencies with virtual currencies and vice versa, represented a provision of services pursuant to art. 2, paragraph 1, of the VAT Directive and, in this case, if art. 135, paragraph 1, of such Directive were to be interpreted meaning that the exchange activities at issue were tax exempt.

On October 14th, 2013, the Swedish Tax Administration had previously held that, lacking a definition of cryptocurrency in the VAT Directive, it was to be treated as a means of payment.

The Skatteverket stated the Bitcoin exchange required the same conditions as the financial intermediation of financial instruments and Bitcoin could be used as well as any other means of payment having legal tender.

Consequently, transactions in such a currency were to be considered as VAT exempt, pursuant to art. 135, paragraph 1, letter e, VAT Directive[39].

First, the ECJ established the transactions involving the exchange of Bitcoin were to be deemed as supply of services pursuant to art. 2 VAT Directive.

Then, for what concerns the VAT regime of such transactions, the Court held the provisions set forth in art. 135, paragraph 1., letter e, applied to the transactions at issue. The Court argued that, since "*it is common ground that the 'bitcoin' virtual currency has no other purpose than to be a means of payment and that it is accepted for that purpose by certain operators*"[40], interpreting the prevision in question as if it ruled only transactions in traditional currencies would result in depriving it of its effects[41]. As it has been correctly pointed out, the solution given by the ECJ could work only as long as the transaction consisted in an exchange of bitcoin with other virtual currency, while it could not be applied if bitcoin were exchanged with goods or services[42].

---

[37] Directive 2006/112/EC of the Council of November 28th, 2006 L 347/1 on a common VAT system.
[38] Case C-264/14 Hedqvist v Skatteverket, ECJ 5th Section, October 22nd, 2015.
[39] For a quick exam of the opinions of the EU Member States on Bitcoin, see CAPACCIOLI S., 'VAT & Bitcoin', in EC Tax Review, [2014], 6, 361. The Author gives also his own interpretation, claiming "[…] bitcoin acts like a security and the failure of an issuer is not decisive under VAT Directive".
[40] Case C-264/14 Hedqvist v Skatteverket, ECJ 5th Section, October 22nd, 2015, paragraph 52. In the following paragraph, the ECJ holds that: "it must be held that Article 135(1)(e) of the VAT Directive also covers the supply of services such as those at issue in the main proceedings, which consist of the exchange of traditional currencies for units of the 'bitcoin' virtual currency and vice versa, performed in return for payment of a sum equal to the difference between, on the one hand, the price paid by the operator to purchase the currency and, on the other hand, the price at which he sells that currency to his clients". See PIASENTE M., 'Esenzione IVA per I "bitcoin": la strada indicata dalla Corte UE interpretando la nozione divise", in Corriere Tributario, [2016], 2, 141.
[41] The ECJ did not rule on the application of VAT provisions to the mining activity. In this respect, see WOLF R., 'Bitcoin and EU VAT', in International VAT Monitor, [2013], 254. According to the Author, also the mining activity is ruled by art. 135 VAT Directive and is, thus, VAT exempt. See also SPAZIANTE F., 'Le operazioni concernenti I "bitcoin": la declinazione pratica dei principi espressi nella sentenza Hedqvist', in Fiscalità e Commercio Internazionale, [2016], 8, 29.
[42] In this respect, see PALUMBO G., 'Il trattamento tributario dei bitcoin', in Diritto e Pratica Tributaria, [2016], 1, 2079.

Once the EU approach has been introduced, it is possible to focus on the Italian approach.

3.3. The Italian approach

Italy has not introduced any piece of legislation that sets forth provisions on virtual currencies. This is why the above-described judgment represents a lighthouse and a starting point for the decisions the Italian Tax Administration has made so far[43].

While the answers of the Italian Tax Administration regarding the application of VAT are not ground-breaking, as they simply copy and paste what the ECJ had previously held in the Hedqvist Case, they certainly appear more interesting when they deal with direct taxation.

First, the Tax Administration states that the activities of buying and selling of cryptocurrencies and exchanging virtual currencies with traditional currencies are relevant for the purpose of the Italian Tax on Company Revenue (IRES, Imposta sul Reddito delle Società), the Italian Tax on Individual Revenue (IRPEF, Imposta sul Reddito delle Persone Fisiche) and the Italian Tax on Regional Productive Activities (IRAP, Imposta Regionale sulle Attività Produttive).

In the first case, a limited liability company asked the Italian Tax Administration if the provision of services concerning the use of virtual currencies, such as the purchase and the sale of Bitcoin for its customers would be subject to IRES. In response, the Italian Tax Administration held IRES would apply to the gain obtained by the company, consisting in the difference between the purchase price and the sale price. Such gain is to be considered as an income deriving from the supply of financial services[44].

In other words, the Italian Tax Administration considered the business activity carried out by the requesting company equal to the provision of financial services, not having regards to the intrinsic characteristics of Bitcoin and held that such activity was subject to IRES and IRAP. For what concerns the Bitcoins remaining at the end of the fiscal year, they must be valued at fair value, pursuant to art. 9, Italian Tax Code, Presidential Decree n. 917, December 22nd, 1986 (TUIR, Testo Unico sulle Imposte sui Redditi).

In the following response, the Italian Tax Administration cleared out that activities such as virtual currency exchange, if not carried out by a business enterprise, give rise to "other income", taxable pursuant to art. 67, paragraph 1, letter c-*ter* and paragraph 1-*ter* TUIR, as much as it happens with activities involving traditional currencies[45].

To sum up, according to the Italian Tax Administration, if a business activity consists in the exchange of virtual currency with traditional currency, the profits deriving from it are taxed as business profits. Conversely, if natural persons have bitcoins outside of their business activity, the income is taxed as "other income".

---

[43] Response n. 72/E September 2nd, 2016 and Response n. 14 to tax ruling n. 956-39/2018.

[44] See CLAPS P. – PIGNATELLI M., 'L'acquisto e la vendita per conto terzi di bitcoin non sconta l'IVA ma rileva ai fini IRES ed IRAP', in Corriere Tributario, [2016], 40, 3073.

[45] The applicability of art. 67, paragraph 1, letter c-ter TUIR had already been suggested by commentators even before the response of the Italian Tax Administration. In this respect, see MOLINARO G., 'Sono tassabili le manifestazioni di capacità economica emergenti nelle operazioni relative a Bitcoin?', in Il Fisco, [2014], 25, 2447.

Let alone the relevance for VAT purposes of the aforementioned activities, a remarkable topic the Italian Tax Administration did not deal with is the exchange of information, pursuant to EU Directive EU/2015/2376 (Common Reporting Standard, CRS) and tax monitoring, pursuant to Legislative Decree n. 90/2017.

More specifically, the Legislative Decree in question establishes service suppliers who deal with virtual currencies are deemed to comply with the money laundering provisions, as set forth by art. 3, paragraph 5, letter I, Legislative Decree November 21st, 2007, n. 231. In fact, those subjects are considered as a category of financial operators.

As it has been correctly pointed out, such a category includes not only the exchangers (those who exchange cryptocurrencies with traditional currencies), but also the wallet providers (those who provide services like the custody of the credential required to have access to virtual currencies)[46].

Even though this is a step ahead towards the transparency of transactions involving bitcoins, it is necessary to keep in mind that in case the transactions do not involve intermediaries, but take place only between privates, or in case of mining, the parties of the transactions will still be anonymous[47].

4. Conclusions: a clash between two systems?

Finally, after having shortly described some issues related to the world of cryptocurrencies and having given a glance at the US, EU and Italian approach, it seems necessary to highlight certain points.

To start with, it is impossible to deny the huge impact of the "virtual world" on the real world, which is evident now more than ever and, at the same time, the vulnerability of the latter and the inadequacy of the legal systems. What is baffling is that the governments and the Authorities – either administrative or jurisdictional – have tried to interpret the phenomenon of cryptocurrencies and the Blockchain technology under traditional paradigms, without realising how innovative they are. This has resulted in approximate and sometimes controversial applications of pre-existing provisions and in a puzzling and confusing mayhem where it is impossible it comes to finding out what to tax and how to tax it.

However, if we think about it, the Blockchain technology exists in a parallel and detached world, which has sometimes an overwhelming influence on the real world, and which can thrive in the absence of a central regulatory authority, because the principles it is based on have nothing to do with those you may find in democratic Constitutions.

In other words, democratic values are things you would not even mention in that context, which may sound quite scary. What is likely to happen is this developing virtual world, with its own rules and the lack of authorities will eventually clash with "our world", made of deeply rooted principles, which is also facing a huge identity crisis. This apocalyptic scenario could only be evaded if the current authorities realised that the traditional juridical tools are not adequate and up to date and if they started to elaborate and process new

[46] See BIXIO I., 'Valute Virtuali e adempimenti antiriciclaggio: riflessi sui soggetti obbligati, nuovi e non', in Corriere Tributario, [2017], 34, 2676.
[47] See MAIORANA D., 'Disciplina giuridica e fiscale delle criptovalute: sfida al legislatore dal web', in Corriere Tributario, [2018], 8, 630.

categories and a new legal framework, which would allow to break through this nebulous barrier represented by the Blockchain world.

Bibliography

1. CFTC Docket n. 15-29 (CFTC Filed September 17, 2015) https://www.irs.gov/pub/irs-drop/n-14-21.pdf;
2. Opinion of the European Central Bank (October 12th, 2016), § 1.1.3;
3. ECB Opinion on Virtual Currencies, EBA/op/2014/08;
4. IRS Notice 2014-21. 2014-16, I.R.B. 938 March 25th, 2014;
5. Response of the Italian Tax Administration n. 72/E September 2nd, 2016 and Response n. 14 to tax ruling n. 956-39/2018
6. South African Reserve Bank (SARB) Position Paper on Virtual Currencies, December 3rd, 2014, SARB 2014;

Books and Articles

1. ALLEN K, 'A Bitcoin Primer', Arizona Daily Star, 2014 https://tucson.com/business/local/a-bitcoin-primer/article_aff0568e-bf71-5c88-b821-38c1b9c4e277.html;
2. ALVARO M. – LEWIS J.T., 'Who Needs Bitcoin? Venezuela has its "Sucre", [2014], http://www.wsj.com/articles;
3. ANAND J., 'Virtual Economies Virtually Unregulated: How Clear Taxpayer Guidance Can Mitigate Tax Compliance Risks', in Hofstra Law Review, [2014];
4. ANTONIKOVA N., 'Real Taxes on Virtual Currencies: What Does the I.R.S. Say, in Virginia Tax Review, [2015];
5. BILANEY S. K., 'From Value Chain to Blockchain – Transfer Pricing 2.0', in International Transfer Pricing Journal, [2018];
6. BIXIO I., 'Valute Virtuali e adempimenti antiriciclaggio: riflessi sui soggetti obbligati, nuovi e non', in Corriere Tributario, [2017];
7. BRYANS D., 'Bitcoin and Money Laundering: Mining for an Effective Solution', in Indiana Law Journal, [2014];
8. CAPACCIOLI S., 'VAT & Bitcoin', in EC Tax Review, [2014];
9. CHODOROW A., 'Rethink Basis in the Age of Virtual Currencies', in Virginia Tax Review, [2017];
10. CIRILLO A. – ATZENI C., 'Aspetti operative, giuridici e fiscali delle criptovalute, in Amministrazione e Finanza, [2018];
11. CLAPS P. – PIGNATELLI M., 'L'acquisto e la vendita per conto terzi di bitcoin non sconta l'IVA ma rileva ai fini IRES ed IRAP', in Corriere Tributario, [2016];
12. ELLIOTT A., 'Collection of Cryptocurrency Customer-Information: Tax Enforcement or Invasion of Privacy?', in Duke Law & Technology Review, [2017];
13. FERRARI E., 'Bitcoin e criptovalute: la moneta virtuale tra Fisco e antiriciclaggio', in Il Fisco, [2018];
14. FRANKLIN M., 'A Profile of Bitcoin Currency: An Explanatory Study', in International Journal of Business and Economic Perspectives, [2016];

15. HARASIC V., 'It's Not Just About the Money: A Comparative Analysis of the Regulatory Status of Bitcoin Under Various Domestic Securities Laws', in American University Business Law Review, [2014];
16. HUGHES S.J. – MIDDLEBROOK S.T., 'Are These Game Changers? Developments in the Law Affecting Virtual Currencies, Prepaid Payroll Cards, Online Tribal Lending, and Payday Lenders', in The Business Lawyer, [2014];
17. HURTADO C.R., 'Fiscal Policies as Decisive Solutions for Troubled Economics: Differing Legislative Enactments in Argentina Ecuador, in Loyola L.A. International & Comparative Law Review, [2014];
18. KIEN-MENG LY M., 'Coining Bitcoin's "Legal Bits": Examining the Regulatory Framework for Bitcoin and Virtual Currencies, in Harvard Journal of Law & Technology, [2014];
19. LAMBERT E.E., 'The Internal Revenue Service and Bitcoin: A Taxing Relationship', in Virginia Tax Review, [2015];
20. MAIORANA D., 'Disciplina giuridica e fiscale delle criptovalute: sfida al legislatore dal web', in Corriere Tributario, [2018];
21. MARIAN O., 'Are Cryptocurrencies Super Tax Havens?', in Michigan Law Review First Impressions, [2013];
22. MIRJANICH N., 'Digital Money: Bitcoin's Financial and Tax Future Despite Regulatory Uncertainty', in De Paul Law Review, [2014];
23. MOLINARO G., 'Sono tassabili le manifestazioni di capacità economica emergenti nelle operazioni relative a Bitcoin?', in Il Fisco, [2014];
24. NAKAMOTO S., 'Bitcoin: A Peer-to-Peer Electronic Cash System', [2008];
25. NIEMAN A., 'A Few South African Cents' Worth on Bitcoin', in PER, [2015];
26. PALUMBO G., 'Il trattamento tributario dei bitcoin', in Diritto e Pratica Tributaria, [2016];
27. PERRY B., Forex Currencies: Commodity Pairs (USD/CAD, USD/AUD, USD/NZD), INVESTOPEDIA;
28. PIASENTE M., 'Esenzione IVA per I "bitcoin": la strada indicata dalla Corte UE interpretando la nozione divise", in Corriere Tributario, [2016];
29. PIAZZA F., 'Bitcoin in the Dark Web: A Shadow over Banking Secrecy and a Call for Global Response', in Southern California Interdisciplinary Law Journal, [2017];
30. PRENTIS M., 'Digital Metal Regulating Bitcoin as a Commodity', in Case Western Law Review, [2015];
31. ROMAN J.A., 'Bitcoin: Assessing the Tax Implications Associated with the IRS's Notice Deeming Virtual Currencies Property', in Review of Banking & Financial Law, [2018];
32. SHAPIRO D.C., 'Bitcoin Loans and Other Cryptocurrency Tax Problems', in Journal of Taxation of Investments, [2017];
33. SMALL S., 'Bitcoin: The Napster of Currency', in House Journal of International Law, [2015];
34. SONDEREGGER D., 'A Regulatory and Economic Perplexity: Bitcoin Needs Just a Bit of Regulation', in Washington University Journal of Law & Policy, [2015];
35. SPAZIANTE F., 'Le operazioni concernenti I "bitcoin": la declinazione pratica dei principi espressi nella sentenza Hedqvist', in Fiscalità e Commercio Internazionale, [2016];

36. TARKOWSKI TEMPELHOF S., ‘Bitnation, Pangea Jurisdiction and Pangea Arbitration Token (PAT), The Internet Sovereignty’, https://tse.bitnation.co/;
37. TU V.K. – MEREDITH M.W., ‘Rethinking Virtual Currency Regulation in the Bitcoin Age’, in Washington Law Review, [2015];
38. VIGNA P. – CASEY M.J., ‘Cryptocurrency: The Future of Money?’, Random House, [2016];
39. WOLF R., ‘Bitcoin and EU VAT’, in International VAT Monitor, [2013].

Case law

1. Case C-264/14 Hedqvist v Skatteverket, ECJ 5th Section, October 22nd, 2015Florida v Espinoza F14-2923, 6 (Florida District Court 2015);
2. SEC v Shavers, 2013, U.S. District. LEXIS 110018 (E.D. Texas August 6, 2013);
3. SEC v W. J. Howey Co., 328 U.S. 293 [1946].

THE UNMANNED AERIAL VEHICLE ON THE LEGAL HORIZON- AN INVASION OF THE RIGHT TO PRIVACY

Michał Lutek[1]

Abstract

Recent years have shown a significant increase in the operations performed by unmanned aerial vehicles. The development of this kind of aircrafts may also impose a threat to several human rights. Drone operators must follow a number of rules not only to avoid causing damages on the ground, but they also have to keep in mind the obligation to comply with norms setting up a human rights regime. The paper aims to show a comprehensive approach towards the issues of violation of right to privacy performed by drones. Firstly, legal definitions of drones are presented. The author discusses the legal framework regarding privacy issues surrounding the use of drones. The analyzed regulations are followed by examples. The author also addresses practical legal issues connected with the use of drones. The references to court rulings are made in the course of the paper.

Key words: drones, privacy, international law, privacy invasion

Introduction

Recent years have shown a significant increase in potential application of unmanned aerial systems. Previously drones-which is a colloquial term used to describe unmanned aerial vehicles, have been used primarily for military purposes. Subsequently they became more accessible to wider group thus their scope of commercial application has been broadened. Nowadays, drones are used both by operators from private sector as well as governmental authorities like police or FRONTEX[2]. In 2017 in Dubai a maiden passenger flight of 18-rotor drone manufactured by German Company Velocopter was performed[3]. Flying drone taxi takes up to 2 passengers on board and should be able to offer flights lasting up to 30 minutes. The above-mentioned shows that in the near future unmanned aerial vehicles, to a certain extent, may replace traditional aircrafts used in civil aviation.

The number of drones registered with the Federal Aviation Authority in the United States of America vividly reflects the popularity of such machines. As per 10th of January 2018, there were 1,000,000 drones registered with the competent authority[4]. This number is

[1] Ph. D candidate at Institute of International Air and Space Law at University of Warsaw. Scientific activities and research interests are focused on aviation law, space law and law of new technologies as well as corporate law with particular reference to start-ups and venture capital.

[2] Frontex begins testing unmanned aircraft for border surveillance, https://frontex.europa.eu/media-centre/news-release/frontex-begins-testing-unmanned-aircraft-for-border-surveillance-zSQ26A (retrieved 8.04.2019).

[3] Dubai tests drone taxi services, https://www.bbc.com/news/technology-41399406 (retrieved 8.04.2019).

[4] „FAA Drone Registry Tops One Million", https://www.transportation.gov/briefing-room/faa-drone-registry-tops-one-million (retrieved 8.04.2019).

composed of two major groups. The first one relates to non-commercial users who perform drone operations solely as a leisure activity, this group is quite numerous as it counts approximately 880 000 machines. The latter; constituting of mostly vehicles used for commercial, public and governmental purposes, is definitely smaller and amounts to 120 000. The development of unmanned aerial system is a serious challenge for international community, especially now when the scope of application of such system has drastically increased. It is often the case, that a rapid technological development does not always go hand in hand with regulations creating a legal framework within which such technologies functionate. Nevertheless, it has to be stressed out that lawmakers, with particular emphasis on European Union, have made a lot effort to create a coherent legal regime for drones.

One cannot forget that drones apart from their beneficial aspects, often pose a threat to safety of aviation thus also to passengers and even third parties unrelated to the flight. The most common drone-related issues are: ground damages, mid-air collisions and trespasses. It has to be highlighted that unmanned aerial vehicles, especially those fitted with cameras and recording devices, can be used as a tool for invading privacy right attributed to both natural and legal persons. This publication aims to present legal aspects related to use of drones with regard to the invasion of privacy right. Firstly, the definition of drone will be outlined. The second paragraph will concern the evolution of privacy right in the international law. Third part will discuss the matter of privacy in a widely understood aviation sector. The summary will be followed by a review of court cases referring to the subject matter of the paper.

1. Definition of drone

Due to the environment in which the aircraft operates which is an airspace, considerations on the subject matter should begin with defining the aircraft sensu stricto. According to Annex VI to the Convention on International Civil Aviation signed on 7th of December 1944 in Chicago, an aircraft should be understood as "Any machine that can derive support in the atmosphere from the reactions of the air other than the reactions of the air against the earth's surface."[5]. It is worth stressing out that, despite the fact that the Chicago Convention uses in article 8 the notion of "aircraft without a pilot" it has not been defined there. According to Karol Karski, incorporating the regulations referring to unmanned aircrafts already in 1944 was dictated by the high level of German activity in this regard during the Second World War[6].

The doctrine uses many notions referring to unmanned aerial vehicles. Chronologically the first was the afore-mentioned concept of "an aircraft without a pilot" as it was introduced by the Chicago Convention in 1944. In 2012, the Task Force on Unmanned Aerial Vehicle Systems (UASS-G) created the definition of remotely piloted aircraft (RPA)[7]. In the light of which, such object should be understood as "Unmanned aircraft that is piloted from a

[5] Annex to Chicgago Convention „6 Operation of Aircraft"

[6] K. Karski, Cywilne bezzałogowe statki powietrzne w świetle przepisów prawa międzynarodowego,in: 50 lat konwencji tokijskiej-bezpieczeństwo żeglugi lotniczej z perspektywy przestrzeni powietrznej i kosmicznej. Księga dedykowana Profesorowi Markowi Żyliczowi, Z.Galicki, K.Myszona-Kostzrewa(ed.), Stowarzyszenie Absolwentów Wydziału Prawa i Administracji UW, Warsaw , 2014, p.128

[7] M.Bujanowski, Bezpieczeństwo lotnictwa cywilnego. Aspekty współpracy międzynarodowej, Wydawnictwo Naukowe Scholar, Warsaw, 2016, p. 75

remote-control station on an aircraft." The European Organization for the Safety of Air Navigation (hereinafter referred to as EUROCONTROL) uses the term "remote-controlled aircraft system" (hereinafter UAS)[8].

While for a layman the designatum of all the above concepts is a drone, for experts in the field of aviation, the interchangeable use of these terms is unacceptable as they have specific differences. When talking about UAS, the term "unmanned" may be misleading as to the autonomy of these objects. They are controlled from ground station operators. It seems that the technological concept and the essence of these machines most accurately reflects the RPA.

Speaking of autonomy, this feature has already been included in the definition set forth by new basic regulation of the European Parliament and the Council on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91[9]. According to the article 3.30 of recently introduced European regulation, an unmanned aerial vehicle shall be understood as any aircraft operating or designed to operate autonomously or to be piloted remotely without a pilot on board[10]. Multitude of definitions may cause some troubles during the processes of legal analysis of the incidents involving drone operators. For the sake of clarity in this paper, drones should be understood as in the definition given in the preceding sentence.

2. Right to privacy

Humans have always strived to protect personal aspects of their lives. Such need is deeply rooted in every human being. Although the concept of privacy is not something new, we have observed a significant increase in the interest in this particular are after the Second World War[11]. This period of time should be also associated with a rudimental date in the history of human right protection which is 4th of November 1950 when, in Rome, the Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter referred to as ECHR) was opened for signatures. Pursuant to article 8 of ECHR “Everyone has the right to respect for his private and family life, his home and his correspondence”. Although, only private and family life is expressly indicated in the this intranational treaty, also such spheres as file or data gathering and everybody’s right to image and photographs are covered by scope of application of ECHR[12]. Almost the same provisions in this matter were stated article 7 of European Charter of Fundamental Rights which says: “Everyone has the right to respect for his or her private and family life, home and communications.”[13].

[8] M.Bujakowski, op.cit.,p. 76.
[9] Official Journal of European Union L 212 vol.61.
[10] Ibidem.
[11] M.Kenyon, M.Richardson (.ed), New Dimensions in Privacy Law: International and Comparative Perspectives, Cambride University Press, 2006.
[12] Directorate of the Jurisconsult, Guide on Article 8 of the European Convention on Human Rights, 2018
[13] Official Journal of the European Union C 326/391

Privacy, along with freedom or equality, forms a catalogue of constitutionally protected values in many national legal systems. Polish constitution in article 47 grants everyone right to "[…] to legal protection of his private and family life, of his honour and good reputation and to make decisions about his personal life."[14]. Also, in common law systems, like the United States of America, right to privacy is reflected in their constitution. This right was introduced to American legal system by Fourth Amendment which prevents unreasonable searches and seizures.

The problem with the privacy right is that, it often remains unclear what should be understood under this term. Sometimes it is improperly equated with data protection, this seemingly two identical notions cannot be used interchangeably[15]. Privacy and data protection share more common features than differences. If we compare them, their conceptual scope shall overlap to a certain extent, meaning that personal information is directly linked with the rights to privacy, which grants a wide-scaled protection including but not limited to data protection[16]. It should be noted in this place, that apart from forgoing concepts, there is also a phenomenon called "dataveillance". This refers to the situations when data is used for the purposes of conducting surveillance of the citizens, thus also passengers[17].

3. Privacy in aviation

Privacy is important in many aspects of human's life. It is especially protected in the sectors where the data being processed is notably vulnerable i.e. banks, hospitals or insurance companies. It has to be stressed out that data we share when booking a flight ticket is also quite vast. The necessity of securing this type of data combined with prevailing tendency towards fighting with terrorism has led to adopting on 27th April 2016 a directive 681/2016 of the European Parliament and the Council on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime[18] (hereinafter referred to as PNR Directive). Due to the topic limitations of this paper I will only briefly address the issue of the PNR data, as an example of data protection legislation in the field of civil aviation.

As mentioned above, the European lawmakers have decided to set up a legal framework for controlling passenger name record data in a form of directive which means that member states of European Union are obliged to take up an implementing measures as, unlike regulations, they are not self-executing. The spectrum of gathered data is quite wide as it reaches from basic information like itinerary through contact details to forms of payment. The data can be accessed by national authorities like border guards or police.

Analyzing the matter of widely-understood privacy in aviation sector, the reference to the airport security measures and body scanners has to be made. During the process of body scanning and regular security control at the airport one's privacy or other fundamental

[14] The Constitution Of The Republic Of Poland Of 2nd April, 1997 As published in Polish Journal of Law No. 78, item 483
[15] S. Gutwirth, R. Leenes, P. de Hert (.ed), Data protection on the move. : Current Developments in ICT and Privacy/Data, Springer, 2016.
[16] O. Mironenko Enerstvedt, Aviation Security, Privacy, Data Protection and Other Human Rights: Technologies and Legal Principles, Springer, 2017.
[17] N. Bessis, F. Xhafa (. ed), Next Generation Data Technologies for Collective Computational Intelligence, Springer, 2011.
[18] Official Journal of the European Union L 119/132

rights including dignity, freedom of movement or physical integrity might be endangered. At the international level, general rules applying to security in aviation result from Annex 17 to Chicago Convention. The need to set a legal regime for such undertakings has also been observed by the Commission and resulted in issuing a special communication date 15th June 2010[19]. The main massage of the aforementioned communication was the need to adopt common standards to guarantee same level of protection in EU member states in respect to the fundamental rights[20]. Moreover, the Article 29 Working Party was of the opinion that the use of scanning machines at the airports involves protection of the data and falls into Directive 95/49EC on Data Protection (replaced by 2016/679 Regulation 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, GDPR) and, thus, has to comply with the principles of necessity and proportionality[21].

Nowadays, one of the rudimental threats to the privacy comes from unmanned aerial vehicles. They can turn out to be really dangerous for commercial airline transport, especially in terms of mid-air collisions but also for individuals when their privacy is at stake.

4. **Invasion of privacy by drone operators**

Although the issue of privacy invasion performed by drone operators has been widely discusses on the forum of the European Union, no legal framework has been introduced. It should be highlighted that some stated in the United States of American did adopt a legislation explicitly referring to the subject matter of this paper. California which is renowned for their technological development, has recently amended their Civil Code, allowing now to held liable those who invade privacy by knowingly entering into the airspace above the land and capturing "[…] any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a private, personal, or familial activity"[22]. Pursuant to the new regulations, the level of their liability amounts up to three times the amount of damages related to the violation, as well as a civil fine of between $5,000 and $50,000. It is also not a coincidence that such law was passed in California-a state preferred by celebrities who were primarily supposed to benefit from this law[23]. The liability is not limited to civil cases, in state of Florida the infringing party may be even charged with criminal charges.

The distinction between private and public users has to be clearly made. The activity of the law enforcement agencies also must be done in compliance with following principles: necessity, proportionality, purpose limitation and data minimization[24]. Processing of the date gathered by drones done by law enforced under no circumstances should enable constant tracking of individuals. Furthermore, a constant review of the necessity to process personal data by the use of drones has to be done by the competent authority-preferably by courts and independent judges.

---

[19] F. Rossi Dal Pozzo, EU Legal Framework for Safeguarding Air Passenger Rights, Springer, 2015.
[20] Ibidem.
[21] J. Figueras Tugas, Privacy and Body Scanners at EU Airports, Privacy and New Technologies, Novatica, 2013.
[22] California Code, Civil Code - CIV § 1708.8 sec. a
[23] J. Azriel, Restrictions Against Press and Paparazzi in California: Analysis of Sections 1708.8 and 1708.7 of the California Civil Code, UCLA Entertainment Law Review, 2017.
[24] Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones, 2015, https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2015/06/wp231_en.pdf (retrieved 12.04.2019)

It is predicted that in 2019 European Parliament with the Council will adopt a law, probably in form of regulation, laying legal grounds for liability of drone operators violating other's right to privacy.

5. Court cases regarding infringement of privacy by unmanned aerial vehicles

The number of drone-related cases will probably grow proportionally with the development of this market and growing range of commercial application of unmanned aerial vehicles. The range of matters brought to court is relatively wide as the proceeding may concern both the problem of liability for damages as well as registration negligence or even more serious crimes like voluntary body injury. This shows that drone operators should bear in mind that they can be held responsible for violation of civil and criminal law. It deserves to be highlighted in this place, that drone operators may cause harm to both natural and legal persons. Whereas in case of the first category it is obvious, an additional explanation shall be made to the latter group.

One of the possible scenarios when a legal person could claim damages from drone operators may regard so called corporate espionage. Probably, nobody would pay attention to drones hoovering outside the window of a conference room where a porotype of a new product is being presented-not yet reveled to the market-but if the footage from such presentations would go public, the technological advance of the company would be destroyed.

Some who do not believe in legal remedies for infringement of law, have tried to take the matter into their own hands. In 2015 in Kentucky, United States of America William Meredith shot down a drone flying over his yard[25]. The man was later arrested on a criminal mischief charge but, finally, the case was dismissed as the judge had classified the act of the drone operator as an invasion of privacy legitimating Mr. Meredith to shoot down the aircraft.

The proof of the topicality of the subject matter the United States, is the fact that there were already some cases brought to the Supreme Court. Three most important cases are jointly referred to as the Aerial Surveillance Trilogy. Professor Joseph J. Vacek, from University of North Dakota has made such reference to the Ciraolo, Dow Chemical and Florida v. Riley cases[26].

Conclusions

The development of new technologies, also drone-based, is unstoppable. Moreover, there is nothing wrong with the technology being developed as long as it goes hand in hand with a reasonable legislation setting up a coherent legal regime. Unfortunately, due the long lasting and very formal law-making processes, this task is getting more and more difficult to accomplish. This often makes lawyer look for analogies to currently applicable regulations.

[25] M. McNabb, The Kentucky "Drone Slayer" Case Dismissed, 2017, https://dronelife.com/2017/03/22/kentucky-drone-slayer-case-dismissed/ (retrieved 10.04.2019).

[26] J.J. Vacek, Big Brother Will Soon Be Watching—Or Will He? Constitutional, Regulatory, and Operational Issues Surrounding the Use of Unmanned Aerial Vehicles in Law Enforcement, North Dakota Law Review, 85:673, 2009.

Having in mind prevailing trends in the respect of data protection reflected for instance by the adopting of General Data Protection Regulation, European legislator proves that privacy is an important value. It also has to be noted, that particular emphasis on this issue should be put during the course of training of the drone operators. It is desired in the democratic society, that lawful behavior of the citizens shall result from their respect to the law and thus from values protected by certain regulations.

The obligation to respect privacy shall also apply to the law enforcement and governmental agencies, as they are provided with a significant surveillance capabilities. Their temptation to break the law is extraordinarily high because possible benefits might turn out to be greater than misdemeanor, they shall pay attention to being exceptionally cautious in this regard.

An interesting solution to consider is the idea of privacy by design which transfers the burden of privacy protection onto the drone manufactures but even in this case it cannot be forgotten that there is a human being behind each vehicle.

Bibliography:

1. Annex to Chicgago Convention „6 Operation of Aircraft”
2. Azriel J., Restrictions Against Press and Paparazzi in California: Analysis of Sections 1708.8 and 1708.7 of the California Civil Code, UCLA Entertainment Law Review, 2017.
3. Bessis N., Xhafa F. (. ed), Next Generation Data Technologies for Collective Computational Intelligence, Springer, 2011.
4. Bujanowski M., Bezpieczeństwo lotnictwa cywilnego. Aspekty współpracy międzynarodowej, Wydawnictwo Naukowe Scholar, Warsaw, 2016, p. 75
5. California Code, Civil Code - CIV § 1708.8 sec. a
6. Directorate of the Jurisconsult, Guide on Article 8 of the European Convention on Human Rights, 2018
7. Dubai tests drone taxi services, https://www.bbc.com/news/technology-41399406 (retrieved 8.04.2019).
8. FAA Drone Registry Tops One Million, https://www.transportation.gov/briefing-room/faa-drone-registry-tops-one-million (retrieved 8.04.2019).
9. Figueras Tugas J., Privacy and Body Scanners at EU Airports, Privacy and New Technologies, Novatica, 2013.
10. Frontex begins testing unmanned aircraft for border surveillance, https://frontex.europa.eu/media-centre/news-release/frontex-begins-testing-unmanned-aircraft-for-border-surveillance-zSQ26A (retrieved 8.04.2019).
11. Gutwirth S., Leenes R., de Hert P. (.ed), Data protection on the move. : Current Developments in ICT and Privacy/Data, Springer, 2016.
12. Karski K., *Cywilne bezzałogowe statki powietrzne w świetle przepisów prawa międzynarodowego,*in: *50 lat konwencji tokijskiej-bezpieczeństwo żeglugi lotniczej z perspektywy przestrzeni powietrznej i kosmicznej. Księga dedykowana Profesorowi Markowi Żyliczowi*, Z.Galicki, K.Myszona-Kostzrewa(ed.), Stowarzyszenie Absolwentów Wydziału Prawa i Administracji UW, Warsaw , 2014, p.128.
13. Kenyon M., Richardson M. (.ed), New Dimensions in Privacy Law: International and Comparative Perspectives, Cambride University Press, 2006**.**

14. McNabb M., The Kentucky “Drone Slayer” Case Dismissed, 2017, https://dronelife.com/2017/03/22/kentucky-drone-slayer-case-dismissed/ (retrieved 10.04.2019).
15. Mironenko Enerstvedt O., Aviation Security, Privacy, Data Protection and Other Human Rights: Technologies and Legal Principles, Springer, 2017.
16. Official Journal of European Union L 212 vol.61.
17. Official Journal of the European Union C 326/391
18. Official Journal of the European Union L 119/132
19. Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones, 2015, https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2015/06/wp231_en.pdf (retrieved 12.04.2019)
20. Rossi Dal Pozzo F., EU Legal Framework for Safeguarding Air Passenger Rights, Springer, 2015.
21. The Constitution Of The Republic Of Poland Of 2nd April, 1997 As published in *Polish Journal of Law* No. 78, item 483
22. Vacek J.J., Big Brother Will Soon Be Watching—Or Will He? Constitutional, Regulatory, and Operational Issues Surrounding the Use of Unmanned Aerial Vehicles in Law Enforcement, North Dakota Law Review, 85:673, 2009.

COMMON LAW RIGHT TO ACCESS TO MEDICAL RECORDS: THE COMMONWEALTH AND EUROPEAN COURT OF HUMAN RIGHTS PRACTICE

Anatoliy Lytvynenko[1]

Abstract

The confidence of patient-physician relationship, inter alia, involves the duty of a non-disclosure of patient's personal information to any third parties, being either strict or qualified and arguable involves a right to access to health records. The latter became a substantial problem owing to various restrictions imposed by health authorities on such data release. In some countries, as in the United Kingdom of the 1970s, courts ruled such health records to be disclosed only to medical advisors or solicitors and even after reversing such judgments, a number of other restrictions were imposed making the access to health records quite arduous to be gained. The European Court of Human Rights occasionally dealt with "access to records" cases as well, predominantly being outstanding for the late 80s Gaskin trial lying in the scope of "respect to private and family life". Apart from the United Kingdom, similar cases arose in several other commonwealth states, posing a complexified issue of the ownership of health records and their maintenance on basis of a proprietary right, but not rather of a fiduciary duty.

Keywords: access to health records; common law right to privacy; right to autonomy; data protection; medical records.

Introduction

The confidential relationship between the patient and physician as a legal concept of vintage, if not ancient nature[2]. The maintenance of patient's health records and by its gist is akin to other professional bilateral legal relationships, such as a solicitor and client, a bank or brokerage agency employee and a depositor[3], or any other similar combinations that may

[1] PhD student at Ivan Franko National University of Lviv (International law); PhD student at Robert Gordon University of Aberdeen (Law/common law). E-mail: anat.lytvynenko@gmail.com

[2] See. D. W. Shuman, The Origins of the Physician-Patient Privilege and Professional Secret, [1985] 39.2 S.M.U.L.R. 661, 667-672.

[3] Occasionally, there were trials for a disclosure of client's personal bank records concerning debts, transactions and many similar items. A substantial number of such cases were decided upon ordinary common law tort doctrines or the theory of implied contract. See: Foster v. Bank of London, 3 F. & F. 214, 215-217 (1862) [breach of (implied or express?) contract]; Dixon v. Holden, L.R. 7 Eq. 488, 491-493 (1869) [libel/fraud]; Tournier v. National Provincial and Union Bank of England, [1924] 1 K.B. 461, 473; 480-481 [slander; breach of implied contract]; Robertson v. Canadian Imperial Bank, [1994] 1 W.L.R. 1493, 1495-1496; 1499-1500 [negligence and breach of contract]; United States: Brex v. Smith, 104 N.J. Eq. (3 Backes) 386, 390-392 (1929) [bank's property rights in clients' personal records]; Annenberg v. Roberts, 2 A.2d 612, 617-618 (1937) [privacy and unreasonable search & seizure]; Peterson v. Idaho First National Bank, 83 Idaho 578, 582-583; 585-589 (1961) [claim for an invasion of privacy, adjudicated upon a breach of confidence]; In Re Addonizio, 53 N.J. 107, 133-134 (1968) [unreasonable search & seizure of mayor's bank records, the dictum recognized the bank's obligation as contractual]; Milohnich v. First National Bank of Miami Springs, 224 So. 2d 759, 761-762

involve professional secrecy[4]. The case law on the subject in the United States, especially in earlier times commonly involved suits for a disclosure of patient's personal information on his or her health state to third parties causing adverse effect on plaintiff in various ways[5]; these cases were not very frequent in older times[6]. The patient's data privacy, despite of

---

(1969) [breach of contractual obligation]; Suburban Trust Co v. Waller, 44 Md. App. 335, 340-344 (1979) [breach of privacy and contractual obligation]; see also Australia: Australian Securities Comm'n v. Zarro et al., 32 F.C.R. 546, 550-551 (1991) [statutory duty of disclosure to a specially empowered body; or when the legislation entitles disclosure of customer's bank account, e.g. in the embrace of legal proceedings, both civil and criminal, see. e.g. Williams v. Summerfield, [1972] 2 Q.B. 512, 517-518; Barker v. Wilson, [1980] 1 W.L.R. 884, 887] In United States, in the Milohnich and Waller cases, the courts gave respect to the Tournier decision by the King's Bench Division, stating (in Waller) that American courts seemingly give less exceptions which were announced in the Tournier case, [1924] 1 K.B. 461 at. p. 473. Various credit agencies and banks, for instance, were subjected to disclose the banking records of clients complying with a subpoena: McMann v. Securities and Exchange Commission, 87 F.2d 377, 378-379 (1937). The case of Brex involved the subject of proprietary rights in clients' asset records which were recognized as property of the bank. There, a prosecutor demanded to check the records of several police officers without commencing a trial or investigation against them and thereafter he was restrained from their inspection; see Brex v Smith, at p. 389-392. Some US states, under their law, do not find credit reporting history to be actionable upon "false light privacy": Polin v. Dun & Bradstreet, Inc. 768 F.2d 1204, 1206-7 (Okla. 1985) [privacy claim failed as credit reporting to subscribers was not "public"]; Schoneweis v. Dando, 231 Neb. 180, 183; 189-191 (1989); or a limited disclosure of debtor's crediting information: Graney Development Corp v. Taksen, 92 Misc. 2d 764, 768-769 (1978). In Germany, a similar question arose before the Supreme Court in 1927 (then its name was the Reichsgericht). In the case of IV 489/26 (reported as 115 RGZ 416), a merchant in his early 40s sued a credit reference agency for disclosing his criminal affairs when the plaintiff was young. He was convicted for perjury, embezzlement, attempted fraud, he was amnestied and thereafter led a virtuous life, but his criminal records remained and were disseminated twenty years after to the customers of the said agency. Plaintiff managed to prevail in action on basis of a personal right violation (named "personlichkeitrecht" in Germany) as well as a "breach of good morals" (see p. 416-419). A number of intriguing notes on the banking confidentiality were presented in a relatively recent work by Mr. Stokes, namely R. Stokes, The Genesis of Banking Confidentiality, [2011] 32 J.L.H. 279, 282-289

[4] For instance, see an extended analogy interpretation in K. B. Remick, Breach of Confidence – The Need For a New Tort – Watts v. Cumberland County Hospital System, [1985] 8 C.L.R. 145, 146-147; 153-154. On issues of the confidence of bank employee and depositor, or debtor-creditor relationships, as discussed in fn. 3, see J. K. Le Valley & J. S. Lancy, The IRS Summons and The Duty of Confidentiality: A Hobson's Choice for Bankers, [1972] 89 B.L.J. 979, 988

[5] See, for instance, Simonsen v. Swenson, 104 Neb. 224; 177 N.W. 831, 832 (1920) Berry v. Moench, 8 Utah 2d. 191, 197-198 (1958), Clark v. Geraci, 29 Misc. 2d 791, 793-794 (1960); Horne v. Patton, 291 Ala. 701, 707-709 (1973); Fedell v. Wierzbieniec, 485 N.Y.S.2d 460, 462-463 (1985)

[6] Quoting Tournier, at p. 479, per Scrutton, L. J.: "It is curious that there is so little authority as to the duty to keep customers' or clients' affairs secret, either by banks, counsel, solicitors or doctors. The absence of authority appears to be greatly to the credit of English professional men, who have given so little excuse for its discussion". It's difficult to say how old the medical data privacy is. For instance, A. Hopper, The Medical Man's Fiduciary Duty, [1973] 7 L. T. 73, 74-75. In this article, Mr. Hopper gives a brief, but a very interesting vintage common law legacy on this type of breach of confidence. I would possibly name a few older cases on the subject, but in the terms of brevity, I would agree with his position, adding that the Canadian case of Halls v. Mitchell [1927] S.C.R. 125. There an ex-serviceman attempted to strike out a compensation for an iritis attack while working on a railway, but his application was rejected as he was thought to contract it within his military service, but not on the railroad. These inferences were made on basis of his earlier health records. Therefore, the plaintiff sued a physician who had communicated his medical history and other personal information to other doctors and bodies, which made his ordeal for compensation, fail. The Supreme Court of Canada (at p. 146-148) found that the acts of the physician were not justified by an urgent need, finding for plaintiff. In fact, the action was for libel, as the doctor misspelt the diagnosis abbreviation and so communicated this mistake to others (see at p. 130-131). This was exactly a common law development of data protection law and thus medical data privacy is seemingly even more vintage then Halls. The confidentiality of medical personal data was recognized in the 19th century in United

being recognized by courts since a very early date[7], quickly became a subject of qualifications: indeed, the aspect of health record disclosure were mainly upon medical evidence at a civil or a criminal trial rather than a disclosure of medical secret of the patient to a third party (e.g. an another physician[8], the plaintiff's employers[9], or insurers[10], or in a memoire with a full disclosure of patient's medical records[11]). In American common law, in case a doctor discloses the personal data of his patient, or his "medical secrets"[12], he will be liable for a breach of an implied contract of secrecy that derives from the confidence of physician-patient relationship, or on basis of a privacy invasion, or a confidence breach[13]; and in some cases, it may be an action for defamation if plaintiff alleges that the communicated information was not truthful[14]. As a general rule, under ordinary circumstances, the physician has to keep the records confidential, maintaining their privacy[15]. A common law duty of confidence is applied to the hospitals in regard to patients as well[16]. As in any other type of confidential relationships, the retention mode of patient's data will not be absolute. Indeed, the United States courts, despite recognizing the confidence[17] concluded that the duty to non-disclosure of patient's personal data is far not of

---

States: Buffalo Loan & Trust & Safe Deposit Co. v. Knights Templar & Masonic Mutual Aid Assn., 27 N.E. 942, 944 (N.Y. 1891). Mr. Hopper cites two "anonymous" cases in Scotland affirming confidentiality of medical records and reports, being adjudicated in 1851 and 1904 respectively (they were cited both as "AB v. CD"), while in fact their names are Whyte v. Smith, 14 D. 177 (No. 46); 24 S.C. 78 (1851) as well as McEwan v. Watson [1904] S.C. 213. In Continental Europe, the principle of confidentiality of medical records was decently depicted in the German case of Günther v. Gerhard, B.G.H.Z. 24, 72, 78-81 (1957). At such point, I wouldn't fancy to discuss something even more old or obscure, but some authors attempted to investigate on the ancient nature of professional confidence principle in British common law.

[7] See. Halls v. Mitchell [1927] S.C.R. 125 and discussion note 6 supra; note W. K. Bernfield, Medical Secrecy, [1972] 3 Cam.L.R. 11, 12-13

[8] Holzman v. Zimmerman, 47 Pa. D. & C. 3d 608, 616-618 (1988)

[9] Clark v. Geraci, 29 Misc. 2d 791, 793-794 (1960); Horne v. Patton, 291 Ala. 701; 287 So. 2d 824, 827-830 (1974)

[10] Hague v. Williams, 37 N.J. 328, 331 (1962); Hammonds v. Aetna Casualty & Surety Group, 243 F. Supp. 793, 799-802 (1965); Rea v. Pardo, 522 N.Y.S.2d 393, 395 (1987)

[11] Doe v. Roe, 93 Misc. 2d 201, 204-205 (1977)

[12] These "medical secrets" are nothing more than a more old-fashioned label for "sensitive personal data" which is a more attractive and trendy word shaping patient's records which are bound to be disclosed (see a definition in Griffith v. Austman Hospital, 146 Ohio St. Rep. 196, 200-202 (2016)), such as psychiatric records of the patient: In Re Lifschutz, 2 Cal. 3d 415, 423-428, etc. (1970), or infant health records in the custody of municipal health authorities involving the same: . The health records are presumed not to be made up from communications or already reported and documented entries, but from the observations and examinations of the physicians: Capps v. Lynch, 116 S.E. 137, 140 (1960); Cates v. Wilson, 321 N.C. 1, 13-14; 361 S.E.2d 734, 740-742 (1987).

[13] Horne v. Patton, 291 Ala. 701; 287 So. 2d 824, 830 (1974); Doe v. Roe, 93 Misc. 2d. 201, 209-211 (1977). In Hammer v. Polsky, 36 Misc. 2d. 482 (1962) an alleged disclosure of confidential information made plaintiff commence a suit for malpractice, but no bilateral confidential relationship was proved and thus the action failed.

[14] See. Berry v. Moench, 8 Utah 2d. 191; 331 Pa. 814, 816-817; 819-820 (1958)

[15] Hague v. Williams, 37 N.J. 328, 332 (1962)

[16] Estate of Behringer v. Medical Center, 297 N.J. Super. 597, 632 (1991)

[17] Some decisions attribute this confidence to various statutory duties: Munzer v. Blaisdell, 183 Misc. 773, 775 (1944); Doe v. Roe, 93 Misc. 2d 201, 205-207 (1977). The confidence of the physician-patient relationship itself hadn't actually been doubted: Hammonds v. Aetna Casualty & Surety Co., 24 F. Supp. 793, 797-801 (1965). Some courts contended that initially, there was no common law privilege as to doctor-patient communications: Capps v. Lynch, 253 N.C. 18, 21-22; 116 S.E. 2d 137, 140-141 (1960). In the beginning of the 20th century, some courts held that there was no common law duty of secrecy, but rather a sort of a statutory one: Smith v. John L. Roper Lumber Co., 147 N.C. 62; 60 S.E. 717, 718-719 (1908). The problem of communication secrecy within the subject is quite an aged one: see a discussion on it in Metropolitan Life Ins. Co. v. Boddie, 194 N.C. 199; 139 S.E. 228

absolute character[18]. Apart from administration of justice, where a court order may compel a physician to disclose the information for needs of trial, there may be some other specimen. The instances of confidence waiver (without patient's consent) may occur when the person reported would likely to bring hazard to others[19], or be contracted with a disease contagious to the ones surrounding[20]. Upon legislative provisions, the physicians may be obliged to report medical records of the patients[21], or as extension of a physician's common law duty or care as well[22]. A number of various US jurisdiction decisions held that the toll of personal information that may be communicated and exchanged should not be more than it is required for one separate trial, as an action for personal injury or malpractice; in such situation, this confidence may be derogated[23]. The patient may waive this confidence by his own will, for instance consenting (or at least, not objecting), or by commencing a lawsuit on medical malpractice or personal injuries wherein medical records would be disposed in the course of the proceedings[24]. Since not only hospitals are possessors of health records, but so are various factories concerning their employees' health data, the state authorities may move for a court order their disclosure in the course of inspection of the working conditions; however the disclosure may be tapered only to specific records but not all of them[25]. Therefore, I will not test the contention that, as it was held in the 70s and 80s cases that the patient-physician relationship involving confidence derives from Hippocratic oath[26], or is a protocol practice having it's routes in some ethics code (and I even do not doubt that it has got it's splendid place in this protocol, just like, seemingly the rule of consent to treatment was said to be of such nature[27]); but every litigation may be a more complicated thing than an interpretation in an ethics code. In fact, the ethics code or similar regulations could be

---

(1927). Still, as most of the cases cited herein are from North Carolina, we may presume that the confidence may be narrowed for justice administration for sure. The Boddie ruling, however, gave a space for maneuvers: the doctor would not be compelled to give medical evidence unless the legislation would order so. That is, these common law and statutory duties may vary from one jurisdiction to another but most of them are alike.

[18] See, for instance, Simonsen v. Swenson, 104 Neb. 224; 177 N.W. 831, 832 (1920); Berry v. Moench, 8 Utah 2d. 191, 197-198 (1958), or Clark v. Geraci, 29 Misc. 2d 791, 793-794 (1960); Horne v. Patton, 291 Ala. 701, 707-709 (1973); Fedell v. Wierzbieniec, 485 N.Y.S.2d 460, 462-463 (1985). Indeed, the older cases were much based upon medical evidence rather than a disclosure of medical secret of the patient: Smith v. Driscoll, 94 Wash. 441 (1917). However, as time passed the qualifications for disclosure became too apparent not to be applied at common law).

[19] Tarasoff v. Regents of University of California, 17 Cal. 3d 425, 431 (1976) [suit by parents of a murdered woman brought to recover damages for non-confinement of a psychiatric patient who killed her]; Davis v. Lhim, 124 Mich. App. 291, 298-302 (1983) [suit for negligence of a psychiatric patient discharge who was likely to cause violence to others]

[20] Jones v. Stanko, 160 N.E. 456; 118 Ohio St. 147, 150 (1928) [smallpox infection; the Ohio legislation provided a code regulation obliging the physician discovering a hazardous case to report it, including all personal data of the patient]

[21] In Re Lifschutz, 2 Cal. 3d 415, 428 etc. (1970)

[22] Hunter v. Mann [1974] Q.B. 767, 771-773; see also A. Samuels, The Duty of Doctor to Respect the Confidence of Patient, [1980] 20 M.&Sc.&L. 58, 58-61. The American case of Alexander v. Knight, 197 Pa. Super. 79; 177 A 2d. 142, 146-148 (1962), displayed a contrary view to the English case of Hunter.

[23] See, for instance, Garner v. Ford Motor Co., 61 F.R.D. 22, 23-24 (1973); Anker v. Brodnitz, 98 Misc. 2d 148, 151 (1979) and cases cited therein.

[24] Cates v. Wilson, 321 N.C. 1, 14; 361 S.E.2d 734, 741-742 (1987)

[25] U.S. v. Westinghouse Electric. Co., 638 F2d. 570, 578-580 (1980)

[26] Hague v. Williams, 37 N.J. 328, 332 (1962); Hammonds v. Aetna Casualty and Surety Co., 243 F. Supp. 793, 797 (1965); Horne v. Patton, 287 So. 2d. 824, 829 (1974); Roe v. Doe, 93 Misc. 2d 201, 205; 211, (1977); Moses v. McWilliams, 549 A. 2d 950, 956 (1982)

[27] Bolam v. Friern Hospital Management Committee, [1957] 1 W.L.R. 582, 588-591; see also Chatterson v. Gerson, [1981] 1 Q.B. 432, 442-445 [per Bristow, J.]

derogated by the needs of justice, as it was in *Allegheny County Grand Jury Investigation of June 1979*[28].

Main body

Thus, having stated the issue of data privacy within medical confidence, let us turn to a more recent problem, namely to the access to patient's medical records by himself, his solicitors or medical advisors. What are the reasons for accessing? The primary reason for it is obviously for trial – in a suit for negligence, personal injury or a wrongful death medical records are valuable evidence, if such may be admissible at all[29]. In some instances, adults being abandoned at birth would wish to know their forbearer's identity, commonly a grossly secret type of personal information: such outstanding trials are known in US (e.g. for a specimen where access was granted, *Massey v. Parker*[30]) as well as to European Court of Human Rights (*Odievre v. France*[31], restriction prescribed by law). Of very high confidence are HIV records, the disclosure of which may subject the physician to various tort and statutory liability[32]. So are psychiatric records[33]. Occasionally, in the course of investigations, the subpoenas may be announced by grand juries, workman compensation boards and other bodies in order to produce health records of the patients furnishing sensitive personal information[34]. After the enactment of the Administration of Justice Act in 1970, it became possible to apply to a court obtain access to records by a an order; before its adoption the only way of compelling a hospital to produce records was a *subpoena*[35]; in fact the construction of the said statute presumed that the records were bound to be disposed only for the needs of *trial*, but not for any other purposes, as, for instance, mere curiosity or for any extra-judicial matters. The personal records of the patient, being in custody of hospital, or some health or municipal authorities[36], were assumed to be *property*, but qualified in the sense that in the scope of right to autonomy, the patient should have access to all his records – this was the position of the Court in *ex parte Martin*[37]. Therefore, after the Act was enacted, the trials did not make us to wait for long. Initially, English courts did not recognize a patient's common law right to access to *hospital* (note the italics) records, only limiting this disclosure to a medical or legal advisor, in some instances

[28] 415 A.2d 73, 76-77 (1979)
[29] See inferences on the subject upon the American common law: R. B. Dunsmore, Hospital Records as Evidence, [1959] 8 C.-M.L.R. 459, 463-464
[30] 369 So. 2d 1310, 1314-1315 (1979)
[31] 42336/98 [2003] E.C.H.R. 86
[32] At the same time, the identities of blood donors and other personal data in cases where a person (plaintiff) was contracted with AIDS by the transfusion may be disclosed : Boutte v. Blood Systems Ltd, 127 F.R.D. 122, 125-126 (1987); Stenger v. Lehigh Valley Hospital Center, 609 A.2d 796, 803 (1992), see cases cited on p. 803. This rule is not uniform.
[33] In some jurisdictions, psychiatric records were even bound to be disclosed upon a subpoena: In Re B, 394 A. 2d 419, 425-426 (1978) [per curiam]; contra: Ceasar v. Mountanos, 564 F2d. 1064, 1068-1069 (1978). Pennsylvania recognized the right to privacy in psychological test results in a child custody litigation over the necessity to disclose them to other parties involved: In Re T.R., 731 A.2d. 1276, 1280-1282 (1999)
[34] In Re June 1979 Allegheny Cty. Gr. Jury, 415 A.2d 73, 76-78 (1980)
[35] Davidson v. Lloyd Aircraft Services Ltd., [1974] 1 W.L.R. 1042, 1045
[36] Very decently illustrated in Gaskin v. Liverpool City Council, [1980] 1 W.L.R. 1549, 1551-1553 [per Denning, L. M.R.]; 1554-1555 [per Megaw, L.J].
[37] Regina v. Mid Glamorgan Family Health Services Authority & Another / Ex Parte Martin, [1995] 1 W.L.R. 110, 116; 119-120

to third parties as independent experts, but *not to plaintiff personally*[38]. The case of *Dunning* was the first to deal with the application of the Act. Plaintiff, a woman who underwent treatment from pneumonia and other ailments in 1963 was dissatisfied with it as her three-month treatment was unsuccessful resulting in a deterioration of her health. In 1969 she received legal aid and a medical adviser made a report concluding it would be necessary to reveal hospital records in order not to prolong litigation. She applied to the court to get access to the medical records and notes; after the lower court order the health board appealed contending that the provision concerning pre-trial discovery was inapplicable for them, but the Court held it was, as a) patient was prospective plaintiff; b) the board was likely to be a party at trial; c) it definitely had the needed documents in their possession. Thus, appeal dismissed[39]. In *Deistung v. South West Metropolitan Health Board* a father and an infant daughter attempted to sue a hospital for negligence. The girl and father were poisoned and the child was unsuccessfully treated, undergoing two laparotomies but fully recovered after being put into another hospital; what is notable, a surgical registrar suspected a pregnancy (which was later withdrawn). The hospital agreed to disclose the records only to a medical adviser, not to plaintiffs' lawyers or themselves. The adviser made a report of her treatment, but the solicitors found it to be not sufficient enough to prevail in action. The Court found that the adviser who made the report would be a potential expert witness for plaintiff and so he would be able to communicate with the hospital further on necessary details; therefore plaintiffs and counsel could communicate with the adviser but the records would not need to be disclosed to them[40]. In *Davidson v. Lloyd Aircraft Services*, a liaison engineer brought an action against his employers to recover damages for having contracted tertian malaria having suffered some complexifications rendering him incapable for work. In 1969 plaintiff was sent to Zanzibar not being vaccinated before and so he developed malaria in a week; after being treated and returning to work, he experienced major heart problems, so he brought an action against Lloyd Aircraft Services, and his solicitors wished all health records (concerning his treatment in 1969 and 1973) to be disclosed to a professor, a specialist in tropic diseases, as well as to themselves and to plaintiff. The order of the lower court was to reveal all the records, but the Court of Appeal found only a limited disclosure would be suitable as 1) non-professionals may conceive them incorrectly; 2) the prognosis or any other doctor's notes may be too deplorable to be disclosed; 3) the existing statements (which are not always verified) could be embarrassing to the patient and his relatives; 4) records are highly confidential and so the physicians may deter from entering them fully and frankly if they know that records may be disclosed beyond their profession[41]. Thus, the Court upheld the appeal finding the disclosure to be limited to the professor, but not more. The decision of *McIvor* overruled the aforementioned ones. Plaintiff brought an action against one Reid for personal injuries sustained in a car accident and sought discovery attempting to figure out whether his ailments were provoked by accident or by his previous maladies. The body which possessed his medical records appealed to quash the lower court's order to produce the documents and limit it only to his medical adviser but not to plaintiff himself or his solicitors, but the House of Lords found that the 1970 Act provisions concerning production of records are not meant to be so limited as 1) solicitors could ask an assistance of a medical advisor to interpret them; 2) these records

[38] See, for example, Dunning v. United Liverpool Hospitals' Board of Governors, [1973] 1 W.L.R. 586 (per curiam) and Deistung v. South West Metropolitan Regional Hospital Board, [1974] 1 W.L.R. 213, 215-217. On the same subject was Davidson v. Lloyd Aircraft Services Ltd., [1974] 1 W.L.R. 1042. The said cases were overruled by the McIvor decision.

[39] Dunning v. United Liverpool Hospitals' Board of Governors, [1973] 1 W.L.R. 586, 590 etc.

[40] Deistung v. South West Metropolitan Regional Hospital Board, [1974] 1 W.L.R. 213, 216-217

[41] This construction was analyzed and withdrawn in McIvor v. Southern Health & Social Service Board, [1978] 1 W.L.R. 757, 760-761

are bound to be used beyond one trial; 3) if there is an urgent need the records may not be shown to plaintiff personally, e.g. in case they are detrimental to him. Thus, the board's appeal was dismissed[42]. The discovery of health records in the possession of municipal authorities remained limited: in *Gaskin v. Liverpool City Council*, plaintiff having a "bad record" and being in the custody of various foster parents, orphanages and hospitals at his child years blamed defendant in negligent care, as he experienced various (involving psychiatric) health problems and was unable to find a job; so in order to be confident he would prevail in action, plaintiff desired to see all of his records, so did his advisors. The Court, however was on the position that the childcare reports should not be disclosed and there is public interest in maintaining them confidential[43] citing analogous cases on the subject[44]. The Gaskin case later went to the European Court[45]. A very similar case was *Martin*, where plaintiff applied to disclose his medical records (suspecting to find more on some incidents which happened to him in the 1960s), though not contemplating to commence an action against anyone. He was refused on basis of the finding the facts he plead to discover would be too detrimental for him; though the Court found that he generally had a common law right to access to health records, it was in his "best" interests not to see them and the hospital had discretion to choose not to unveil the records[46]. The 80s trials of the Scientology Church against the Department of Health and Social Security arose from allegedly libelous letters by defendant claiming that Church representatives had inexpertly treated mental patients some of whom went more deteriorated, plaintiffs commenced several libel suits, but were restrained in disposing health records of the patients being limited to one medical adviser; it was held that although they had a right of inspection upon a definite action, it had to be limited to avoid abuse of process[47].

The American cases on access to health records are not too frequent and are not bound as to their content to be shown to some solicitors unlike the English ones. As early as 1940, in the trial of *Goldwater*, the City Council of New York demanded Lincoln Hospital to produce all patients' records upon a subpoena in the course of maladministration investigation but hospital officers refused to divulge most records but few; the Court of Appeal found that such evidence wouldn't be admissible under this privilege statute[48]. Forty years later in similar case, the Supreme Court of Indiana found necessary to produce patients' records in the course of *Allegheny County Grand Jury Investigation*[49]. The New York statute was held to be not applicable in case plaintiff demanded the records: in *Hoyt*, a woman contracted syphilis after a blood transfusion and applied for discovery prior to file a negligence suit; the Court found the hospital could not avoid producing the records[50]; the same conclusion was reached by an another New York court in *Weiss* where plaintiff was to file a negligence suit and the hospital sealed the names of the doctors who performed malpractice[51]. In fact, application to produce records prior to a malpractice suit became common, especially in New York since mid-20th century[52]. In *Gotkin*, plaintiff desiring to write a book on her experience and requested her medical records, but was refused; she claimed

[42] Id, p. 759-761
[43] Gaskin v. Liverpool City Council, [1980] 1 W.L.R. 1549, 1552-1553 [per Denning, L.J]
[44] See. In Re D (Infants), [1970] 1 W.L.R. 599, 600 etc.; D v. NSPCC, [1978] A.C. 171, 242-246 (summary)
[45] (1989) 12 E.H.R.R. 36
[46] Ex parte Martin, [1995] 1 W.L.R. 110, 117-119
[47] Church of Scientology v. DHSS, [1979] 1 W.L.R. 723, 728 etc.
[48] N.Y. City Council v. Goldwater, 31 N.Y.2d 31, 32-33 (1940)
[49] 415 A.2d 73, 76-77 (1979)
[50] Hoyt v. Cornwall Hospital, 169 Misc. 361, 363 (N.Y. 1940)
[51] In re Weiss, 147 N.Y.S 2d. 455, 456 (1955)
[52] See. Gotkin v. Miller, 514 F.2d 125, 128-129 (1975) and cases cited.

proprietary rights in her records, but the Court found she had none though stating patients have some right to control their medical records[53]. In *Cannell*, one of the most outstanding of these cases, plaintiff's agent demanded his medical record and defendant refused claiming he had property rights in his records and such were to be handed in only upon a subpoena and not upon a prehearing discovery, the Court found that one of the fiduciary duty of the physician is to disclose the records for patient's best interests and holding that the patient doesn't need to commence a lawsuit in order to obtain the records[54]. In *Rabens*, a lawyer who was hospitalized and treated at defendant's clinics asked a copy of his hospital bill and his medical record, but was refused to get the bill copy free and was supplied with an abstract of his record; though he didn't succeed in stating a cause of action for mental anguish, he prevailed in his counts for a breach of duty to furnish records, both a common law, and a statutory one[55]. In *Rogders v. St. Mary's Hospital of Decatur*, a man whose wife died two days after giving birth to a baby filed a negligence action against the hospital and physicians. He contended that his spouse died of volvulus which could have been found on the X-ray, but the hospital failed to maintain the roentgens which could supposedly give stringent evidence of negligence and thus he lost the suit; so, he brought an action against hospital and managed to recover on basis of an X-ray preservation act obliging hospitals to keep roentgens for five years and more in case such would be disposed as evidence at trial; the issue of his conjectural loss of suit against physicians due to non-preservation of X-rays was addressed to the trier of fact[56]. Concerning some other commonwealths, Scottish courts found that production of medical records could be done by a court order and no common law right to access exists (case of *Boyle*, etc.[57]). Canada recognizes a common law right such access upon *McInerney v. Macdonald*[58]. In an analogous trial of *Breen v. Williams*, the High Court of Australia found there was no such a right under contract, property law or under a fiduciary duty[59].

The European Court of Human Rights has repeatedly faced data privacy cases involving various circumstances, but the entries on allegedly wrongful data disclosure are not frequent; through the years, some trials were dedicated to tax and financial records disclosure[60], personal records retention[61] (probably, the case of *Leander* is the most outstanding one), intelligence records discovery[62] and several cases concerning access to medical records. The *Gaskin* trial, supposedly being one of the leading data privacy cases of the European Court arose from the 1980 trial. There, upon the facts abovestated, plaintiff recovered on basis of the Court's findings he didn't have an independent body to appeal. The Court recognized jurisdiction over access to health records as a particle of "private and family life" and held plaintiff had had a justified interest in his health records. To the same conclusion the Court came in the trial of *MG v. United Kingdom*. There plaintiff being in custody of orphanages desired to gain access to childcare and medical records in order to

[53] Id., 129
[54] Cannell v. Medical and Surgical Clinic, 315 N.E.2d 278, 280 (1974)
[55] Rabens v. Jackson Park Hospital, 351 N.E.2d 276, 278-280 (1976)
[56] 149 Ill. 2d 302, 307-310; 312-313 (1992)
[57] [1969] S.C. 69, 77-84
[58] [1992] 2 S.C.R. 138, 157-161
[59] [1996] H.C.A. 57, various
[60] Compare the principles applied: Denoncourt v. Com. State Ethics Com'n, 470 A.2d 945, 947-950 (Pa. 1983) and Wypych v. Poland, N2428/05 (2005); see also: GSB v. Switzerland, [2015] ECHR 1122; compare: California Bankers Assn. v. Schulz, 416 U.S. 21 (1974)
[61] [1987] 9 E.H.R.R. 433. Compare, e.g. with Laird v. Tatum, 408 U.S. 1 (1972); what as to medical records retention, see S. & Marper v. United Kindgom [2008] ECHR 1581; compare: Eddy v. Moore, 5 Wash. App. 2d 334; 487 P.2d 211, 213-214 (1971)
[62] Szulc v. Poland, [2013] 57 E.H.R.R. 5, 163-167 (see facts on pages cited)

reckon up the memories on his custody and facts he had been violently treated by his father, as well as foreseeing a negligence lawsuit in case such records would tend to show he was mistreated by municipal bodies. He gained some access, but limited and not depicting most of his adolescence years which were basically not conveyed neither to him nor his solicitors. The Court found that since he plead for documents covering a substantial period of his life he had vital interest and no independent body to appeal, and so found that plaintiff was entitled to relief[63].

The case of *Miculic v. Croatia* featured a suit to establish paternity. Plaintiff, an infant suing on behalf of mother was born in concubinage. The mother applied to a Croatian trial court to establish a one man's paternity. The proceedings went in an inadequate manner where the case, being initially adjudicated in favor of defendant, being repeatedly affirmed, reversed and remanded; defendant not once obstructed the proceedings by being absent (likely to avoid the order for a DNA-test which could confirm his paternity). However, the appellate court found the evidence of his absence at trial not to be sufficient to affirm his paternity and thus quashed the trial court decision remanding the case. Then defendant and his counsel continued to obstruct the proceedings which had started over four years before. This brought plaintiff to the European Court, which found firstly the length of proceedings was inadequate; secondly, the Court had jurisdiction over actions for paternity claims in respect within the scope of "right to respect private and family life"; and thirdly, establishment of paternity for child (plaintiff) by revealing her father's identity constituted her "private life interest" and hence the failure of domestic courts to do it had been a violation of the Convention's provision regarding the right to privacy[64].

The case of *Odievre v. France* was initially a discovery suit. Plaintiff was a French national born in 1965, abandoned by her forbearers. She was adopted years later and carried the Odievre surname thereafter but 20 years later she applied to a local child welfare service in Seine (where she was registered) to obtain the information on her parents. Having received depersonalized information, plaintiff applied to the court to receive an order to disclose the true identity of her forbearers, believing she had had siblings and desiring to learn more information on them. She was refused. The Court confirmed its jurisdiction under the provisions of private life protection in respect with health records and denoted it was not very typical for most the European countries' to permit anonymized childbirth and abandonment, but France seemingly had a centuryfold tradition of such legislation, dating back to seventeenth century, as well as the contemporary legislation. Moreover, existing French law provided plaintiff could obtain access to depersonalized records. Thus, judgment of the French court was affirmed finding that the restriction of access to records was in compliance with the law[65].

Conclusion

The medical confidence extends to patient's health records which results in the possessor's liability for disclosure of the records with few qualifications. The common law access to patient's health records is of relatively recent concern and is desired to be exercised primarily upon the following reasons: a prospective suit for negligence or personal injuries; a paternity claim suit; a discovery for different reasons (which is less frequent). In

[63] [2003] 36 E.H.R.R. 3, 27-29
[64] [2002] E.C.H.R. 27
[65] [2003] F.C.R. 621

England the access to records used to be limited to medical advisers or clearly specified persons. Even after *McIvor*, the records in the possession of municipal authorities involving medical ones remained restricted and subject to various qualifications. The American case law on the subject is more liberal. The cases in other commonwealths are not frequent and are diverse both in principle and in the decisions. The subject of access to medical records is also featured in the European Court case law involving paternity claims and discoveries.

Bibliography

1. D. W. Shuman, *The Origins of the Physician-Patient Privilege and Professional Secret*, [1985] 39.2 S.M.U.L.R. 661

2. R. Stokes, *The Genesis of Banking Confidentiality*, [2011] 32 J.L.H. 279

3. J. K. Le Valley & J. S. Lancy, *The IRS Summons and The Duty of Confidentiality: A Hobson's Choice for Bankers*, [1972] 89 B.L.J. 979

4. A. Hopper, *The Medical Man's Fiduciary Duty*, [1973] 7 L. T. 73

5. W. K. Bernfield, *Medical Secrecy*, [1972] 3 Cam.L.R. 11

6. A. Samuels, *The Duty of Doctor to Respect the Confidence of Patient*, [1980] 20 M.&Sc.&L. 58

7. R. B. Dunsmore, *Hospital Records as Evidence*, [1959] 8 C.-M.L.R. 459

DATA PORTABILITY THROUGH THE LENS OF COMPETITION LAW

Iga Małobęcka-Szwast[1]

Abstract

Although the main objective of the right to data portability enshrined in Article 20 of the GDPR is to ensure that data subjects are in control of their personal data, its impact goes beyond data protection. As it enables users to switch easily between service providers, the data portability right may also reduce lock-in inherent to many, in particular online, services. Thereby, can be regarded as a pro-competitive and pro-consumer right, which is of interest also for competition policy. By reducing switching costs and consumer lock-in, data portability can lower entry barriers for potential competitors and stimulate competition in a given market. However, having regard to these pro-competitive effects, incumbent firms may find it profitable to restrict data portability, lock customers into their services and consequently prevent them from switching to competing providers. As a result, they may be able to exclude competitors from the market, prevent entry of new ones and further entrench their established market position, leading to a market outcome undesirable from competition law perspective.

In this context, the right to data portability, which at the first sight seem to be of interest only to data protection laws, may acquire also a competition law dimension. In particular, it can be argued that a refusal of a dominant undertaking to facilitate data portability may constitute both a form of an exploitative abuse or exclusionary abuse contrary to Article 102 TFUE. Against this background this paper attempts to answer the question whether it is possible and necessary to enforce data portability also under EU competition law by way of Article 102 TFEU. Intrinsically, this question requires determining the scope of enforcement of the data portability right under GDPR and instances under which this enforcement may not be sufficient to ensure a level-playing field for firms competing in specific markets.

Keywords: Data portability, Big data, personal data, GDPR, competition law, abuse of dominant position

Introduction

The General Data Protection Regulation (GDPR)[2], which is applicable as of 25th May 2018, significantly broadened the scope of data subject's rights. In Article 20 GDPR

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

[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

introduced the right to data portability, which was a novelty for the existing data protection law regime[3]. The right to data portability provides a data subject with a right to receive his personal data from a data controller, and to transfer them to another data controller, subject to limitations and conditions which will be discussed further below.

However, although the main objective of the right to data portability is to ensure that data subjects are in control of their personal data (recital 68 GDPR) and that they trust the digital environment[4], it is widely recognized as a pro-competitive and pro-consumer right[5]. As it enables users to move their data from one service provider to another, it reduces the costs resulting from switching and mitigates the lock-in effect inherent to many services[6].

Although the data portability right is not limited to online environment, its role seems to be particularly visible in context of online services. In online environment both lock-in and switching costs are main factors that may prevent consumers from switching from the current service provider to a new one, thereby raising a barrier to entry for potential competitors[7]. Without being able to have its data transferred to a new provider, consumers may find it too cumbersome, for example in context of social networks, to rebuild their profile and re-insert their personal data. That, in turn, may effectively discourage them from using services of a competing provider, which as a result may not be able to gain critical mass of users necessary to achieve a viable scale of operation. Such scenario may be therefore tempting for a dominant undertaking, which by refusing data portability may lock-in its users and raise entry barriers to a particular market[8]. Consequently, an incumbent may be able to exclude competitors from the market, prevent entry of new ones and further entrench its market position.

---

movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[3] M. Czerniawski, 'Komentarz do art. 20 RODO', in: E. Bielak-Jomaa, D. Lubasz (eds.), 'RODO. Ogólne rozporządzenie o ochronie danych. Komentarz' (Wolters Kluwer Polska 2017), LEX.

[4] Commission Staff Working Paper — Impact Assessment accompanying the General Data Protection Regulation and the Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, SEC(2012) 72 final [25 January 2012] ("Impact Assessment report") 3, 41, 72, 75.

[5] J. Drexl, 'Designing Competitive Markets for Industrial Data - Between Propertisation and Access' [2017] 8(4) JIPITEC 286; M. Czerniawski, 'Komentarz do Art. 20 RODO', in: E. Bielak-Jomaa, D. Lubasz (eds.), 'RODO. Ogólne rozporządzenie o ochronie danych. Komentarz' (Warszawa: Wolters Kluwer Polska 2017), LEX. Different approach is presented by W. Wiewiórowski (Assistant Supervisor at the EDPS), who claims that the pro-consumer meaning of the right to data portability is not self-evident, because the use of consumer data by the controller receiving data may not necessarily benefit the consumer. Consumer may not always be fully aware of how the data will be used by the new controller. In his view excessive use of the right to data portability may adversely affect innovation, inhibit competition and impose disproportionate obligations on entities. See: W. Wiewiórowski, 'Prawo do przenoszenia danych w ogólnym rozporządzeniu o ochronie danych osobowych' [2017] EPS 5 23-30.

[6] I. Graef, J. Verschakele, P. Valcke, 'Putting the right to data portability into a competition law perspective' [2013] 2; I. Graef, 'Data Portability at the Crossroads of Data Protection and Competition Policy', Big Data e Concorrenza [9 November 2016] LUISS Guido Carli 1.

[7] I. Graef, 'Mandating portability and interoperability in online social networks: Regulatory and competition law issues in the European Union' [2015] 39(6) Telecommunications Policy 503, 505-506; D. Geradin, M. Kuschewsky, 'Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue' [2013] 9.

[8] C.S. Yoo, 'When Antitrust Met Facebook' [2012] 19(5) George Mason Law Review 1155; D. Geradin, M. Kuschewsky, Ibid., 9.

Therefore, it seems legitimate to argue that data portability should be perceived not only as a data subject's right, but also as an important duty for undertakings[9]. This is particularly important in case of dominant firms, since restrictions of data portability they impose may be capable of significantly distorting competition on a given market[10]. For these reasons, it is argued that the right to data portability should also be seen as a regulatory tool that aims to stimulate competition and innovation in data-driven markets[11]. Thereby, the right to data portability, which at the first sight seem to be of interest only to data protection laws, may acquire also a competition law dimension[12].

Against this background this paper analyses the question whether it is possible and necessary to enforce data portability also under EU competition law by way of Article 102 of the Treaty on the Functioning of the European Union (TFEU)[13]. Intrinsically, this question requires determining the scope of enforcement of the data portability right under GDPR and instances under which this enforcement may not be sufficient to ensure a level-playing field for firms competing in specific markets.

The structure of this paper is as follows. First, the scope of right to data portability under GDPR is outlined. Then, it is explained why data portability has also a competition law dimension. Next, it is discussed whether competition law has a role to play in enforcing data portability within a broader meaning of this term, and what limitations this enforcement may face. Finally, concluding remarks will be provided.

1. The scope of the right to data portability under GDPR

The global debate about data portability stems from the need to ensure that internet users are able to move the content they have created with significant effort on one website (such as lists of friends, e-mail address books, photos, posts or profile data) to the other[14]. In this context, data portability emerged as a tool enabling widespread transferring of information between websites. This broad concept of data portability was, however, only partially introduced to the GDPR.

The right to data portability enshrined in Article 20 of the GDPR provides data subjects[15] - an individual to whom the data relates - with a right to receive personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format, and a right to transmit those data to another

[9] S. Lucchini, J. Moscianese, I. de Angelis, F. Di Benedetto, 'Online Digital Services And Competition Law: Why Competition Authorities Should be More Concerned About Portability Rather than About Privacy' [2018] 9(9) Journal of European Competition Law & Practice 565.
[10] R.C. Picker, 'Competition and Privacy in Web 2.0 and the Cloud' [2008] 103 Northwestern University Law Review Colloquy 6-8.
[11] I. Graef, M. Husovec, N. Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' [2018] 19(6) German Law Journal 1359.
[12] See e.g.: D. Geradin, M. Kuschewsky, Ibid., 10-11; I. Graef [2015], Ibid. 508.
[13] Treaty on the Functioning of the European Union (Consolidated version) [2012] OJ C 326/47.
[14] G. Zanfir, 'The Right to Data Portability in the Context of the EU Data Protection Reform' [2012] 2 (3) International Data Privacy Law 149.
[15] According to Article 4(1) GDPR, a data subject as "an identified or identifiable natural person". An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. In this paper, the terms „data subject," „user", „individual" and „consumer," will be used interchangeably.

controller without hindrance from the controller to which the personal data has been provided. Without hindrance from the controller means that the controller should not put in place any legal, technical or financial obstacles which would slow down or prevent the transmission of the personal data to the individual, or to another organisation[16]. Where technically feasible, the data subject has also a right to have the personal data transmitted directly from one controller to another (Article 20 (2) GDPR).

Thus, the right to data portability consists of three elements: (1) a right to receive a copy of personal data; (2) a right to have personal data transmitted without hindrance from the controller[17]; (3) a right to have personal data transmitted directly between controllers without participation of data subject (if technically feasible)[18].

As can be observed from the text of Article 20 GDPR, the data portability right is subject to a number of requirements and limitations. First of all, it applies only where the processing is carried out by automated means and is based either on the data subject's consent or a contract. It does not apply where processing is based on a different legal ground (recital 68 GDPR). Secondly, the right to data portability covers only personal data of a data subject which he or she has provided to the controller. According to Article 29 Working Party's guidelines on the right to data portability[19], the term "provided by the data subject" should be interpreted broadly, as including data that result from the data subject activity or observation of his or her behaviour. Nevertheless, it does not cover "inferred data" and "derived data", which include personal data that are created by a service provider as a result of subsequent analysis of the data subject's behaviour[20].

The third limitation is that the exercise of the right to data portability should not adversely affect the rights and freedoms of others (Article 20 (4) GDPR). Thus, if the transmission would adversely affect the rights and freedoms of others, a controller may refuse to undertake the transmission[21]. Fourthly, a controller can refuse to comply with a request for data portability if it is manifestly unfounded or excessive, in particular because of their repetitive nature (Article 12(5) GDPR). In such case, the controller can either charge a reasonable fee taking into account the administrative costs of complying with the request or refuse to deal with the request. In the latter case, the controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request. Finally, data portability encompasses the right to have personal data transmitted directly between controllers, where such a transfer is "technically feasible". In fact, the latter element of data portability right seems to be the most important from the competition law perspective. By allowing a data subject to freely move his data between data controllers, it stimulates competition between data controllers and drives innovation.

However, GDPR does not provide any explanation with regard what is meant by "technically feasible". This, in turn, leaves a substantial leeway and even a room for potential

[16] ICO, GDPR Guide, available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/.
[17] ICO, Ibid.
[18] M. Czerniawski, Ibid.
[19] Article 29 Working Party, Guidelines on the right to data portability, adopted on 13 December 2016, as last revised and adopted on 5 April 2017, WP 242 rev.01 ("Guidelines").
[20] Guidelines 10.
[21] ICO, Ibid.

abuse for data controllers to who may find it profitable to prevent transfer of user's data to another controller[22].

Having regard to all the above-mentioned remarks, it is apparent that the right to data portability under GDPR has rather limited scope. Article 20 GDPR focuses on the data portability only from the perspective of the individual users (data subjects) and even in that regard it provides multiple restrictions on its applicability[23]. Not surprisingly, GDPR, which mainly aims at protecting personal data of individuals, is not concerned with the rights of businesses or other entities that cannot be qualified as data subjects under GDPR, in particular other service providers and competitors. Nonetheless, as will be shown below, data portability concept and its implications for both competition and consumer welfare go beyond the narrow framework of GDPR protection[24].

2. The broader meaning of data portability and its relevance for EU competition law

As already noted, whereas the main policy objective of the data portability right under GDPR was to ensure that individuals **are in control of their personal data and trust the digital environment[25],** it may also reduce switching costs that the users have to incur while changing service providers and the resulting lock-in effect[26]. In particular in online environment, high switching costs and the lock-in effect are main factors that may prevent consumers from switching from the current service provider to a new one[27].

From the theoretical perspective, **switching costs** are the costs (both perceived and real) incurred by customers when they change brands or suppliers[28]. Customers face a switching cost if they make investments specific to their current provider that they would have to duplicate for any new provider[29]. Switching costs can include financial costs but also the value of customers' time and efforts made e.g. to create a profile on a social network or build reputation on e-commerce platforms[30]. In practice, due to switching costs customers may be deterred from changing providers and lock them in to a particular platform or technology[31]. If the switching costs are high, providers will be able to create a high degree of

[22] A. Diker Vanberg, M.B.Ünver, 'The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?' [2017] 8(1) European Journal of Law and Technology available at: http://ejlt.org/article/view/546/726.
[23] A. Diker Vanberg, M.B. Ünver, Ibid.
[24] I. Graef, M. Husovec, N. Purtova, Ibid., 1362.
[25] Impact Assessment report 41.
[26] I. Graef, M. Husovec, N. Purtova, Ibid., 1365.
[27] I. Graef [2015] 503, 505-506; D. Geradin, M. Kuschewsky, Ibid., 9; G. Zanfir, Ibid., 152.
[28] P. D. Klemperer, 'Markets with consumer switching costs' [1987] 102(2) Quarterly Journal of Economics 375–376; J. Farrell, P. Klemperer, 'Coordination and Lock-In: Competition with Switching Costs and Network Effects', in: M. Armstrong R. Porter (eds.), 'Handbook of Industrial Organization' Volume 3 (Elsevier 2007) 1977.
[29] J. Farrell, P. Klemperer, Ibid., 1977; C. Shapiro, H.R. Varian, 'Information Rules. A Strategic Guide to the Network Economy' (Boston: Harvard Business School Press 1999).104.
[30] A.S. Edlin, R.G. Harris, 'The Role of Switching Costs in Antitrust Analysis: A Comparison of Microsoft and Google' [2013] 15(2) Yale Journal of Law and Technology 176. In many cases, it is often value of customer's time that is the most important factor influencing decision about switching.
[31] I. Graef, 'EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility' (Alphen aan den Rijn, The Netherlands: Kluwer Law International 2016) 40.

user lock-in[32]. Consequently, even if a user prefers products of a competing provider, he will not be willing to switch, if he calculates that the costs of switching exceed its benefits[33].

High switching costs are particularly common in case of online services, such as social networks, e-mail or messaging services. The reason behind it is that users upload and generate increasing amount of data on platforms they use, and the more user data is stored on a given platform, the more difficult it will be for a user to leave it[34]. For example, users of social networks tend to spend increasing amount of time and efforts in creating their profiles, uploading content such as videos, photos or posts, or engaging in interactions with other users. If they want to switch to a competing social network, and are unable to take their carefully created dataset along, they are likely to face switching costs[35]. They would have to duplicate the investment and costs they have already made on the current platform, i.e. re-enter their profile data, and upload photos, videos and other content to a new platform again[36]. Depending on the value users attach to such dataset, they may perceive is as too time-consuming and burdensome and may not be willing to switch to a competing provider, even if it offers products or services of better quality[37].

In practice, switching costs resulting from the inability to transfer data between service providers and consumers' lock-in may create substantial barrier to entry for potential competitors[38]. Even if a competing provider offers products or services of better quality or superior technology, it may be unable to attract locked-in consumers, who will not be willing to bear the costs of adapting to a new platform[39]. In turn, without users, any competitor would not be able to enter the market and viably compete with established market players.

In order to understand the importance of data portability for market entry, it is worth comparing it with number portability in the telecommunications field[40]. If a telephone user wanted to change operator, but was not able to retain his telephone number, he would most probably stick with operator of his first choice, so as not to lose his number and possibly also contacts. Similarly, a social network or email user would not want to switch to a competing provider, if he risked losing all the uploaded data and content or, respectively, list of contacts and emails. In such a way, users often become locked-in to their early choices[41], which may actually become long-term commitments[42]. Thus, restrictions on data portability may prevent even a more efficient competitor from gaining critical mass of users and achieve a viable scale[43]. For providers that rely on data provided by users as the main input to their

[32] C. Shapiro, H.R. Varian, Ibid., 104.
[33] A.S. Edlin, R.G. Harris, Ibid., 176.
[34] P. Moura, 'Data Portability Series: Capitalising on the Market for Interoperability' [16 April 2014] available at: https://blogs.lse.ac.uk/mediapolicyproject/2014/04/16/data-portability-series-capitalising-on-the-market-for-interoperability/.
[35] I. Graef [2016], Ibid., 43; P. Swire, Y. Lagos, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique' [2013] Maryland Law Review 72(2) 338; A. Lambrecht, C. E. Tucker, 'Can Big Data Protect a Firm from Competition?' [2015] 338.
[36] I. Graef [2016], Ibid., 43.
[37] D. S. Evans, R. Schmalensee, 'A Guide to the Antitrust Economics of Networks' [1996] 10 Antitrust 37; J. Farrell, P. Klemperer, Ibid., 2033; I. Graef [2016], Ibid., 40.
[38] D. Geradin, M. Kuschewsky, Ibid., 9; C.S. Yoo, Ibid., 1155.
[39] D. S. Evans, R. Schmalensee, 'A Guide to the Antitrust Economics of Networks' [1996] 10 Antitrust 37; J. Farrell, P. Klemperer, Ibid., 2033. I. Graef [2016], Ibid., p. 40.
[40] D. Geradin, M. Kuschewsky, Ibid., 9; I. Graef [2015] 506-508.
[41] J. Farrell, P. Klemperer, Ibid., 1970-1971, 1976.
[42] J. Farrell, P. Klemperer, Ibid., 1976.
[43] D. S. Evans, 'The Antitrust Economics of Multi-Sided Platform Markets' [2003] 20(2) Yale Journal on Regulation 365.

businesses, limiting data portability is a way to tie users to their services and secure their established user base and entrench their market position[44].

In that regard, it seems apparent that influence of data portability goes beyond data protection and may have far-reaching implications also for competition policy[45]. Data portability, by enabling users to move their data from one service provider to another, reduces the switching costs and mitigates the resulting lock-in effect, which arise in case of all products or services that require specific investments by users[46]. Thereby, it also lowers entry barriers for potential competitors, which would not have to offset potential switching costs to users, and stimulate competition in a given market. Having regard to the above remarks, it is apparent that data portability has an important competition law dimension[47].

As argued by the former Competition Commissioner J. Almunia, the right of data portability "*goes to the heart of competition policy*" [48]. In order to develop a healthy competitive environment in a market, it is crucial to allow consumers to "*easily and cheaply transfer the data they uploaded in a service onto another service*" [49]. He emphasized that data portability is particularly important on the markets that "*build on users uploading their personal data or their personal content*", and in such case retention of these data may serve as barriers to switching, which effectively can lock in customers to a company of their first choice. He also stated that "*if customers were prevented from switching from a company to another because they cannot carry their data along*" then this could be a "*competition issue*"[50].

Although the former Competition Commissioner made this statement in context of the EU reform of data protection laws, its significance goes beyond the framework of GDPR. Whereas the data portability right enshrined in the GDPR applies only to personal data, it should be emphasized that the switching costs and the lock-in effect are not restricted only to personal data and relations between business and consumers (B2C)[51]. A lock-in effect may equally arise in business (B2B) relations and with regard to non-personal data.

For example, in case of e-commerce platforms, the lock-in effect arises on the sellers' (i.e. business) side. Prevailing e-commerce platforms such as eBay or Amazon provide wide range of tools (such as rating systems, consumer feedback or trust scores) that allow sellers to build a reputation on their platforms based on the prior transactions[52]. However, the reputation they built on one platform cannot be transferred to another platform[53]. Since the potential buyers may not be willing to transact with sellers without established reputation,

---

[44] I. Graef, J. Verschakele, P. Valcke, Ibid., 6.
[45] I. Graef, M. Husovec, N. Purtova, Ibid., 1359-1398; I. Graef, 'Data Portability at the Crossroads of Data Protection and Competition Policy', Big Data e Concorrenza [9 November 2016] LUISS Guido Carli 1.
[46] I. Graef, J. Verschakele, P. Valcke, Ibid., 2; A. Diker Vanberg, M.B.Ünver, Ibid.
[47] I. Graef [2015], Ibid., 508.
[48] J. Almunia, 'Speech: Competition and personal data protection, Privacy Platform event: Competition and Privacy in Markets of Data Brussels' [26 November 2012].
[49] Ibidem.
[50] Ibidem. See also: 'Businesses that fail to adhere to data portability rules could face investigation into anti-competitive behaviours, says EU Commissioner' [27 November 2012] available at: http://www.out-law.com/en/articles/2012/november/businesses-that-fail-to-adhere-to-data-portability-rules-could-face-investigation-into-anti-competitive-behaviour-says-eu-commissioner/.
[51] J. Drexl, Ibid., 286.
[52] J. Haucap, U. Heimeshoff, 'Google, Facebook, Amazon, eBay: Is the internet driving competition or market monopolization?' [2014] 11(1) International Economics and Economic Policy 58.
[53] Ibidem. That is why reputation systems of e-commerce platforms are considered „sticky". See: R.C. Picker, Ibid., 6.

sellers may be reluctant to switch to a new provider for fear of losing their critical asset – reputation. Thereby, sellers may become locked-in to the platform of their first choice[54]. That, in turn, may prevent potential competing platforms from entering the market, and lead to market "tipping" in favour of a small number of established players, or even result in dominating the market by a single platform[55]. Ultimately, such markets become more vulnerable and open to exclusionary or exploitative practices of dominant players[56]. Therefore, some scholars argue even that the lack of data portability can be even seen as a potential **source of monopoly power**[57].

This case illustrates that preventing business parties (e.g. sellers) from transferring their data (e.g. reputation and transaction history) to a competing provider may have equally negative consequences for competition in terms of entrenching dominance by incumbents, as in the case of personal data of consumers.

Therefore, since data portability is considered a most suitable form of pro-competitive regulation counteracting the lock-in effect, it seems that there is no reason why the data portability should be limited exclusively to personal data or B2C relations[58]. As GDPR protection of the right to data portability is limited to personal data and is subject to specific restrictions, competition law appears as a tool that could complement the GDPR and enable portability of data in cases falling outside scope of the GDPR[59].

Therefore, in the next section it is analysed under what circumstances data portability in its broader meaning can be enforced under the EU competition law.

3. Enforcing data portability through EU competition law

It is argued that depending on the factual circumstances, imposing restrictions on data portability may constitute an abuse of a dominant position under Art. 102 TFEU[60]. However, possibility to pursue restrictions on data portability under EU competition law is subject to specific conditions, which will be outlined below.

3.1. General remarks on abuse of dominance under Art. 102 TFEU

[54] R.C. Picker, Ibid., 6; I. Graef [2016], Ibid., 42-43.
[55] C. Shapiro, H.R. Varian, Ibid., 176; R. Whish, D. Bailey, 'Competition Law' (London: Oxford University Press 2012) 12; M. Bourreau, A. de Streel, I. Graef, 'Big Data and Competition Policy: Market power, personalised pricing and advertising' [2017] CERRE report 29.
[56] V. Diker Vanberg, M.B. Ünver, Ibid.
[57] C.S. Yoo, Ibid., 1154.
[58] J. Drexl, Ibid., 286.
[59] V. Diker Vanberg, M.B. Ünver, Ibid.; S. Lucchini, J. Moscianese, I. de Angelis, F. Di Benedetto, , Ibid., 563. The author knowingly will not elaborate on the issue whether violation of the data portability right in particular and data protection law in general may constitute an infringement of competition law. That topic was subject of her paper submitted for the 6th International Conference of PhD students and Young Researchers "Digitalization in Law". See: I. Małobęcka, Data protection as a competition concern: can data protection violation amount to abuse of a dominant position?, in: "Digitalization in Law" conference papers 94-106, available at: http://lawphd.net/wp-content/uploads/2018/09/International-Conference-of-PhD-studentand-and-young-researchers-2018.pdf.
[60] I. Graef, J. Verschakele, P. Valcke, Ibid., 7; A. Diker Vanberg, M.B. Ünver, Ibid.

Article 102 TFUE prohibits an abuse of a dominant position by one or more undertakings. Hence, in order to determine that an undertaking has abused its dominant position under Art. 102 TFEU, it is essential to, firstly, establish that an undertaking concerned holds a dominant position on a given relevant market, and, secondly, that it has abused its dominant position.

Therefore, a first step in any abuse of dominance case is to define the relevant (product and geographical) market and, subsequently, to establish that a particular undertaking holds a dominant position on that market[61]. Under EU competition law, dominance is defined as "*a position of economic strength enjoyed by an undertaking, which enables it to prevent effective competition being maintained on a relevant market, by affording it the power to behave to an appreciable extent independently of its competitors, its customers and ultimately of consumers*"[62]. This independence means that dominant undertaking's decisions are largely insensitive to the actions and reactions of competitors, customers and, ultimately, consumers[63]. However, being dominant or having significant market power is not in itself a competition problem, as long as an undertaking does not abuse it[64]. Nonetheless, the Court of Justice of the European Union (CJEU) in *Michelin* indicated that a firm in a dominant position has a "special responsibility not to allow its conduct to impair undistorted competition" on the internal market[65].

In general, abuse of dominant position can take different forms and the list included in Art. 102 TFEU is not exhaustive[66]. The CJEU in its case law has significantly extended the list of practices that qualify as an abuse under Art. 102 TFUE[67]. Typically, they are divided into exclusionary and exploitative abuses[68]. Whereas exclusionary abuse covers different types of practices that aim at excluding competitors from the relevant market and restrict competition, exploitative abuse consists of directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions, thereby exploiting customers or suppliers. In other words, prohibition of exploitative abuses aims to protect the opposite market side (customers, suppliers, consumers) from being exploited by a dominant undertaking. While exploitative abuses directly harm consumers or customers, exclusionary abuses harm consumers or customers in an indirect way, as the result of exclusion of competitors[69]. In its enforcement practice, the European Commission gives priority to exclusionary abuses[70]. The latter are also more often identified than exploitative abuses[71].

---

[61] R. Whish, D. Bailey, Ibid., 180-181.

[62] Case 27/76 United Brands Company and United Brands Continentaal v Commission, ECLI:EU:C:1978:22, par. 65. However, economists would not consider whether an undertaking has a dominant position but whether it has substantial market power. See: R. Whish, D. Bailey, Ibid., 180.

[63]Communication from the Commission - Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, OJ C 45/7 ("Guidance"), par. 10.

[64] Guidance, par. 1.

[65] Case 322/81 Michelin v Commission, ECLI:EU:C:1983:313, par. 10.

[66] R. Whish, D. Bailey, 'Competition Law', Ibid., 193. See also: Case 6/72 Continental Can v Commission, ECLI:EU:C:1973:22, par. 26.

[67] R. Whish, D. Bailey, Ibid., 193.

[68] R. Whish, D. Bailey, Ibid., 201.

[69] P. Akman, 'The Role of Exploitation in Abuse under Article 82 EC' [2009] 11 Cambridge Yearbook of European Legal Studies 165.

[70] Guidance, par. 2.

[71] K. Coates, 'Competition Law and Regulation of Technology Markets' (Oxford: Oxford University Press 2011) 27.

3.2. Potential abuses resulting from restrictions on data portability

From the theoretical point of view, it seems that a refusal of a dominant undertaking to facilitate data portability may constitute both a form of an exploitative, as well as exclusionary abuse[72]. In the first case, a dominant firm may take advantage of its privileged position and exploit its users or customers by locking them into its services and preventing them from switching to competing providers that may offer better or more privacy-friendly service, thereby restricting their choice of competing offers[73]. An exploitative abuse in this context can be perceived as a stand-alone abuse that goes beyond the data portability right under GDPR and may not necessarily be derived from it. In this sense, a refusal to transfer data to another provider may directly harm consumers or customers who are unable to switch to a different provider that offers better or more innovative services. However, the current decision-making practice of the European Commission and the case law of the CJEU on exploitative abuses is rather limited and provides little guidance on how such case could be established under Art. 102 TFEU[74].

In turn, an exclusionary abuse can arise on the premise that a dominant firm, which restricts portability of consumers' or customers' data, may raise entry barriers for competitors, for whom such data is necessary to viably compete in a given market. Consequently, an incumbent may be able to drive its competitors out of the market, prevent entry of new ones and strengthen its market power[75]. Some scholars argue that restrictions on data portability may amount to infringement of Art. 102 (b) TFEU by limiting markets and technical development to the prejudice of consumers[76]. However, it may equally constitute a new type of abuse which is not explicitly listed in Article 102 TFEU[77]. As already mentioned, the list of abuses in Article 102 TFEU is not exhaustive, and also other unilateral practices, not explicitly mentioned in Article 102 TFEU, can fall under its scope.

Regardless of the classification of restrictions on data portability under Article 102 TFEU, if a competition authority finds that a dominant undertaking has thereby abused its dominant position, it is entitled to impose remedies on the dominant undertaking that aim at bringing the infringement effectively to an end[78]. In case of a lack of data portability, authorities could impose a duty on a dominant provider to enable users or customers to transfer their data between services[79].

While so far there has been no competition case directly concerning restrictions on portability of user data or competitors' access to user data in the European Union[80], basing on the above cited statement of the former Competition Commissioner, it cannot be excluded that the European Commission will intervene within its powers of a the EU competition watchdog if a dominant undertaking does not allow users to transfer their data to

[72] I. Graef, 'Data Portability at the Crossroads of Data Protection and Competition Policy', Big Data e Concorrenza [9 November 2016] LUISS Guido Carli 2; I. Graef, M. Husovec, N. Purtova, Ibid., 1391.
[73] I. Graef, M. Husovec, N. Purtova, Ibid., 1391.
[74] P. Akman, Ibid., 169.
[75] I. Graef, 'Data Portability at the Crossroads of Data Protection and Competition Policy', Big Data e Concorrenza [9 November 2016] LUISS Guido Carli 2; A. Diker Vanberg, M.B. Ünver, Ibid.
[76] C.S. Yoo, Ibid., 1154-1155; D. Geradin, M. Kuschewsky, Ibid., 11; I. Graef, J. Verschakele, P. Valcke , Ibid., 7.
[77] A. Diker Vanberg, M.B. Ünver, Ibid.
[78] Article 5 and 7(1) of Council Regulation 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty [2002] OJ L1/1.
[79] I. Graef, J. Verschakele, P. Valcke, Ibid., p. 7.
[80] I. Graef, Y. Wahyuningtyas, P. Valcke, Ibid., p. 383.

competing service providers[81]. Current Competition Commissioner M. Vestager also announced that "*if a company's use of data is so bad for competition that it outweighs the benefits*" the European Commission "*may have to step in to restore a level playing field*"[82]. In particular, it might be the case if few companies that control vast amounts of data, use this data to drive their rivals out of the market[83].

However, one aspect of the abuse of dominance investigation against Google initiated by the European Commission in 2010 relates to restrictions on portability of customers (advertisers) data and provides evidence for the above-mentioned statement[84]. The European Commission expressed a concern that Google by imposing restrictions on the portability of online advertising campaign data from its platform AdWords to competing online advertising platforms could be in breach of Article 102 TFUE[85]. In the Commission's view Google must stop imposing contractual obligations on advertisers that prevent them from transferring their advertising campaigns to rival search advertising platforms[86], which in other words, hinders data portability.

The concern is that such restrictions are likely to lock-in advertisers to Google's online advertising platform (AdWords). Since the costs of recreating an online advertising campaign are high, smaller advertisers will most probably use only Google's AdWords[87] and be deterred from switching, even if competing providers may offer better and cheaper options[88]. That in turn may have a negative effect on other online search advertising platforms (Google's competitors such as Bing), which may be consequently excluded from the online advertising market[89].

The Commission negotiated with Google about commitments that would remedy the identified anticompetitive concerns[90]. As a result, Google committed to remove restrictions on the ability for search advertising campaigns to be run on competing search advertising platforms[91]. However, the case is pending and it is not clear whether the Commission will

[81] D. Meyer, 'Facebook beware? EU antitrust chief warns over data portability' [27 November 2012] available at http://www.zdnet.com/facebook-beware-eu-antitrust-chief-warns-over-data-portability-7000007950/; D. Geradin, M. Kuschewsky, Ibid., p. 11.

[82] M. Vestager, Speech: Competition in a big data world [17 January 2016] available at: https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/competition-big-data-world_en.

[83] Ibidem.

[84] I. Graef [2015], Ibid., 508; European Commission, 'Antitrust: Commission probes allegations of antitrust violations by Google' [30 November 2010] available at: http://europa.eu/rapid/press-release_IP-10-1624_en.htm?locale=en#footnote-2.

[85] European Commission, 'Antitrust: Commission probes allegations of antitrust violations by Google' [30 November 2010] available at: http://europa.eu/rapid/press-release_IP-10-1624_en.htm?locale=en#footnote-2; Competition Policy Statement of VP Almunia on the Google antitrust investigation [21 May 2012] SPEECH 12/372, available at: http://europa.eu/rapid/press-release_SPEECH-12-372_en.htm.

[86] European Commission, 'Antitrust: Commission seeks feedback on commitments offered by Google to address competition concerns' [25 April 2013] available at: http://europa.eu/rapid/press-release_IP-13-371_en.htm.

[87] I. Graef [2016], Ibid., 41; A. Diker Vanberg, M.B. Ünver, Ibid.

[88] I. Graef [2016], Ibid., 41.

[89] A. Diker Vanberg, M.B. Ünver, Ibid.

[90] See: European Commission, 'Antitrust: Commission seeks feedback on commitments offered by Google to address competition concerns' [25 April 2013]; European Commission, 'Antitrust: Commission obtains from Google comparable display of specialised search rivals' [5 February 2014] available at: http://europa.eu/rapid/press-release_IP-14-116_en.htm.

[91] For Google's commitments, see: Case COMP/C-3/39.740 Foundem and others [3 April 2013] par. 27–31, http://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_8608_5.pdf. See also:

accept the remedies proposed by Google as sufficiently addressing the identified anticompetitive concerns[92]. This case also provides evidence that restrictions on data portability may qualify as an abuse of dominance under Article 102 TFEU and will be pursued by the European Commission[93].

3.3. Limitations of enforcing data portability through competition law

The possible enforcement of data portability under competition law differs substantially from the way of implementation of the right to data portability under GDPR. Under EU competition law, action can be taken against restriction on portability of any data, regardless of whether they are personal or non-personal and whether they are provided by a data subject, or a company, as long as they can qualify as an anticompetitive behaviour[94]. In this sense competition law has wider scope of application.

However, it should be noted that scope of potential competition enforcement of data portability under EU competition law is subject to certain limitations. First of all, Article 102 TFEU could be applied only if the restrictions on data portability were imposed by an undertaking that had a dominant position in a given market. Thus, under EU competition law it is not possible to pursue restrictions on data portability by an undertaking that is not dominant in a given relevant market. Secondly, such behaviour must qualify as an abuse of dominance within the meaning of Article 102. Therefore, competition law can facilitate data portability only with the specific purpose of remedying harm to competition[95]. It means that competition law cannot pursue refusals to data portability, if they do not have an adverse effect on competition. In particular, competition law should not be used to counteract infringements of other branches of law (in this case, data protection law), if a given practice does not reveal anticompetitive effect[96]. Thereby, an intervention under EU competition law would only be possible, if a lack of data portability results in competitive harm in the factual circumstances of the case[97].

Conclusions

J. Almunia, Speech: The Google Antitrust Case: What is at Stake?, [1 October 2013] available at: http://europa.eu/rapid/press-release_SPEECH-13-768_en.htm.

[92] The recent fine imposed on Google on March 20th 2019 also concerned abusive practices in online advertising, but the focus of the case was different. The Commission found that Google abused its dominant position in the market for online search advertising intermediation by imposing contractual restrictions on third party websites (publishers) that obliged them to obtain all or most of their online search advertisements from Google. See: European Commission, 'Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising' [20 March 2019] available at: http://europa.eu/rapid/press-release_IP-19-1770_en.htm.

[93] D. Geradin, M. Kuschewsky, Ibid., p. 11; A. Diker Vanberg, M.B. Ünver, Ibid.

[94] I. Graef, M. Husovec, N. Purtova, Ibid.,1359-1360.

[95] I. Graef, M. Husovec, N. Purtova, Ibid.,1359-1360, 1388-1389; O. Lynskey, 'Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability' [2017] European Law Review 42(6) 801-802.

[96] For a more elaborate discussion on this issue, see: I. Małobęcka-Szwast, 'Naruszenie prawa ochrony danych osobowych jako nadużycie pozycji dominującej? Postępowanie Bundeskartellamt przeciwko Facebookowi' [2018] iKAR 8(7) 139-153.

[97] I. Graef, M. Husovec, N. Purtova, Ibid.,1389. In contrast to data protection law, which protects personal data of data subjects, competition law aims at protecting consumer welfare by safeguarding the competitive process to benefit consumers, competitors, and the economy as a whole.

The right to data portability introduced in the GDPR, while forming part of the EU data protection regime, has also important implications for competition law. As it allows consumers to move their data from one service provider to the other, it lowers switching costs and reduces consumer lock-in, which is particularly discernible in case of online services. Thereby, it stimulates competition in the given markets and allows rival service providers to compete on the level-playing field with incumbents.

Nevertheless, the scope of the right to data portability under GDPR is limited. Art. 20 GDPR focuses only on the portability of personal data and from the perspective of the individual users (data subjects). Businesses or other entities that do not qualify as data subjects cannot invoke Art. 20 GDPR. However, restrictions on data portability may give rise to substantial switching costs and customer lock-in also in B2B relations, as can be evidenced by the Google case, and may have equally adverse effect on competition. Thereby, EU competition law, in particular Art. 102 TFEU, appears as a tool that can be used to enforce data portability and enable portability of data in cases falling outside scope of the GDPR[98]. In such a way the GDPR and EU competition law could complement each other and create a more efficient data portability mechanism that stimulates competition and enhances consumer welfare, however, bearing in mind limitations of both regimes[99].

Bibliography

Books

1. M. Armstrong, R. Porter (eds.), 'Handbook of Industrial Organization' Volume 3 (The Netherlands: Elsevier 2007).
2. E. Bielak-Jomaa, D. Lubasz (eds.), 'RODO. Ogólne rozporządzenie o ochronie danych. Komentarz' (Warszawa: Wolters Kluwer Polska 2017).
3. I. Graef, 'EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility' (Alphen aan den Rijn, The Netherlands: Kluwer Law International 2016).
4. K. Coates, 'Competition Law and Regulation of Technology Markets' (Oxford: Oxford University Press 2011).
5. C. Shapiro, H.R. Varian, 'Information Rules. A Strategic Guide to the Network Economy' (Boston: Harvard Business School Press 1999).
6. R. Whish, D. Bailey, 'Competition Law' (London: Oxford University Press 2012).

Articles

1. P. Akman, 'The Role of Exploitation in Abuse under Article 82 EC' [2009] 11 Cambridge Yearbook of European Legal Studies 165-188.
2. M. Bourreau, A. de Streel, I. Graef, 'Big Data and Competition Policy: Market power, personalised pricing and advertising' [2017] CERRE report, available

[98] V. Diker Vanberg, M.B. Ünver, Ibid.; S. Lucchini, J. Moscianese, I. de Angelis, F. Di Benedetto, Ibid., 563.
[99] S. Lucchini, J. Moscianese, I. de Angelis, F. Di Benedetto, Ibid., 563, 567.

at:
https://www.cerre.eu/sites/cerre/files/170216_CERRE_CompData_FinalReport.pdf.

3. A. Diker Vanberg, M.B. Ünver, ‘The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?’ [2017] 8(1) European Journal of Law and Technology available at: http://ejlt.org/article/view/546/726.

4. J. Drexl, ‘Designing Competitive Markets for Industrial Data - Between Propertisation and Access’ [2017] 8(4) JIPITEC 257-292.

5. A.S. Edlin, R.G. Harris, ‘The Role of Switching Costs in Antitrust Analysis: A Comparison of Microsoft and Google’ [2013] 15(2) Yale Journal of Law and Technology 169-213.

6. D. S. Evans, R. Schmalensee, ‘A Guide to the Antitrust Economics of Networks’ [1996] 10 Antitrust 36-40.

7. D. S. Evans, ‘The Antitrust Economics of Multi-Sided Platform Markets’ [2003] 20(2) Yale Journal on Regulation 325-381.

8. D. Geradin, M. Kuschewsky, ‘Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue’ [2013] available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2216088.

9. I. Graef, ‘Data Portability at the Crossroads of Data Protection and Competition Policy’, Big Data e Concorrenza [9 November 2016] LUISS Guido Carli, available at: http://www.agcm.it/component/joomdoc/eventi/convegni/20161109_07.pdf/download.html.

10. I. Graef, J. Verschakele, P. Valcke, ‘Putting the right to data portability into a competition law perspective’ [2013] available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2416537.

11. I. Graef, M. Husovec, N. Purtova, ‘Data Portability and Data Control: Lessons for an Emerging Concept in EU Law’ [2018] 19(6) German Law Journal 1359-1398.

12. I. Graef, Y. Wahyuningtyas, P. Valcke, ‘Assessing Data Access Issues in Online Platforms’ [2015] 39(5) Telecommunications Policy 375-389.

13. I. Graef, ‘Mandating portability and interoperability in online social networks: Regulatory and competition law issues in the European Union’ [2015] 39(6) Telecommunications Policy 502-514.

14. J. Haucap, U. Heimeshoff, ’Google, Facebook, Amazon, eBay: Is the internet driving competition or market monopolization?’ [2014] 11(1) International Economics and Economic Policy 49-61.

15. P. D. Klemperer, ‘Markets with consumer switching costs’ [1987] 102(2) Quarterly Journal of Economics 375–394.

16. A. Lambrecht, C. E. Tucker, ‘Can Big Data Protect a Firm from Competition?’ [2015] available at: http://ec.europa.eu/information_society/newsroom/image/document/2016-6/computer_and_communications_industry_association_-_can_big_data_protect_a_firm_from_competition_13846.pdf.

17. S. Lucchini, J. Moscianese, I. de Angelis, F. Di Benedetto, ‘Online Digital Services And Competition Law: Why Competition Authorities Should be More Concerned About Portability Rather than About Privacy’ [2018] 9(9) Journal of European Competition Law & Practice 563–568.

18. O. Lynskey, ‘Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability’ [2017] 42(6) European Law Review 793-814.

19. P. Moura, ‘Data Portability Series: Capitalising on the Market for Interoperability’ [16 April 2014] available at: https://blogs.lse.ac.uk/mediapolicyproject/2014/04/16/data-portability-series-capitalising-on-the-market-for-interoperability/.
20. R.C. Picker, ‘Competition and Privacy in Web 2.0 and the Cloud’ [2008] 103 Northwestern University Law Review Colloquy 1-12.
21. P. Swire, Y. Lagos, ‘Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique’ [2013] Maryland Law Review 72(2) 335-380.
22. C.S. Yoo, ‘When Antitrust Met Facebook’ [2012] 19(5) George Mason Law Review 1147-1162.
23. G. Zanfir, ‘The Right to Data Portability in the Context of the EU Data Protection Reform’ [2012] 2 (3) International Data Privacy Law 149-162.

Legislation

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.
2. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) [1995] OJ L 281/31.
3. Treaty on the Functioning of the European Union (Consolidated version) [2012] OJ C 326/47.
4. Council Regulation 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty [2002] OJ L1/1.

Other sources

1. J. Almunia, Speech: Competition and personal data protection, Privacy Platform event: Competition and Privacy in Markets of Data [26 November 2012], available at: http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm.
2. Art. 29 Working Party, Guidelines on the right to data portability, adopted on 13 December 2016 as last revised and adopted on 5 April 2017, WP 242 rev.01.
3. Commission Staff Working Paper - Impact Assessment accompanying the General Data Protection Regulation and the Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, SEC(2012) 72 final [25 January 2012].
4. ICO, GDPR Guide, available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/.
5. M. Vestager, Speech: Competition in a big data world [17 January 2016] available at: https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/competition-big-data-world_en.

TO BE OR NOT TO BE… AN AUTHOR? SOME REMARKS ON COPYRIGHTABILITY OF ARTIFICIAL INTELLIGENCE'S WORK

Adrianna Michałowicz[1]

Abstract

Recent years have brought huge changes in the development of artificial intelligence. Using robots to perform repetitive and simple tasks is not surprising nowadays, but using AI to create artistic work still raises many questions and controversies. According to the EU copyright legislation and case law, the term authorship is commonly referred to human activities. Copyright work must be original in the sense that it should reflect the author's own intellectual creation and his personal touch. Our law accentuates author's strong position, as well as the need to protect his moral rights related to the sphere of his inner experiences. Works created by AI, even if they are considered as original and unique, do not fulfill these requirements, since there is no emotional link between the machine and its copyright work. However, does it mean that they cannot be granted any protection? I believe this issue should not be underestimated, because a general and wide use of AI is just a matter of time and if we do not settle basic legal solutions now, the problem will only arise in the future.

The following article will address the potential authorship rights and copyright protection that could be afforded to computer-generated works. The presented analysis will be based mainly on the EU copyright regulations and case law, however in order to make the evaluation more clear and complex some remarks will concern also copyright law in common-law countries, in particular U.K. and U.S.

Keywords: artificial intelligence, copyright works, computer-generated works, copyright protection, intellectual property.

Introduction

Artificial intelligence (AI) has recently become a hot topic. Self-driving cars, self-learning algorithms that assess and decide on our creditworthiness, recommendation systems on online platforms, personalized marketing, artificial assistants setting up a meeting with a business client are just a few examples of modern technologies being already used or to be used in the near future. The usage of AI is visible in almost every part of our lives and consequently it affects nearly every field of law: from civil, commercial, criminal and financial law to data protection and intellectual property law. However, a dynamic and often unpredictable development of modern technologies, including AI, challenges the current legal framework, making it outdated and maladjusted to the newest inventions.

Intellectual property law is one of those disciplines that lack proper regulations

[1] Advocate trainee at the Łódź Bar Association and Ph.D. student at the Faculty of Law and Administration, University of Łódź. Specializes in data protection law and intellectual property law.

regarding the employment of AI. A lot of questions may be raised in relation to the fundamental issues of copyright law, e.g. the scope of definition of "copyright work" and "author". Thus this article focuses on matters concerning copyrightability of AI works and refers to one of the basic problems, which is an authorship of AI works.

1. Is an authorship of copyright work reserved only for humans?

Before discussing the main subject of the article, some remarks have to be made concerning the notion of "copyright work". This term has no legal definition in the European Union (EU) copyright law, since the EU legislator left Member States with a discretionary power to regulate this concept in accordance with already developed legal practice in every state. Along with the development of the internal market, the need for a unitary EU-wide applicable definition had been increasing. So far no legally binding definition of "copyright work" has been introduced to the EU copyright law, but the Court of Justice (the Court) managed to establish in its case law basic rationales to be taken into account while assessing whether a work is eligible for copyright protection.

In Infopaq Case[2] the Court stated that, based on the general scheme of the Berne Convention, "the protection of certain subject-matters as artistic or literary works presupposes that they are intellectual creations"[3], which means that they must be original[4]. This conclusion the Court derived from Articles 1(3) of Directive 91/250[5], 3(1) of Directive 96/9[6] and 6 of Directive 2006/116[7], setting up a prerequisite of originality for accordingly computer programs, databases or photographs. The Court in its subsequent judgments has reiterated the above-mentioned approach, giving even more guidelines on interpretation of original copyright work, e.g. by explaining that criterion of originality is satisfied when an author is able to express his creative abilities in the production of the work by making free and creative choices in order to stamp his 'personal touch'[8]. In fact, the Court has harmonized the concept of a copyright work, focusing rather on a model accepted in the continental law, which stresses an individual character of a copyright work[9]. At the same time the Court rejected the common law model, which places emphasis on a high level of author's work and skills. In common law countries the criterion of originality is usually defined

[2] Judgment of the Court of 16 July 2009 in Case C-5/08 Infopaq International, ECLI:EU:C:2009:465 (hereinafter: "Infopaq Case").
[3] Infopaq Case, paragraph 34.
[4] Infopaq Case, paragraph 37.
[5] Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, OJ L 122, 17.5.1991 – in force at that time; replaced by: directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, OJ L 111, 5.5.2009.
[6] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27.3.1996.
[7] Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights; OJ L 372, 27.12.2006.
[8] Judgment of the Court of 1 December 2011 in Case C-145/10 Painer, ECLI:EU:C:2011:798, paragraph 89, 92; judgment of the Court of 1 March 2012 In Case C-604/10 Football Dataco and Others, ECLI:EU:C:2012:115, paragraph 38.
[9] E. Laskowska, Przedmiot prawa autorskiego – utwór a pojęcie oryginalności w prawie UE – wprowadzenie i wyrok TS z 16.07.2009 r. w sprawie C-5/08 Infopaq International A/S przeciwko Danske Dagblades Forening, Europejski Przegląd Sądowy 2017, No. 1, p. 47.

by tree elements which are skill, judgment and labor[10]. It is rather not an artistic creativity or novelty that is protected, but the potential economic value of the author's investment, skill and labor deployed in the making of a property which copyright protects[11].

Developing the scope of conditions that must be met for a work to be protected under the copyright law directly affects the scope of the definition of the author. Can an original and intellectually sophisticated work be produced by a non-human creator? The answer is ambiguous and provokes an interesting debate on copyrightability of non-human works, particularly works created by artificially intelligent machines.

The problem of granting copyrights to a machine-produced work is not a brand new problem, since the first doubts arose already in 1884, when a photographic portrait of Oscar Wilde's was created. In case Burrow-Giles Lithographic Co. v. Sarony the U.S. Supreme Court decided to extend copyright protection to photography. According to the court, photographer Napoleon Sarony used his camera as a tool to capture the image of Oscar Wilde, and therefore the camera only aided the author in creating an original work of art[12]. Another inspiring discussion concerned copyrightability of animals' works. In Naruto – Slater case the plaintiffs, the People for the Ethical Treatment of Animals ("PETA") and Antje Engelhardt – the reserve where the macaque Naruto lived, searched for protection against violating Narutos' copyrights, since the monkey took a selfie using a photograph's David Slater camera. During the proceedings they underlined that Naruto took a photo by "'independent, autonomous action' in examining and manipulating Slater's unattended camera and 'purposely pushing' the shutter release multiple times, 'understanding the cause-and-effect relationship"[13]. Does it mean that the macaque created an original photo, which may be protected under the copyright law? According to the U.S. district court Naruto cannot be considered as an author of photos within the meaning of the Copyright Act[14]. The judgment refers to the practice of the US Copyright Office, which states that an original work of authorship can be registered for copyright provided that the work "owes its origin to a human being. Materials produced solely by nature, by plants, or by animals are not copyrightable"[15].

The recent popularization of AI shows that a human is no longer the only source of creative works. Computer programs are also capable of creating original or innovative works. Computer-generated works are being more and more appreciated for their artistic values, which is perfectly reflected in competitions organized specifically for machines, e.g. Robot Art Competition organized since 2016[16]. Another example of a true human-like piece of art is so called Next Rembrandt - the painting created by a machine. The program analyzed and „learned" the style of the famous painter, and then produced a portrait - a new, independent, and original work of art which mirrors Rembrandt's style flawlessly[17].

A work produced by a computer program has been even exhibited at New York

[10] D. Liu, Forget the monkey copyright nonsense for goodness sake, dude!, European Intellectual Property Review 2018, p. 63.
[11] A. Rahmatian, Originality in UK Copyright Law: The Old "Skill and Labour" Doctrine Under Pressure, IIC - International Review of Intellectual Property and Competition Law 2013, Vol. 44, Issue 1, pp 4–34.
[12] Cf. Burrow-Giles Lithographic Co. v. Sarony, 111 U.S. 53 (1884).
[13] Naruto v. Slater, 2016 U.S. Dist. LEXIS 11041 (N.D. Cal. 2016). See: G. Huson, I, Copyright, 35 Santa Clara High Tech. L. J. 54 (2018), p. 71.
[14] Naruto,2016 U.S. Dist. LEXIS 11041 at 4.
[15] U.S. COPYRIGHT OFFICE, Compendium of U.S. Copyright Office Practices II § 202.02(b) (1984).
[16] See: https://robotart.org (access: 16.06.2019).
[17] See: https://www.nextrembrandt.com (access: 16.06.2019).

Christie's, where it was sold for $432,500. The work - Portrait of Edmond Belamy, was created by Generative Adversarial Network, composed of two algorithms: Generator and Discriminator. The Generator made images based on the data set containing 15,000 portraits painted between the 14th and the 20th century. Then the Discriminator's task was to spot the difference between a human-made image and one created by the Generator; when the Discriminator got mislead and thought that the newly created images are real-life portraits, the result was obtained[18]. One more absolutely compelling example of a creative computer program is The Painting Fool[19]. The program was developed by Simon Colton in order „to see whether software can be accepted as creative in its own right"[20]. The robot painted the portraits of guests visiting the exhibition „You Can't Know my Mind"[21]. Interestingly, its painting style was affected by its current mood, which depended on what kind of article the robot had read that day in newspaper - a positive or a negative one. The robot could even refuse to paint if it was in a very bad mood. What is more, it was able to make a self-assessment and correct the final outcome if it was necessary.

Increasing use of modern technologies based on AI raises two basic questions: is it possible to grant a status of copyrightable work for computer-generated works, and if so - who should be eventually considered as an author of such works? Neither in the EU law, nor in common law countries copyrightability of works produced by AI is regulated. What is more, the criteria developed so far through practice and case law relate to intellectual creativity of an author, thus are widely interpreted as referring only to human authors[22]. The work would be protected with copyrights if it fulfills the condition of originality and human intellectual creation. Does it mean that computer-generated works cannot be protected at all? To answer this question it is necessary to distinguish two types of usage of AI-based programs: when an AI is used only as a tool to create an artistic work and when it creates independently from a human.

1. AI used as a tool vs. creative AI

Programs based on AI, and consequently works produced by them, are often divided into two main categories. The first category includes programs built on AI, for which human action is essential. Works of such programs would not be generated without the direct guidance, assistance or input of human beings[23]. These include for e.g. software being programmed to give a specific outcome. To put it simply, these programs take an input, apply a prescribed formula or rule to the input and compute an output[24]. In such programs AI is used as a tool to achieve a determined goal or a predicted outcome. Sometimes the result might seem random or might be unknown for the programmer, however it is still a programmed output, e.g. a program that generates passwords[25]. More sophisticated programs are able to answer users' questions by consulting and checking external sources,

[18] See: https://www.christies.com/features/A-collaboration-between-two-artists-one-human-one-a-machine-9332-1.aspx (access: 16.06.2019).
[19] See: http://www.thepaintingfool.com/index.html (access: 19.06.2019).
[20] K. Shubber, Artificial artists: when computers become creative, Wired 7 August 2013, available at: https://www.wired.co.uk/article/can-computers-be-creative (access: 19.06.2019).
[21] See: http://www.thepaintingfool.com/galleries/you_cant_know_my_mind/index.html (access: 19.06.2019).
[22] J. Dickenson, A. Morgan, B. Clark, Creative machines: ownership of copyright in content created by artificial intelligence applications, European Intellectual Property Review 2017, p. 459.
[23] K. Hristov, Artificial Intelligence and the Copyright Dilemma, 57 IDEA 431 (2017), p. 435.
[24] J. Wagner, Rise of the Artificial Intelligence Author, 75 Advocate (Vancouver) 527 (2017), p. 528.
[25] J. Wagner, Rise of the Artificial…, p. 529.

e.g. an application that responds to queries concerning the weather by verifying the weather forecast and user's geolocation[26]. This category includes also programs that create paintings or other similar artistic works - firstly a programmer or a user defines the parameters of the future outcome, e.g. by selecting colors, type of brushes, texture, painting style etc., then the program generates a final result. Even if a programmer or a user cannot exactly predict the outcome, he has directly contributed to its creation and has some expectations as to how it may look like, because he had inserted some of his ideas and requirements into the AI algorithm that created the painting[27].

Taking into account the above-mentioned, the authorship of such works belongs to humans - a programmer or a user, depending on whose instructions the program realized. In common law countries this kind of programs are considered incapable of exercising either skill or judgment, since they do not develop over time, but only follow pre-programmed rules[28]. In the EU countries, except for UK, the assessment would be the same as the computer-generated work created with human assistance reflects intellectual personality of its creator.

The second category is represented by computer programs and works created by AI acting autonomously. Such programs employ so-called machine learning - a method to achieve AI. Machine learning gives computers an ability to „learn" from large volumes of data without being explicitly programmed[29]. Instead of simply following instructions, machine learning program is capable of creating new mathematical algorithms, as well as making predictions and recommendations based on patterns detected in training data sets, so that machine's performance can improve progressively[30]. As a result, machine learning programs can change or adapt their programming based on new data and then create something unexpected or unintended by the original programmer[31]. This way a program might start developing its own creative capacities and produce an output not only independently from its programmer, but also having an artistic value. The point is that a programmer has no influence on program's work and is not able to anticipate the final result of this work. The examples of such computers programs were mentioned in part 1 of this article, where AI-based robots receive only certain guidelines from a programmer and then operate on their own, coming up with unforeseeable outcome.

The fundamental question is whether the current framework of intellectual property law allows protecting works created by autonomous computer programs. In case of a positive answer, another question arises - who should be granted copyrights? The following part of this article presents possible solutions regarding both continental and common law regulations.

3. Creative AI – how to tackle the problem?

As it was already explained, the concept of copyright work and authorship in the EU law has been harmonized by the Court of Justice. Given the requirements established

[26] J. Wagner, Rise of the Artificial…, p. 529.
[27] K. Hristov, Artificial Intelligence…, p. 435.
[28] J. Wagner, Rise of the Artificial…, p. 529.
[29] Centre for Information Policy Leadership Hunton Andrews Kurth, First Report: Artificial Intelligence and Data Protection in Tension, 10 October 2018, p. 5.
[30] Centre for Information Policy Leadership Hunton Andrews Kurth, First Report: Artificial…, p. 5.
[31] J. Wagner, Rise of the Artificial…, p. 530.

mainly in the Infopaq Case, the work must be author's own intellectual creation and should reflect his „personal touch". It means that some form of a human authorship is necessary, and therefore no copyright protection should be granted for computer-generated works created without human impact[32]. As the preconditions of a copyright work are not satisfied, theoretically the protection should be denied. However it could be argued that works produced by computer programs somehow reflect the intellectual creativity of their creators, because it was a programmer that pre-scribed the rules and gave an incentive to create a work. Assuming that a test for author's intellectual creation could be stretched to cover works created with AI assistance, it is still difficult to apply these rules to machine learning programs, where the process of creation was commenced by a human author, but completed by AI acting autonomously and independently from a human[33].

In common law countries regulations regarding copyrightability of AI works are different from those applied in the EU. In the UK[34] a relatively low threshold for protection exists, allowing the protection of machine creation. It stems from the provision of the British Copyright, Design and Patents Act 1988, which grants protection for computer-generated works where no human authorship can be found[35]. In such circumstances the copyright holder would be the person who has undertaken the arrangements necessary for the creation of the work. In most cases it would be the person who made a financial investment in the computer and the program that produced a copyrightable work. The doubts arise since the said provision was drafted when the level of AI development and its recognition was low, thus there is no legal certainty now that this provision should be taken into account by courts. Moreover, the mentioned provision does not prejudge a copyrightability of AI-generated works, because it regulates only the authorship and does not set up any requirements for protection. For this reason the traditional test for originality must be fulfilled. Assessing whether a work expresses author's skill, labor and judgment might be problematic as well, since no rules have been established on how to evaluate the level of originality of works created not directly by a human[36]. Envisaged solution is that courts may focus on skill, labor and judgment of a person who made necessary arrangements for the process of creation, mainly in order to preserve the consistency of the provisions and to interpret them in accordance with the purpose for which they were introduced[37]. However type of AI used during the process should not be negligible, because in the case of more sophisticated AI algorithms, e.g. deep machine learning, it may not be obvious that a person who created the algorithm undertook the necessary arrangements for the creation of the final work[38].

Different approach is applied in US, since AI-generated works fall outside the scope of protection. This is derived directly from the practice of the U.S. Copyright Office, which denies the possibility to „register works produced by a machine or mere mechanical process that operates randomly or automatically without any creative input or intervention from a human author"[39]. It means that unless a computer-generated works could be attributed to a human author, these works would not be copyrightable[40]. In the absence of case law, the

[32] M. de Cock Buning, Autonomous Intelligent Systems as Creative Agents under the EU Framework for Intellectual Property, 7 Eur. J. Risk Reg. 310, p. 314.
[33] J. Dickenson, A. Morgan, B. Clark, Creative machines: ownership…, p. 459.
[34] However it has to be taken into account that as long as the UK is a Member State of the Union all EU regulations and case law regarding copyrights are applicable.
[35] Copyright, Designs and Patents Act 1988, Chapter 48, § 9.3.
[36] J. Dickenson, A. Morgan, B. Clark, Creative machines: ownership…, p. 459.
[37] J. Dickenson, A. Morgan, B. Clark, Creative machines: ownership…, p. 460.
[38] J. Dickenson, A. Morgan, B. Clark, Creative machines: ownership…, p. 460.
[39] U.S. COPYRIGHT OFFICE, Compendium of U.S. Copyright Office Practices § 313.2.
[40] K. Hristov, Artificial Intelligence…, p. 437.

most probable solution is releasing AI-generated works all into the public domain[41]. No matter how creative and valuable an AI-generated work might be, as long as there is no other legal regulation governing copyrights in such a case, that work should naturally revert to the „collective wealth", enrich the human world and culture, and thus reside in the public domain[42].

Based on the above remarks, granting copyrights for AI-generated works is rather a theoretical concept, because the current legal framework does not refer to this subject directly. Yet this solution is not definitely excluded, as the requirements for copyright protection were establish mainly through courts' case law or practice. At the same time due to the rapid development of AI, the more and more sophisticated and autonomously creative programs are yet to be revealed, resulting in an increasing number of works deprived of any form of copyright protection[43]. Allowing computer-generated works to fall directly into the public domain is a considerable disadvantage, because it might discourage AI developers from further improving and expanding the capabilities of AI. It gives no incentive to invest time and money in developing AI-based machines, since there is no perspective to enjoy copyright protection or other financial benefits associated with it[44]. As a result it may be counterproductive to development of AI and decrease the need for creativity. Because of these potential shortcomings other concepts have been formulated in order to find a solution more favorable to AI creators. These solutions are mainly based on current regulatory gaps and grey areas, which make applicable law open to different interpretations.

4. Assigning copyrights to humans

To tackle the problem of depriving any form of copyrights for AI-generated works, the most appealing and realistic concept is to assign copyrights to humans, for eg. AI developers, owners or users. This concept is based on the fact that always some kind of a human involvement originally stands behind the created work and gives AI-based programs an ability to create. A human develops the program firstly, lays dawn rules for that program, and establishes the requirements. Even if AI learns itself and creates something on its own, it's always a human that is the origin of that work. It would not be done without a human previous engagement in the process. In other words AI creates something because of a human that created a computer program and allowed AI to create. No matter how this concept is acceptable and logical, it is difficult to be reconciled with the requirement of originality, both within the meaning in the EU law and common law. As is was explained works generated by AI programs lack intellectual creativity; additionally it is impossible to accept that AI-based programs perform their own skill and judgment, but rather imitate skill and judgment of the programmer, thus the traditional test for originality is not fulfilled[45]. This concept poses also more general question whether AI is at all creative, if it is incapable of understanding the output it creates and assigning the values and judgment to the symbols it processes?[46] Despite the objections, it is beyond any doubt that a programmer or a person that commission a programmer is the party that owns a commercial interest in exploiting the

[41] K. Hristov, Artificial Intelligence…, p. 437.
[42] A. H. Khoury, Intellectual Property Rights for Hubots: On the Legal Implications of Human-like Robots as Innovators and Creators, 35 Cardozo Arts & Ent. L.J. 2017, p. 636.
[43] K. Hristov, Artificial Intelligence…, p. 438.
[44] K. Hristov, Artificial Intelligence…, p. 438.
[45] J. Wagner, Rise of the Artificial…, p. 531.
[46] J. Wagner, Rise of the Artificial…, p. 531.

work created by AI-based programs. Thus another two competing theories have been elaborated with regard to the extend to which a human could enjoy copyrights of computer-generated works. Although these theories have been developed on the basis of copyright rules applied in common law countries, recognizing them may contribute to a fruitful discussion concerning the approach that should be adopted within the EU.

The first theory assumes that a human (an AI programmer, owner or user) could be considered as a co-author with an AI-based program, since he introduces the skill and judgment into the initial programming of the AI program[47]. Even if he contributed to the final output to a small extend, he is the person who gave an incentive to create, and - as it is regulated in the UK law - undertook necessary arrangements in the process of creating of the work. Another theory is based on American made for hire doctrine, according to which copyrights of works created by an employee during the scope of his or her employment belong to an employer[48]. For the purpose of applying made for hire doctrine for AI-generated works, some fundamental modifications would be necessary, especially regarding the notion „employee" in order to encompass an AI within its meaning. Then, an AI-based program could be considered as an employee as its generated services are employed by its programmer or owner[49]. It does not eliminate however other drawbacks, which concern i.e. working under employer's control, possibility of an employer to give instructions and determine instrumentalities and tools to work, receiving a remuneration etc. These factors would not be applicable when an AI creates works[50]. Furthermore, according to certain opinions, employing made for hire doctrine would be even tricky, because an AI, in theory, may never stop creating as it needs no incentive to do so. For this reason an AI programmer or owner would become dependent on AI and loose his personal need to create and develop new capabilities of an AI programs[51].

To sum it up, the concept of assigning copyright to humans cannot be directly derived from the current framework of the EU copyright law. In order to apply this concept either the EU legislator would have to adopt special regulations regarding this issue or the Court of Justice would have to modify its case law and accept a wide interpretation of a copyright work and authorship.

5. AI as the author

Some experts argue that the most innovative approach is to assign copyrights to non-humans[52]. This concept has been created in the light of certain practices of the U.S. Copyright Office and guidelines released by different legal authorities. Proponents of this theory underline that when the Copyright Office was first addressed the issue on copyrightability of computer-generated works, it suggested that it is necessary to asses whether a computer was merely an assisting instrument or whether a computer conceived and executed the traditional elements of authorship[53]. This opened up and popularized a

[47] J. Wagner, Rise of the Artificial…, p. 532.
[48] S. Yanisky-Ravid, Generating Rembrandt: Artificial Intelligence, Copyright, and Accountability in the 3A Era: The Human-like Authors Are Already Here: A New Model, 2017 Mich. St. L. Rev., p. 707.
[49] K. Hristov, Artificial Intelligence…, p. 447.
[50] G. Huson, I, Copyright…, p. 74.
[51] G. Huson, I, Copyright.… p. 74.
[52] R. Abbott, I Think, Therefore I Invent: Creative Computers and the Future of Patent Law, 57 B.C. L. Rev. 1079 (2016), p. 1098.
[53] See U.S. COPYRIGHT OFFICE, SIXTY-EIGHTH ANN. REP. REG. COPYRIGHTS 4-5 (1966).

discussion on the subject, and finally reached to the point when the U.S. Congress's Office of Technology Assessment issued in 1986 a report, stating that computers are more than just inert tools of creation and in many cases should be considered as at least co-creators[54]. Treating AI programs as the authors of generated works would be also consistent with the rationales for copyright protection, since it would encourage innovation; moreover partially it would reward human creative activity upstream from the computer's inventive act[55].

The above-mention concept is as controversial as theoretical at least for now. It is completely inconsistent with the EU copyright regulations and the Court's case law, which is why it would be rather rejected by the EU authorities. This concept challenges the whole legal system, because non-humans so far are not considered as natural persons, they do not have legal personality and they cannot be held legally responsible for their actions. In order to apply this theory it would be inevitable to define in the first place the legal status of non-humans by for e.g. changing basic rules regarding legal personality. Otherwise, granting copyrights to non-humans raises more questions than answers and would only increase legal uncertainty[56]. What is more, assigning copyrights to computers is also contrary to the most fundamental purpose of a whole system of copyright protection, since these types of rights were introduced and developed to protect human creativity and innovation. Machines do not need any incentive to work and produce creative and original outcomes. Besides, other practical issues would have to be addressed, like whether there might be an adequate remedy for infringing on AI's work or who should be entitled to bring an infringement action on behalf of AI program?[57] It cannot be ruled out that a right to protect AI's interest would be granted to the person who created it or contributed to the process of creation of a copyrightable work. However, it does not give an answer to the question whether at all AI needs any kind of financial compensation for violating its' rights[58].

Conclusions

The current copyright law, considered in general and including both the EU law and common law, is not suitable for developments regarding AI. Applicable EU regulations do not refer to AI and they cannot be adopted or interpreted in such a way that will help us to solve a problem with works created by AI. There are grey areas, particularly in the territory of more sophisticated AI. Also legal practices applied in the US or in UK do not give explicit grounds for protection of AI-generated works. Thus there is a need either to change the law by introducing a brand new regulations or wait until the courts or other legal authorities change their practices and issue a clear guideline on how to tackle the problem.

In my opinion the most appropriate solution is to assign copyrights to humans, in particular to program developers or owners, since their contribution to the process of inventing creative AI is undeniable. Such a solution would be at the same time consistent with the nature of intellectual property rights, which were developed to protect humans' intellectual efforts, and would incentivize creativity by encouraging AI program developers

[54] See U.S. CONGRESS, OFFICE OF TECH. ASSESSMENT, INTELLECTUAL PROPERTY RIGHTS IN AN AGE OF ELECTRONICS AND INFORMATION 70-73 (1986).
[55] R. Abbott, I Think, Therefore I Invent…, p. 1104.
[56] K. Hristov, Artificial Intelligence…, p. 441.
[57] G. Huson, I, Copyright.… p. 76.
[58] Y. J. Liebesman, The Wisdom of Legislating for Anticipated Technological Advancements, 10 J. MARSHALL REV. INTELL. PROP. L. 153, p. 175.

and owners to create more and more sophisticated machines and algorithms. It will protect as well works of AI programs, which are often not less original than human works, from falling into a public domain.

Bibliography

1. R. Abbott, *I Think, Therefore I Invent: Creative Computers and the Future of Patent Law*, 57 B.C. L. Rev. 1079, 2016.
2. Centre for Information Policy Leadership Hunton Andrews Kurth, *First Report: Artificial Intelligence and Data Protection in Tension*, 10 October 2018.
3. M. de Cock Buning, *Autonomous Intelligent Systems as Creative Agents under the EU Framework for Intellectual Property*, 7 Eur. J. Risk Reg. 310.
4. J. Dickenson, A. Morgan, B. Clark, *Creative machines: ownership of copyright in content created by artificial intelligence applications*, European Intellectual Property Review 2017.
5. K. Hristov, *Artificial Intelligence and the Copyright Dilemma*, 57 IDEA 431, 2017.
6. G. Huson, *I, Copyright*, 35 Santa Clara High Tech. L. J. 54, 2018.
7. A. H. Khoury, *Intellectual Property Rights for Hubots: On the Legal Implications of Human-like Robots as Innovators and Creators*, 35 Cardozo Arts & Ent. L.J. 2017.
8. E. Laskowska, *Przedmiot prawa autorskiego – utwór a pojęcie oryginalności w prawie UE – wprowadzenie i wyrok TS z 16.07.2009 r. w sprawie C-5/08 Infopaq International A/S przeciwko Danske Dagblades Forening*, Europejski Przegląd Sądowy 2017, No. 1.
9. Y. J. Liebesman, *The Wisdom of Legislating for Anticipated Technological Advancements*, 10 J. MARSHALL REV. INTELL. PROP. L. 153.
10. D. Liu, *Forget the monkey copyright nonsense for goodness sake, dude!*, European Intellectual Property Review 2018.
11. A. Rahmatian, *Originality in UK Copyright Law: The Old "Skill and Labour" Doctrine Under Pressure*, IIC - International Review of Intellectual Property and Competition Law 2013, Vol. 44, Issue 1.
12. K. Shubber, *Artificial artists: when computers become creative*, Wired **7** August 2013, available at: https://www.wired.co.uk/article/can-computers-be-creative (access: 19.06.2019).
13. J. Wagner, *Rise of the Artificial Intelligence Author*, 75 Advocate (Vancouver) 527, 2017.
14. S. Yanisky-Ravid, *Generating Rembrandt: Artificial Intelligence, Copyright, and Accountability in the 3A Era: The Human-like Authors Are Already Here: A New Model*, 2017 Mich. St. L. Rev.

Judgments:

1. Judgment of the Court of 16 July 2009 in Case C□5/08 Infopaq International, ECLI:EU:C:2009:465.
2. Judgment of the Court of 1 December 2011 in Case C□145/10 Painer, ECLI:EU:C:2011:798.

3. Judgment of the Court of 1 March 2012 In Case C‑604/10 Football Dataco and Others, ECLI:EU:C:2012:115.
4. Cf. Burrow-Giles Lithographic Co. v. Sarony, 111 U.S. 53 (1884).
5. Naruto v. Slater, 2016 U.S. Dist. LEXIS 11041 (N.D. Cal. 2016).

Other:

1. Copyright, Designs and Patents Act 1988.
2. Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, OJ L 122, 17.5.1991.
3. Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, OJ L 111, 5.5.2009.
4. Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27.3.1996.
5. Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights; OJ L 372, 27.12.2006.
6. U.S. COPYRIGHT OFFICE, Compendium of U.S. Copyright Office Practices II (1984).
7. U.S. COPYRIGHT OFFICE, SIXTY-EIGHTH ANN. REP. REG. COPYRIGHTS 4-5 (1966).
8. U.S. CONGRESS, OFFICE OF TECH. ASSESSMENT, INTELLECTUAL PROPERTY RIGHTS IN AN AGE OF ELECTRONICS AND INFORMATION 70-73 (1986).
9. https://robotart.org (access: 16.06.2019).
10. https://www.nextrembrandt.com (access: 16.06.2019).
11. https://www.christies.com/features/A-collaboration-between-two-artists-one-human-one-a-machine-9332-1.aspx (access: 16.06.2019).
12. http://www.thepaintingfool.com/index.html (access: 19.06.2019).
13. http://www.thepaintingfool.com/galleries/you_cant_know_my_mind/index.html (access: 19.06.2019).

MARKETABILITY OF DATA IN CONTRACT LAW

Benjamin Mörschardt[1]

Abstract

In times of Big Data, the issue of data protection is gaining more importance than ever before. But at the same time, trading in data becomes more popular that European legislators can no longer ignore the need of new regulations for data business[2]. This paper will present new European legislative proposals including data as new legal objects. Therefore, digital data on the one hand and personal data on the other hand will be highlighted. Typecasting contractual agreements including these legal objects will be subject of discussion subsequent. Hereafter, it will be analysed which role data protection law plays for these new regulations. Therefore, it will be questioned how to deal with a consent in processing personal data and its revocability.

Afterall, a specific problem of this legal transactions will be presented, demonstrating a legal loophole, whereby a risk of abuse results. Finally, a conclusion present a possible solution how to deal with this legal loophole.

Keywords: Data; Digital Content Directive; General Data Protection Regulation.

Introduction: The requirement of a legislative reform in contract law

Initially contract law was designed to regulate transactions of physical objects[3]. As long as digital content like movies or music has been used in physical form like disk records, video tapes or DVD, legislators did not need to reform private and contract law. In recent years increasing use of downloading and streaming has caused a lot of legal issues: Is a major reform of contract law necessary? The European Commission submitted a proposal for an EU directive on certain aspects concerning contracts for the supply of digital content[4] within its Digital Single Market Strategy[5] for business-to-consumer. The proposal presents new legal regulation on liability of the supplier of digital content. But in fact, defects are nothing new. Actually the European Commission itself intended to reform the whole

[1] PhD Student in Law, Goethe-University Frankfurt with a dissertation on "Contracts of digital content and durable media"

[2] M. Schmidt-Kessel, A. Grimm 'Unentgeltlich oder entgeltlich? – Der vertragliche Austausch von digitalen Inhalten gegen personenbezogene Daten' [2017] ZfPW 2017 84

[3] For German contract law see J. Thiessen in: M. Schmoeckel, J. Rückert, R. Zimmermann (ed.), 'Historisch-kritischer Kommentar zum BGB' (Tübingen: Mohr Siebeck 2013), Annex to sections 433-453

[4] European Commission Proposal for a directive (COD) 2015/0287 concerning on certain aspects concerning contracts for the supply of digital content [2015] (DCD-COM)

[5] 'A Digital Single Market for Europe: Commission sets out 16 initiatives to make it happen' [May 2015] European Commission Press Release http://europa.eu/rapid/press-release_IP-15-4919_en.htm

purchase law making a proposal for a Common European Sales Law[6]. So, the main question of this analysis – using the example of German contract law – should be: Do we really need an exclusive reform of liability regulation in cases of supplying digital content or digital services to protect consumers from detriments? Or, in contrast to physical objects: Do we need regulations for transactions of data, which are not protected by intellectual property rights but by the contract – in short: Do we need a law of obligations for data? In the following this article makes data as legal objects in European and partially in German contract law a subject of discussion. With reference to the proposal for the Digital Content Directive, digital data on the one hand and personal data on the other hand, as subject matters of contract will be highlighted. Also, for these contracts, a specific problem of this directive will be presented, which will illustrate what aspects shall be included for answering the question if data are marketable due to this directive.

1. Data in European contract law

Against this background, it is very interesting to notice that data play a central role in this legislative proposal.

1.1 New legal objects as points of reference for a contract law system

Unlike the Consumer Sales Directive[7] or the Common European Sales Law for example, the Digital Content Directive refers to legal objects, namely digital content and digital services, instead of types of action[8].

The legal term "digital content" was already used in Art. 2 (j) CESL, for "[…] *data which are produced and supplied in digital form, whether or not according to the buyer's specifications, including video, audio, picture or written digital content, digital games, software and digital content which makes it possible to personalise existing hardware or software*" except *"(i) financial services, including online banking services; (ii) legal or financial advice provided in electronic form; (iii) electronic healthcare services; (iv) electronic communications services and networks, and associated facilities and services; (v) gambling; (vi) the creation of new digital content and the amendment of existing digital content by consumers or any other interaction with the creations of other users*".

After the European Commission had withdrawn the regulation, it novated a modified version of this legal term: For its proposal, "digital content" is defined in Art. 2.1. DCD-COM as "[…] *(a) data which is produced and supplied in digital form, for example video, audio, applications, digital games and any other software, (b) a service allowing the creation, processing or storage of data in digital form, where such data is provided by the consumer, and (c) a service allowing sharing of and any other interaction with data in digital*

[6] European Parliament and Council Proposal for a regulation (COD) 2011/0284 concerning a Common European Sales Law [2011] (CESL)

[7] European Parliament and Council Directive (EC) 1999/44 concerning on certain aspects of the sale of consumer goods and associated guarantees [1999] OJ L 171 (Consumer Sales Directive)

[8] F. Faust 'Digitale Wirtschaft – Analoges Recht: Brauch das BGB ein Update?' in: Gutachten zum 71. Deutschen Juristentag (Munich: Beck 2016) A 5; M. Schmidt-Kessel 'Verträge über digitale Inhalte - Einordnung und Verbraucherschutz', [2014] K & R 2014 475

form provided by other users of the service". So, in this proposal, digital content comprised "digital products" like software, e-books or music and video files as well as "digital services" as described, which the Council separated from "digital content" in its proposal[9] in a new Art. 2.1a. DCD-C, novated by the European Parliament in its draft[10]. Both proposals amended digital content on a "durable medium", defined in Art. 2.11. DCD-C as "[…] *any instrument which enables the consumer or the supplier to store information addressed personally to that person in a way accessible for future reference for a period of time adequate for the purposes of the information and which allows the unchanged reproduction of the information stored*". As per Art. 3.1. DCD-C, "*[t]he Directive shall apply to any contract where the supplier supplies or undertakes to supply digital content or a digital service to the consumer*". In addition, as per Art. 3.3. DCD-C, the directive is applicable to digital content or digital services, which are incorporated on tangible media. In contrast, "embedded digital content", defined in Art. 2.12. DCD-C as "[…] *digital content present in a good, whose absence would render the good inoperable or would prevent the good from performing its main functions, irrespective of whether that digital content was pre-installed at the moment of the conclusion of the contract relating to the good or according to that contract installed subsequently*" is excluded from the directive. If the supplier supplies digital content or a digital service on the one hand and other goods or services on the other, as per Art. 3.6. DCD-C "*this Directive shall only apply to the elements of the contract concerning the digital content or digital service*" like buying a computer, the directive shall only apply to the software but not to the hardware. In contrast, "embedded digital content" is part of the directive on certain aspects concerning contracts for the online and other distance sales of goods[11]. Prima facie, data's embodiment seems to be decisive in which regulations shall apply: For analogue data – personal data excluded – current law shall apply, whereas it shall be distinguished between digital data incorporated on servers or tangible media and digital data as embedded digital content.

1.2 Personal data as a new component in European contract law

Besides these conditions, the Digital Content Directive shall not be applicable, if the supplier supplies digital content or digital services free of charge: In Art. 3.1. DCD-C, it's clarified that the directive "*shall not apply to the supply of digital content or a digital service for which the consumer does not pay or undertake to pay a price* […]". But as per the same regulation, the directive shall also not apply if the consumer "*does not provide or undertake to provide personal data to the supplier*" as well as "*personal data are exclusively processed by the supplier for supplying the digital content or digital service, or for the supplier to comply with legal requirements to which the supplier is subject, and the supplier does not process these data otherwise*". "Personal data" are defined in Art. 2.6. DCD-C, referring to the General Data Protection Regulation[12]: In Art. 4.1 GDPR, personal data are described as "*any information relating to an identified or identifiable natural person*". Unlike "data" as part

[9] Council Proposal for a directive (COD) 2015/0287 concerning on certain aspects concerning contracts for the supply of digital content [2015] (DCD-C)

[10] European Parliament Proposal for a directive (COD) 2015/0287 concerning on certain aspects concerning contracts for the supply of digital content [2015] (DCD-EP)

[11] European Commission Proposal for a directive (COD) 2015/0288 concerning on certain aspects concerning contracts for the online and other distance sales of goods [2015]

[12] European Parliament and Council Regulation (EU) 2016/679 concerning on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1 (GDPR)

of the definition of "digital content" in Art. 2.1. DCD-C, "personal data" for supplied digital content or digital services means not only digital data but analogue data, too[13]. It's not the syntactic, but the semantic level, which plays the decisive role[14].

Because of Art. 3.1 DCD-C the European legislator not only involves personal data in European contract law: It makes clear that the consumer's supply of his personal data can no longer be classified as a favour, but as a counter-performance in a mutual contract[15].

2. Personal data: A new means of payment?

Given the possibility of providing personal data in return for obtaining digital content or receiving digital services, it's justified to discuss if personal data can be qualified as a means of payment like money thereby.

2.1 Consumer's personal data – subject matter of contract?

At least, as a conclusion from Art. 3.1. DCD, it is possible to state that business models including the processing of personal data are now explicit mentioned in European contract law: In Recital 13 of its proposal the European Commission makes clear that "*[i]ntroducing a differentiation depending on the nature of the counter-performance would discriminate between different business models; it would provide an unjustified incentive for businesses to move towards offering digital content against data. A level playing field should be ensured*". But taking a closer look, the question arises if supplying personal data is really the consumer's contractual performance: Namely, processing of personal data requires one of the applicability of one of Art. 6.1 (a)-(f) GDPR. Therefore, the supplier usually needs the consumer's consent to process these personal data, which are not exclusively processed for supplying the digital content or digital service or by which the supplier complies with legal requirements to which he is subject and does not process these data otherwise. Insofar, subject matter of the contract could be this consent or the supply of personal data itself. Only in cases of Art. 6.1 (b)-(f) GDPR, the supplier does not need the consumer's consent to process his personal data[16].

2.1.1 Specifications of the Digital Content Directive

[13] See statement about "personal data" of the Article 29 Data Protection Working Party, WP 136 [2007] 8, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

[14] For this differentiation see H. Zech 'Daten als Wirtschaftsgut – Überlegungen zu einem „Recht des Datenerzeugers": Gibt es für Anwenderdaten ein eigenes Vermögensrecht bzw. ein übertragbares Ausschließlichkeitsrecht?', [2017] CR 2015 138; A. Peukert, ‚Das Sacheigentum in der Informationsgesellschaft' in: A. Ohly; T. Bodewig; T. Dreier; H.-P. Götting; M. Haedicke; M. Lehmann [ed.] ‚Perspektiven des Geistigen Eigentums und Wettbewerbsrechts / Festschrift für Gerhard Schricker zum 70. Geburtstag' (Munich: Beck 2005) 152

[15] A. Metzger 'Dienst gegen Daten: Ein synallagmatischer Vertrag', [2016] AcP 216 834

[16] C.f. L. Specht 'Daten als Gegenleistung – Verlangt die Digitalisierung nach einem neuen Vertragstypus?', [2017] JZ 2017 764; A. Metzger, Ibid., 822-823

Unfortunately, the Digital Content Directive itself offers little help for this problem: At least Art. 3.8 DCD-C makes clear that "*Union law on the protection of personal data applies to any personal data processed in connection with contracts referred to in paragraph 1*". As said before, the supplier has to meet the conditions of Art. 6 GDPR. Besides, Art. 7 GDPR sets requirements, if the consumer gives his consent to process his personal data. Especially pursuant to Art. 7.4, Art. 4.11 DCD-C, the consumer's consent must be a "*freely given, specific, informed and unambiguous indication*". For contracts, it is decisive whether the consumer was forced to consent in processing his personal data or had comparable options to obtain this digital content or to receive a specific digital service[17]. Under the named conditions it can hinge supplying digital content or digital services on the consumer's consent.

2.1.2. Approaches of the German contract law

It is helpful to have a look on which role the consumer's consent plays in national contract law: Beyond Art. 6.1 (b)-(f) GDPR, the consumer's consent is necessary for the supplier to process personal data in compliance with data protection law. Therefore, in German contract law this consent is the key element of the contractual agreement if the consumer does not additionally pay money for obtaining digital content or receiving digital services[18].

2.2 Personal data as a "de facto intellectual property right" in contract law

From this point of view, personal data's role in contract law becomes clearer: Instead of a means of payment, personal data are more similar to intellectual property rights. The consent could be categorised like a licence of a copyright or a patent[19]. In German contract law licencing agreements are typecast as rental or lease contracts[20].

3. A new type of contract for digital and personal data?

But then the next question must be: Which type of contract do we have if the supplier supplies digital content or digital services in return for the consumer's personal data. Contracts of supplying digital content like a music file can be classified as purchase

[17] A. Metzger, Ibid., 823
[18] L. Specht, Ibid., 763-764; M. Schmidt-Kessel, A. Grimm, Ibid., 84
[19] L. Specht, Ibid., 765; A. Metzger, Ibid., 837; W. Kilian 'Informationelle Selbstbestimmung und Marktprozesse: Zur Notwendigkeit der Mordernisierung des Modernisierungsgutachtens zum Datenschutzrecht', [2002] CR 2002 924-928
[20] Bundesgerichtshof [BGH] [Federal Court of Justice] Nov. 17, 2005, Gewerblicher Rechtsschutz und Urheberrecht [GRUR] 2006 435 recital 21; A. Metzger, Ibid., 837

contracts, if the consumer pays a price for it[21]. If the consumer streams series or uses social networks in return for payment, the agreement is typecast as a rental or service contract[22].

If the consumer does not pay a price, but consents in processing his personal data, it is a "hybrid contract", combining both components of the supplier's and the consumer's performances[23].

So, was the European legislator's intention to regulate a new type of contract due to this combination? Or shall the new regulations be integrated in the national classified systems? For this purpose, a closer examination of this legislative project helps.

3.1 A new warranty law for contracts of digital and personal data

The directive contains a set of warranty rules: Art. 6-7 DCD-C name the subjective and objective requirements for conformity of the digital content or digital service as well as a rightful integration of digital content or digital services. In addition, due to Art. 8 DCD-C violations of third party's right were put on the same level as lacks of conformity laid down in Art. 6-7 DCD-C[24]. Furthermore, the directive contains its own set of remedies in Art. 11-12 DCD-C[25]: The consumer can terminate the contract under conditions of these regulations and in cases of lack of conformity, the consumer is entitled to have an appropriate reduction in the price. Only the proposal of the European Commission included the right of damages in Art. 14 DCD-C. It was deleted in the proposal of the Council. The contractual performances themselves are not defined in the directive. The only point of reference is an explanation for the supply of digital content or digital services, laid down in Art. 5 DCD-C: According to that, the supplier complies with his obligation when "*(a) the digital content or any means suitable for accessing or downloading the digital content is received by the consumer or by the physical or virtual facility chosen by the consumer for that purpose [or] (b) the digital service is made accessible to the consumer or to the physical or virtual facility chosen by the consumer for that purpose*". In contrast, it does not matter how the contract is typecast[26].

3.2 Conclusions from this new body of rules

Thus, the Digital Content Directive determines a new general contract law[27]. But it remains possible to integrate these regulations in national types of contracts as well as to define a new type of contract or to set general rules for each type of contract as part of the general law of obligations like sections 311 German Civil Code et. seq. in German contract law.

---

[21] C.f. L. Specht, Ibid., 764
[22] C.f. L. Specht, Ibid., 765
[23] L. Specht, Ibid., 765
[24] See amongst many W. Faber 'Bereitstellungspflicht, Mangelbegriff und Beweislast im Richtlinienvorschlag zur Bereitstellung digitaler Inhalte', in: C. Wendehorst, B. Zöchling-Jud (ed.), 'Ein neues Vertragsrecht für den digitalen Binnenmarkt?' (MANZ'sche Vienna 2016) 100
[25] F. Zoll 'The Remedies in the Proposals of the Online Sales Directive and the Directive on the Supply of Digital Content', [2016] EuCML 250
[26] Cf. F. Zoll, Ibid., 251
[27] F. Zoll, Ibid., 251

3.3 A need for a new type of contract

Therefore, the question should be if there is a need for a new type of contract for national contract law systems.

3.3.1 No regulations about the consumer's obligations

At first, it stands out that the consumer's performance is not defined in the Digital Content Directive. Recital 10 DCD-COM clarifies that the directive "*should not affect national laws […] such as national rules providing for obligations of the consumer towards the supplier of digital content*"[28]. Therefore, starting point has to be the supplier's terms, which must be interpreted[29]: Usually, these terms determine that the consumer shall not make untrue or misleading statements[30]. But can the consumer also be obliged to waive his right to withdraw his consent as laid out in Art. 7.3 GDPR? Neither European nor German contract law provide answers on this question. But the answer can be found in data protection law itself: Because of an effective data protection, the supplier cannot claim the consumer's waiver of his right to withdraw[31].

3.3.2 Consequences of the consumer's withdraw

But if the consumer can withdraw his consent at any time, a legal problem arises because the consumer might have used the supplier's offer and the supplier can only terminate the contract with effect for the future pursuant section 543 para. 2 no. 1 German Civil Code in German contract law. The consumer only shall refrain from using the digital content or digital service which means a risk of abuse[32].

Conclusions

This constellation demonstrates a specific problem of data in contract law: As already said, European legislator tries to protect personal data as well as to improve digital data's marketability within its Digital Single Market Strategy. As shown, the Digital Content Directive regulations are incomplete because they only define the supplier's but not the consumer's obligations. Thereby the European legislator does not regulate a complete

[28] A. Metzger, Ibid., 848-849
[29] A. Metzger, Ibid., 849
[30] See amongst many Facebook's Terms of Service 3.1., https://en-gb.facebook.com/legal/terms?ref=pf
[31] L. Specht, Ibid., 769
[32] L. Specht, Ibid., 769

contract, whereby the supplier's remedies lack. The supplier cannot claim compensation for the value of the use[33], which would be an obvious solution to prevent a risk of abuse.

After all, the European legislator or at least national legislators should feel called to amend contract law rules due to making a new data obligation law and regulating a contract of data. Because of the directive's full harmonisation character, a one-sided regulation does not help if business models including the possibility for the consumer to supply his personal data are included.

Bibliography

2. W. Faber 'Bereitstellungspflicht, Mangelbegriff und Beweislast im Richtlinienvorschlag zur Bereitstellung digitaler Inhalte', in: C. Wendehorst, B. Zöchling-Jud (ed.), 'Ein neues Vertragsrecht für den digitalen Binnenmarkt?' (MANZ'sche Vienna 2016)
3. F. Faust 'Digitale Wirtschaft – Analoges Recht: Brauch das BGB ein Update?' in: Gutachten zum 71. Deutschen Juristentag (Munich: Beck 2016)
4. Kilian 'Informationelle Selbstbestimmung und Marktprozesse: Zur Notwendigkeit der Mordernisierung des Modernisierungsgutachtens zum Datenschutzrecht', [2002] Computer und Recht [CR] 2002 921
A. Metzger 'Dienst gegen Daten: Ein synallagmatischer Vertrag', [2016] Archiv für die civilistische Praxis [AcP] 216 817
A. Peukert, ‚Das Sacheigentum in der Informationsgesellschaft' in: A. Ohly; T. Bodewig; T. Dreier; H.-P. Götting; M. Haedicke; M. Lehmann [ed.] ‚Perspektiven des Geistigen Eigentums und Wettbewerbsrechts / Festschrift für Gerhard Schricker zum 70. Geburtstag' (Munich: Beck 2005) 149
5. M. Schmidt-Kessel 'Verträge über digitale Inhalte - Einordnung und Verbraucherschutz', [2014] Kommunikation & Recht [K & R] 2014 475
6. M. Schmidt-Kessel, A. Grimm 'Unentgeltlich oder entgeltlich? – Der vertragliche Austausch von digitalen Inhalten gegen personenbezogene Daten' [2017] Zeitschrift für die gesamte Privatrechtswissenschaft [ZfPW] 2017 84
7. L. Specht 'Daten als Gegenleistung – Verlangt die Digitalisierung nach einem neuen Vertragstypus?', [2017] Juristenzeitung [JZ] 2017 763
8. J. Thiessen in: M. Schmoeckel, J. Rückert, R. Zimmermann (ed.), 'Historisch-kritischer Kommentar zum BGB' (Tübingen: Mohr Siebeck 2013), Annex to sections 433-453
9. H. Zech 'Daten als Wirtschaftsgut – Überlegungen zu einem „Recht des Datenerzeugers": Gibt es für Anwenderdaten ein eigenes Vermögensrecht bzw. ein übertragbares Ausschließlichkeitsrecht?', [2017] Computer und Recht [CR] 2015 137
10. F. Zoll 'The Remedies in the Proposals of the Online Sales Directive and the Directive on the Supply of Digital Content', [2016] Journal of European Consumer and Market Law [EuCML] 250

Legislation

[33] A. Metzger, Ibid., 864; L. Specht, Ibid., 770

1. European Parliament and Council Proposal for a regulation (COD) 2011/0284 concerning a Common European Sales Law [2011] (CESL)
2. European Parliament and Council Directive (EC) 1999/44 concerning on certain aspects of the sale of consumer goods and associated guarantees [1999] OJ L 171 (Consumer Sales Directive)
3. Council Proposal for a directive (COD) 2015/0287 concerning on certain aspects concerning contracts for the supply of digital content [2015] (DCD-C)
4. European Commission Proposal for a directive (COD) 2015/0287 concerning on certain aspects concerning contracts for the supply of digital content [2015] (DCD-COM)
5. European Parliament Proposal for a directive (COD) 2015/0287 concerning on certain aspects concerning contracts for the supply of digital content [2015] (DCD-EP)
6. European Commission Proposal for a directive (COD) 2015/0288 concerning on certain aspects concerning contracts for the online and other distance sales of goods [2015]
7. European Parliament and Council Regulation (EU) 2016/679 concerning on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1 (GDPR)

Other sources

1. 'A Digital Single Market for Europe: Commission sets out 16 initiatives to make it happen' [May 2015] European Commission Press Release, http://europa.eu/rapid/press-release_IP-15-4919_en.htm
2. Article 29 Data Protection Working Party, WP 136 [2007] 8, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf
3. Bundesgerichtshof [BGH] [Federal Court of Justice] Nov. 17, 2005, Gewerblicher Rechtsschutz und Urheberrecht [GRUR] 2006 435 recital 21
4. Facebook's Terms of Service 3.1., https://en-gb.facebook.com/legal/terms?ref=pf

PASSENGER NAME RECORD (PNR) – AN EFFECTIVE TOOL IN FIGHT AGAINST TERRORISM OR AN UNFAIR LIMITATION OF OUR RIGHT TO PROTECTION OF PERSONAL DATA?

Mateusz Osiecki[1]

Abstract

Global war on terror has became a challenge for nearly all liberal democracies of the world; European Union Member States are not of exception here. When at stake is security and life of citizens, the EU often needs to take unusual steps, including adoption of legal instruments that may interfere with fundamental freedoms. That strategy is strongly linked to mechanism of passenger name record (or 'PNR') – in its essence the system is based on collecting data of its passengers by air carriers and subsequent transferring thereof to national authorities for the purpose of detecting potential terrorist suspects. Although that system has became increasingly popular in some democratic states across the globe, the European Union was rather sceptical towards its adoption, mostly due to mentioned high intrusion into fundamental rights of its citizens. But in 2016, after long-lasting series of tragic terrorist attacks on the continent, European Union eventually adopted so-called 'PNR Directive' aimed at better protection of all Member States' nationals from terrorist threat. Hereby article is aimed at detailed and critical study of the Directive's regime and adaptation to reality of fight against terrorism. Analysis of its crucial aspects in the light of current tendencies in preventing terrorist activities and discussion on right to protection of personal data guaranteed by Charter of Fundamental Rights shall lead to answer whether EU really needs such tools as PNR Directive to ensure appropriate level of counter-terrorist protection.

Keywords: terrorism, passenger name record, European Union, personal data.

Introduction

Terrorism threatens our security, the values of our democratic societies and the rights and freedoms of European citizens. Fighting terrorism is a top priority for the EU and its member states as well as its international partners. That statement is displayed on the official website of European Council and Council of the European Union and shows an attitude of the EU towards combat against terrorism that in 21st century became a truly 'global war on terror'.[2] Repetitive terrorist attempts that occurred on Community's Member States' territories strongly affected their counter-terrorist policy in recent years. In similarity with other liberal democracies across the globe, also countries of the EU decided to

1 PhD candidate at the Chair of International Law and International Relations, Faculty of Law and Administration, University of Lodz, Poland. Interests: aviation safety and security law, anti-terorrism law, international public law, European law.

2 <https://www.consilium.europa.eu/en/policies/fight-against-terrorism/ >, [last accessed: 15th April 2019].

implement legislation aimed at protecting their citizens from terrorism, even limiting to some extent their rights and freedoms. An example of such legislation, adopted on EU level is so-called 'PNR Directive' – an instrument reflecting ideas implemented previously on the other side of the Atlantic that raised many controversies, particularly due to its deep interference into right to protection of personal data. Is the Directive really an effective and accurate tool to assure high level of protection of EU citizens? Hereby article is destined to answer that query.

1. Brief history of counter-terrorist solutions within the European Union

Fight against global terrorism has been present on agenda of international community members for decades. Terrorist activities trace their roots even to antiquity[3] and its periods of "re-awakening" can be dated to second half of 19th century and early years of 20th century, when anarchist movements were on the rise on both sides of the Atlantic.[4] But a truly serious approach towards combat against terrorist threat was taken by international community not earlier than in mid-20th century. The growing activity of extremist groups around the world provoked a debate on international level on what legal measures should be implemented to ensure that states are protected from terrorism. To this debate swiftly joined several international organisations, especially those, for whom terrorism became a real obstacle in achievement of principal goals, like United Nations, International Civil Aviation Organisation, etc. European Union is not an exception in that matter. This Community, being a bloc of economic, social and political cooperation of democratic states respecting rule of law has been "a natural target" for many terrorist groups since its early years of existence.[5] However, general approach to terrorism within the Union has been evolving with time and until the beginning of 21st century there were very modest relevant regulations on supranational level – Rome Treaties creating European Economic Community and Euratom were silent on the issue of terrorism. According to C. Murphy, this was due to high political sensitivity of the topic. Therefore, each Member State was conducting its autonomous counter-terrorism policy.[6]

To bring discussion between Member States on trans-national level, an informal TREVI group was formed in 1976 to act as a forum of exchange of concepts that *de facto*

3 If we talk about earliest groups, whose methods can be compared to terrorist practice, one of them would be Zealots – a Jewish guerilla formation of a religious character that aimed at wiping out Roman occupiers of Palestinian territories in 66-70 A.D. Zealots were brutally killing citizens and sympathisers of Rome.

A. Oehmichen, 'Terrorism and Anti-Terror Legislation: The Terrorised Legislator?A Comparison of Counter-Terror Legislation and Its Implications on Human Rights in the Legal Systems of the United Kingdom, Spain, Germany and France' (Antwerp-Oxford-Portland: Intersentia 2009), p. 51.

4 At that time, targets of terrorists were mostly despotic heads of states or oppressive governors. One of the most remarkable attempts was assassination of Archduke heir to Austro-Hungarian throne, Franz Ferdinand.

E. McWhinney, 'Aerial Piracy and International Terrorism' (Dordrecht : Martinus Nijhoff Publishers 1987), p. 127.

5 Democratic states are generally much more sensible to terrorist attacks, than those ruled by authoritarian regimes, as in those former ones public opinion plays much more important role and may strongly influence the decisions taken by government.

C. Townshend, 'Terroryzm' (Lodz: Wydawnictwo Uniwersytetu Łódzkiego 2017), p. 83.

6 C. Murphy, 'EU Counter-Terrorism Law' (Oxford-Portland: Hart Publishing 2012), p. 17.

was a predecessor of Common Foreign and Security Policy. In 1979, TREVI was reinforced by Police Working Group on Terrorism (or 'PWGOT'). The body was formally established in 1990 with imposed duty of informing police forces of a requesting member state of any kind of terrorist activities.[7]

The Treaty of Maastricht signed by Member States in 1992 did not implement any significant solutions relating to terrorism. However, competences of the Union were extended by two more pillars. The second one called Common Foreign and Security Policy was focused mostly on Community's external actions and the third one named Justice and Home Affairs was oriented at common policies of asylum, immigration, and nationals or third countries.[8] However, none of them made a clear reference to counter-terrorist measures. Eventually, the Treaty of Amsterdam, signed in 1997 was the first legal act adopted on EU level that *expressis verbis* referred to terrorism, rating it as a crime of the same category as human trafficking, drug trade, etc. within the third pillar.[9]

Before the Treaty of Lisbon was adopted, some tasks on fight against terrorism were vested on two formal institutions established under EU law regime – European Police Office (or 'Europol') and the European Union's Judicial Cooperation Unit (or 'Eurojust'). The former one, officially established in 1995 had as a main goal (as expressed in Article 2 paragraph 1 of its Convention on the Establishment) *to improve […] the effectiveness and cooperation of the competent authorities in the Member States in preventing and combating terrorism, unlawful drug trafficking and other serious forms of international crime*.[10] In addition to that, pursuant to Article 2 Europol was obliged to deal with crimes that are committed in the course of terrorist action against life, limb, personal freedom or property. In turn, Eurojust, founded in 2000 on the grounds of Treaty of Niece, functions as a crucial partner of Europol responsible for coordination of Member States' prosecutors' actions in fight against international crimes, including terrorist offences. Its main objectives include detecting, pursuing, arresting and forming indictments.[11]

Nevertheless, this whole anti-terrorist legal framework based on Treaties' provisions was rather underdeveloped. In fact, the Old Continent has been targeted many times by terrorists already in previous century, but none of those attacks had such a huge impact on the continent that the EU institutions decided to act more violently. But everything has changed after the attacks on World Trade Center on September 11th, 2001.

Those attacks, although having directly hit the United States, were in reality targeted at the whole international community, with “Western world” on the foreground. Therefore, the European Union also felt their impact.[12] Following years were even more brutal for Europe, as several terrorist attempts struck its largest cities. The most notable were bombings in Madrid on March 2004 and in London on July 2005, as well as later attacks on civil aviation: shooting at Glasgow Airport on June 2007, gunfires at Frankfurt Airport on March 2011 and bombing at Brussels National Airport on March 2016 [see: section 3]. All those events ignited the discussion on the counter-terrorist policy within European institutions that brought

7 J. Gierszewski, 'Unia Europejska w walce z terroryzmem międzynarodowym', [2009] 1(2), Acta Pomerania, p. 137-138.

8 See more: P. Craig, G. de Burca, 'EU Law. Text, Cases and Materials', (New York: Oxford University Press 2011), p. 15.

9 M. Lech., 'Ochrona prawna społeczności międzynarodowej wobec zagrożenia terroryzmem', (Gdansk: Wydawnictwo Uniwersytetu Gdańskiego 2014), p. 158.

10 Council Act of 26 July 1995 drawing up the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Official Journal of the European Communities C 316/1), Art. 2(1).

11 M. Lech, op. cit., p. 164.

12 According to C. Murphy, in the attacks died 67 Britons, 11 Germans, 10 Italians, 6 Irish, 5 Portuguese, 3 French and many other European nationals.
See: C. Murphy, op. cit., p. 22.

its effects in implementation of concrete measures and accession of the Community to relevant international agreements. Some of them sparked many controversies among law experts, especially because some of them seem to clash with freedoms guaranteed by Charter of Fundamental Rights. A glaring example here are agreements and a directive concerning passenger name record (or 'PNR').

2. PNR – a nature and legal origins

'Passenger name record' is a term used mostly in the context of air travel and aviation industry. International Civil Aviation Organisation defined it in its Document no 9940 entitled *Guidelines on Passenger Name Record (PNR) Data* in a following way: *[t]he generic name given to records created by aircraft operators or their authorized agents for each journey booked by or on behalf of any passenger.*[13] An even simpler and also accurate definition can be found on European Commission website: *[i]nformation provided by passengers and collected by airlines, in the normal course of their business, for enabling reservations and carrying out the check-in process.*14 Besides its role in managing reservation and check-in of passengers by airlines, PNR have been used in several countries as a tool to detect and prevent terrorist operations. The first one to introduce it was the United States – in the aftermath of attacks on September 11th, the US government decided to more effectively control movement of air passengers into its territory for the purpose of finding potentially dangerous figures.15 Crucial here is §44909(c) of the U.S. Code that in paragraph 1 obliges all air carriers (both national and from oversees) operating passenger flight in foreign air transportation to the United States to provide to appropriate authorities by electronic transmission a passenger and crew manifest containing specific information.16 Furthermore, paragraph 3 stipulates that air carriers shall provide Customs Service passenger record information only upon request. That mechanism of submitting data on prior authorities' demand, so-called “push method” is less intrusive than 'pull method' under which PNR is transferred automatically to state organs, without a request.

European Union was for many years rather sceptical towards implementation of similar legal measures on PNR, mostly due to their relatively high interference into right to protection of personal data. However, terrorist attacks that occurred in Europe in first years of 21st century [see: *supra*], convinced EU institutions to initiate a debate thereon. Before the Union adopted its own legal instrument concerning PNR, it had signed several international treaties with its allied states. A first bilateral agreement was concluded with the United States in 2004, but was later

13 ICAO, 'Guidelines on Passenger Name Record (PNR) Data', ICAO Doc 9944, para 2.1.1.

14 European Commission, <https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange/pnr_en> [last accessed: 10 April 2019].

15 N. Vavoula, '"I Travel, therefore I Am a Suspect': an overview of the EU PNR Directive', (26 October 2016, EU Immigration and Asylum Law and Policy, <http://eumigrationlawblog.eu/i-travel-therefore-i-am-a-suspect-an-overview-of-the-eu-pnr-directive/> [last accessed: 10 April 2019]).

16 The catalogue of information that has to be provided is enshrined in paragraph 2:
(A) The full name of each passenger and crew member.
(B) The date of birth and citizenship of each passenger and crew member.
(C) The sex of each passenger and crew member.
(D) The passport number and country of issuance of each passenger and crew member if required for travel.
(E) The United States visa number or resident alien card number of each passenger and crew member, as applicable.
(F) Such other information as the Administrator of the Transportation Security Administration, in consultation with the Commissioner of U.S. Customs and Border Protection, determines is reasonably necessary to ensure aviation safety.
See: 49 U.S. Code §44909(c)(3).

annulled by the Court of Justice of the EU due to lack of 'an appropriate legal basis'.17 Soon the European Parliament adopted a Resolution on launching negotiations with third states for PNR agreements that would focus on law enforcement and security purposes. As a result, Commission drafted three proposals oriented at negotiating such agreements with Australia and Canada, as well as re-draft a treaty with the United States.18 In 2012, treaties with Australia and the US were concluded and signed, subsequently approved by Parliament and entered into force on 1st June 2012. However, original PNR treaty with Canada, drafted in 2014 did not receive the approval and instead was subject of request for opinion from CJEU submitted by the Parliament. Ultimately, the Court declared that the agreement was incompatible with EU law in primary form, as some of its provisions were colliding with fundamental rights recognised by the Union.19 As a result, the Commission initiated new negotiations process with Canada in June 2018 under Council authorisation.20

3. Current legal situation of PNR system in the EU

Cooperation with strategic partners, and above all, growing threat of terrorist attacks in Europe in 2010s convinced EU to establish its own legal system of usage of passenger name record for the purpose of preventing terrorism. Its efforts resulted in adoption of Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (hereinafter referred to as 'PNR Directive' or simply 'Directive'). Vital is to note here that nearly a month before the instrument was adopted, a tragic terrorist attack occurred in Belgium – on March 22nd, 2016 bombs at Brussels National Airport and Maelbeek metro station detonated by suicide bombers of Islamic State killed more than 30 people and injured nearly 200.21

The main goal of the Directive is stipulated in Article 1: collection and processing of PNR *only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime*.22 In similarity with already mentioned U.S. Code provisions, the Directive also sets out a mechanism of collecting data of passengers by a specific authority. In that particular case, this authority is called 'passenger information unit' (or 'PIU'). Pursuant to the Directive, each Member State establishes or designates PIU (therefore it can be a completely new state organ or already existing, e.g. functioning within civil aviation authority). However, there is no obligation of designating one PIU per Member State. Two or more countries may ultimately decide to have one common PIU acting for all of them. Regardless of that, each PIU is vested with powers enshrined in Article 4:

---

17 CJEU, Judgment of 3 May 2006, Joined Cases C-317/04 and C-318/04, European Parliament v. Council of the European Union and Commission of the European Communities, ECLI:EU:C:2006:346.

See more: K. Kopyłowska, F. Kruse, 'Passenger Name Records: the transatlantic dimension', (9th Annual Seminar on the European Union constitutionalism, May10-12 2010, <http://pl.zpc.wpia.uw.edu.pl/wp-content/uploads/2010/04/8.-EU-US-PNR-Agreement-final-version1.pdf> [last accessed: 10 April 2019]).

18 S. Villani, 'Some Further Reflections on the Directive (EU) 2016/681 on PNR Data in the Light of the CJEU Opinion 1/15 of 26 July 2017', [2018] 101, Revista de Derecho Politico, p. 902.

19 Ibidem, p. 905.

CJEU Opinion 1/15, [2017] ECLI:EU:C:2017:592;

The Court observed, inter alia, that the transfer of PNR data from EU Member States to Canada and alll rules concerning retention and processing of data seriously interferes with fundamental right to respect for private life, as well as fundamental right to protection of personal data.

20 European Commission, <https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange/pnr_en >, [last accessed: 11 April 2019].

21 See more: M. Osiecki, 'Terrorism vs. International Law – Case of Attacks in Brussels' [in:] 5th International Conference of PhD Students and Young Researchers, 'How deep is your law? Brexit. Technologies. Modern conflicts conference papers 27-28 April 2017' (Vilnius University 2017) p. 280-281.

22 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (hereinafter "PNR Directive"), art. 1.

(a) collecting PNR data from air carriers, storing and processing those data and transferring those data or the result of processing them to the competent authorities […];

(b) exchanging both PNR data and the result of processing those data with the PIUs of other Member States and with Europol […] .23

The Directive stipulates in Article 8 that PNR data are collected via 'push method' – when PIU receives the data from an air carrier and keeps it stored, a Member State needs to make a request to access it. However, forwarding such a request may be ineffective if done after 5 years of their transfer to the PIU of the Member State on whose territory the flight is landing or departing. That results from Article 12 obliging to delete and depersonalise the data through masking out of specific elements after a period of six months.24

Finally, when a Member State is already at the possession of data, it may exchange it with a different EU member or deliver it to Europol via electronic means.25

4. Effective protection against terrorism or intrusion to rights of EU citizens?

Adoption of the PNR Directive met with criticism from some European law experts, mostly due to potential conflict between its provisions with Article 8 of Charter of Fundamental Rights of the European Union, guaranteeing right to protection of personal data. In fact, under the Directive's regime Member States are granted access to great amount of data of air passengers. Annex I enumerates all possible information that can be collected by air carriers; apart from records such as names of passenger, his itinerary or date of reservation, there are also more detailed ones, like frequent flyer programme, or identification of travel agent that issued a ticket. What is more, a limitation of access only to data of passengers that board extra-EU flights encapsulated in Article 1(1) point (a) has a rather formal, if not illusive character – Article 2 entitles Member States to extend application of the Directive also over intra-EU flights, so potentially PNR of all passengers whose flights origin or end on the territory of any Member State might be subject to processing.26 Currently, 20 Member States have expressed their intent to do so.27

A general purpose of implementation of such intrusion is expressed in the PNR Directive's Preamble (Recital 7): [*a]ssessment of PNR data allows identification of persons who were unsuspected of involvement in terrorist offences or serious crime prior to such an assessment and who should be subject to further examination by the competent authorities. By using PNR data it is possible to address the threat of terrorist offences and serious crime from a different perspective than through the processing of other categories of personal data. However, to ensure that the processing of PNR data remains limited to what is necessary, the creation and application of assessment criteria should be limited to terrorist offences and serious crime for which the use of such criteria is relevant. Furthermore, the assessment criteria should be defined in a manner which keeps to a minimum the number of innocent people wrongly identified by the system.28* The wording of that provision clearly shows that *ratio legis* for the Directive is prevention. Member States are then able to, on the basis of acquired data, assess whether a person, that has never been previously suspected of terrorism, may have any connotations with terrorist activity. A typical example would be monitoring a person of exactly the same name and home address as members of family who were responsible for a terrorist attack that occurred some time before the former one booked a flight.

---

23 Ibidem, art. 4.

24 S. Vilani, op. cit., p. 913.

25 Ibidem, p. 913.

26 Most of the flights in the EU are intra-EU (those accounted for 47% of total passengers in 2016), followed by extra-EU (36% in 2016) and domestic flights (17% in 2016).
See: <https://ec.europa.eu/eurostat/statistics-explained/index.php/Air_transport_statistics>, [last accessed: 14 April 2019].
N. Vavuola expressed her concern that in conditions of such a dynamic movements of persons, scope of state surveillance allows constant observation of people, even if none was previously involved in serious crime or terrorist offence.
See: N. Vavuola, op. cit.

27 Since the United Kingdom is expected to leave the EU in 2019, the list of those states shall probably shrink to 19:
<https://ec.europa.eu/home-affairs/news/list-member-states-applying-pnr-directive-intra-eu-flights_en> [last accessed: 14th April 2019].

28 PNR Directive, Preamble.

Is then a system introduced by the Directive relevant for fight against terrorism? Many critics point out that the basic problem with effectiveness of the instrument is a fact that currently most people living in EU countries use rail or road transport, which dramatically limits the possibilities of identifying those that are involved in terrorism. Additionally, the regime of PNR Directive does not establish a single database of records, but instead more than twenty independent databases managed by Member States separately. The flow of data between them is not compulsory, but just voluntary.29 Therefore, the overall effectiveness of protection from terrorism is rather modest and disproportional in relation to limitation of right to protection of personal data guaranteed by Article 8 of the Charter. Air passengers by booking a flight ticket are automatically exposed to possibility of having considerable amount of their data acquired by Member States for the price of doubtful level of security.

Conclusions

It is difficult to imagine today's reality of fight against terrorism without necessity of limiting some of rights normally protected by international treaties or other documents such as EU Charter of Fundamental Rights, especially as methods used by terrorist networks are more brutal than ever before, which was demonstrated by attacks on World Trade Center in 2001, London metro in 2005, Brussels Airport in 2016 etc. PNR Directive is a glaring example of a tool that may seriously limit our right to protection of personal data in exchange for better anti-terrorist security. However, relatively large amount of data that is made accessible for Member State's authorities at purchase of air tickets seems a high intrusion in comparison with low level of safety provided. A potential terrorist, knowing that his data is visible for EU Member States may simply resign from buying an airline ticket and choose another mean of transport to reach his final place, or attack a different target than civil aircraft, like an international airport (airport premises from the landside are normally open to public and then are relatively easier targets than airliners).

What is more, PNR Directive itself features few significant forms of limitation to Member States' control. Any single Member State is entitled to apply the Directive's provisions also to intra-EU flights, which seriously expands the scope of personal data reachable by them and in consequence deepens intrusion of state's authorities into fundamental freedoms. On the other hand, application of “push method” that allows to extract data from PIUs only on demand and not automatically, as well as time limit of records' retention functions as a shortage of Member States' powers in regards to control of citizens' personal data.

Taking into account all arguments mentioned above, it is quite difficult to unequivocally rate the PNR Directive in anti-terrorist context. High level of states' control over citizens' personal data that seems disproportional in regards to protection against terrorist threat is very controversial and raises a question whether EU really has to limit its people's rights in such way in order to assure freedom from terrorist attacks. Here crucial criterion shall be lapse of time – if EU Member States really become safer and their citizens accept the idea of processing of PNR then Directive might be eventually seen as an effective and useful tool to eliminate or at least critically reduce terrorist threat on the Old Continent.

Bibliography

29 G. Verhofstadt, 'Europe's Last Chance. Why the European States Must Form a More Perfect Union' (New York: Basic Books 2017), para 321.

1. Craig P., de Burca G., 'EU Law. Text, Cases and Materials', (New York: Oxford University Press 2011)
2. Gierszewski J., 'Unia Europejska w walce z terroryzmem międzynarodowym', [2009] 1(2), *Acta Pomerania*
3. Kopyłowska K., Kruse F., 'Passenger Name Records: the transatlantic dimension', (9th Annual Seminar on the European Union constitutionalism, May10-12 2010, http://pl.zpc.wpia.uw.edu.pl/wp-content/uploads/2010/04/8.-EU-US-PNR-Agreement-final-version1.pdf
4. Lech M., 'Ochrona prawna społeczności międzynarodowej wobec zagrożenia terroryzmem', (Gdansk: Wydawnictwo Uniwersytetu Gdańskiego 2014)
5. McWhinney E., 'Aerial Piracy and International Terrorism' (Dordrecht : Martinus Nijhoff Publishers 1987)
6. Murphy C., 'EU Counter-Terrorism Law' (Oxford-Portland: Hart Publishing 2012)
7. Oehmichen A., 'Terrorism and Anti-Terror Legislation: The Terrorised Legislator?A Comparison of Counter-Terror Legislation and Its Implications on Human Rights in the Legal Systems of the United Kingdom, Spain, Germany and France' (Antwerp-Oxford-Portland: Intersentia 2009)
8. Osiecki M., 'Terrorism vs. International Law – Case of Attacks in Brussels' [in:] *5th International Conference of PhD Students and Young Researchers, 'How deep is your law? Brexit. Technologies. Modern conflicts conference papers* 27-28 April 2017' (Vilnius University 2017)
9. Townshend C., 'Terroryzm' (Lodz: Wydawnictwo Uniwersytetu Łódzkiego 2017)
10. Vavoula N., *'"*I Travel, therefore I Am a Suspect': an overview of the EU PNR Directive', (26 October 2016, EU Immigration and Asylum Law and Policy, http://eumigrationlawblog.eu/i-travel-therefore-i-am-a-suspect-an-overview-of-the-eu-pnr-directive/
11. G. Verhofstadt, 'Europe's Last Chance. Why the European States Must Form a More Perfect Union' (New York: Basic Books 2017)
12. Villani S., 'Some Further Reflections on the Directive (EU) 2016/681 on PNR Data in the Light of the CJEU Opinion 1/15 of 26 July 2017', [2018] 101, *Revista de Derecho Politico*

DIGITAL AGENTS AND CONTRACTUAL PERFORMANCE – A CONTRIBUTION TO THE MODERN INTERPRETATION OF AN ATTRIBUTION STANDARD IN GERMAN CONTRACT LAW DUE TO THE RISING DEPLOYMENT OF ARTIFICIAL INTELLIGENCE

Theresa Preßler[1]

Abstract

This paper is embedded in the research field of law and artificial intelligence and more particularly in the debate on how current legislation is able to respond to the challenges arising from the use of artificial intelligence. It illustrates on how to investigate whether an attribution rule, Section 278 of the German Civil Code (BGB), could and should be applicable to systems with a certain degree of autonomous and cognitive features. By focussing on this specific key standard of German Contract Liability Law, it illustrates one possible approach to review the current legal framework and to identify its potential to cope with/ concerning new technical innovations.

Pursuant to this rule, the obligor is responsible for fault of persons whom he uses to perform his contractual obligation (so- called "agents") to the same extent as for fault of his own part. The norm has been originally designed for the attribution of human behaviour and aims to cover risks due to the unforeseeable, autonomous decision-making of third persons being deployed by the obligor. It is mainly based on the concept that someone who reaps the benefit of the division of labour, must also accept its disadvantages.

The idea of extending the scope from human to digital agents can be considered as one possibility to cover new liability gaps resulting from the features of such systems: Unlike other simple tools, these systems are able to learn from experience and therefore do not follow a typical stimulus-response scheme. Consequently, their reactions will not always be predictable as they can be the result of a learning process or further development which goes beyond the initial programming.

Whereas the deployment of AI systems could be generally comparable to the risks of the deployment of humans, one would have to overcome a comprehension of concepts which used to be exclusively reserved for humans: Section 278 requires "fault" of the agent to be attributed to the obligor. While there are voices who are willing to open up terms like fault for certain manifestations of artificial intelligence, others do not see the need and rather stick to the traditional interpretation of ordinary rules. In the following, this interface will be addressed by giving an overview of the approaches which have been developed so far and by pointing out in what way they require further research.

[1] PhD Student at the Chair of Civil Law, Commercial Law and Intellectual Property Law of Prof. Dr. Peukert, Civil Law Department at Goethe University of Frankfurt/ Main. Topic of dissertation: "Digital Agents – could and should Section 278 of the German Civil Code be applicable to artificial intelligent systems?" The following paper reflects the author's presentation of her PhD project during the 7th International Conference of PhD Students and Young Researchers "Law 2.0.: New methods, New Laws" in Vilnius.

Keywords: artificial intelligence, autonomy risk, robot law, contract liability, attribution rule, vicarious agents.

Introduction: Artificial intelligence as new challenge for law

Digital phenomena invite to reconsider the complex interaction between law and technical innovation. The implications of regulation have been subject to several discussions that go back to the beginning of the 19th and 20th century when some basic innovations like railways and cars had been made commercially viable.[2] Numerous of technical revolutions followed[3] and kept challenging lawmakers to provide a suitable legal framework that balances technical progress and public acceptance adequately. In this context, it is important to stress that regulation does not only aim to restrict or limit technical possibilities but to create legal certainty for both developers and users.[4] Moreover, legal control and liability standards in particular, can establish public trust in new products which is required to integrate them in the market field and incentivise people to use them. Ultimately, all these effects also facilitate social acceptance of associated change concerning several areas of life.

Generally, two crucial questions need to be answered: when to regulate and how to regulate. To choose the right time for legal control over new phenomena might be the greatest difficulty[5] for two reasons: If adjustment is made too early one must assume fictitious cases and conceivable scenarios which bear the risk of overregulation. If law makers wait too long, they will risk to always "run behind" because of the growing gaps between emerging technologies and legal oversight.

Artificial intelligence[6] belongs to a sort of innovation that is said to profoundly transform societies worldwide.[7] The introduction of this new generation of systems is imminent or has already taken place. Both depends on the system and the country. In Europe, the key questions of when and how to regulate are currently raised. They are embedded in wide debates about the future extent of the fourth technical revolution which calls for reactions of all institutions shaping social coexistence. On the question of timing the European Parliament has already made a clear statement: At the beginning of 2017 it agreed on resolutions on Civil Law Rules for robotics[8] calling for "rules to provide clarity on the legal liability of various actors concerning responsibility for the acts and omissions of robots (...)" and other manifestations of artificial intelligence. While there are several legal scholars who also see an urgent need for research addressing these issues, others do not (yet) see the

[2] M. Kloepfer, 'Technik und Recht im wechselseitigen Werden' (Berlin: Duncker & Humblot 2002), p. 74.
[3] An innovation that is always mentioned in this context is genetic engineering.
[4] M. Kloepfer, 'Technik und Recht im wechselseitigen Werden' (Berlin: Duncker & Humblot 2002), p. 86, 104.
[5] M. Kloepfer, 'Technik und Recht im wechselseitigen Werden' (Berlin: Duncker & Humblot 2002), p. 69.
[6] In the following the abbreviation AI will be used for artificial intelligence.
[7] M. Ebers, S. von Lingen, 'RAILS and GRUR in Conversation with Sharad Ghandi', (26 November 2018), Robotics & AI Law Society (RAILS), https://ai-laws.org/2018/11/ai-is-the-most-profound-technology-created-by-mankind/.
[8] European Parliament,'European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))', 16 Februar 2017, http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.pdf.

need considering them as too futuristic.[9] Ultimately, this reflects the ambivalence of a prospective legal surveillance[10] pointed out above on a concrete example. The present paper follows the approach of the European Parliament as it aims to contribute to the discussion on if and how current legislation is able to cope with AI systems. On the question of how to regulate there are basically two possibilities: by adjusting existing rules or by creating new ones. Either way, to make this decision a review on the potential and limits of the existing rules is required.

1. "Human law" for AI systems

This paper aims to look at one key standard of German contract liability law in particular: Section 278 (1) of the German Civil Code (BGB). It examines whether the standard could and should be applicable to intelligent technical systems. Section 278 is an attribution rule that regulates the responsibility for third parties. It states that the obligor is responsible for fault of persons whom he uses to perform his contractual obligation to the same extent as for fault of his own part. In other words, if the obligor deploys a third person[11] to perform parts of his contractual duty and this person culpably causes a damage in the course of his deployment, Section 278 attributes his or her fault to the obligor. These persons who are used by the obligor are called vicarious agents or just agents in the sense of assistants. Section 278 was originally designed for the attribution of human behaviour[12] and is based on the concept that someone who reaps the benefit of the division of labour, must also bear its disadvantages.[13] Its objective is to cover personnel risks i.e. the risk of unforeseeable, autonomous decisions of a third person involved in the implementation of the contract without being a party.[14] It attributes the effects of unpredictable decisions to the obligor[15] as this can be considered the classic risk when deploying third parties to take on tasks being part of his contractual duties. Ultimately, the choice to delegate these tasks includes the choices that are involved in the execution of those tasks.[16]

On an abstract level, this paper asks whether standards primarily referring to human behaviour can be applicable to certain manifestations of artificial intelligence.

---

[9] With numerous references for both approaches G. Teubner,'Digitale Rechtssubjekte – Zum privatrechtlichen Status autonomer Softwareagenten' [2018] 218 Archiv für die Civilistische Praxis, p.156 et seqq ; G. Sartor, 'Contracts in the Infosphere' in: S. Grundmann: European Contract Law in the Digital Age', (Cambridge: Intersentia 2018), p. 263.

[10] M. Kloepfer, 'Technik und Recht im wechselseitigen Werden' (Berlin: Duncker & Humblot 2002), p. 281.

[11] Third persons mean non-contractual party.

[12] J. Günther, 'Embodied Robots – Zeit für eine rechtliche Neubewertung' in M. Gruber/ J. Bung/ S. Ziemann, 'Autonome Automaten: Künstliche und artifizielle Agenten in der technisierten Gesellschaft, (Berlin: 2014), p. 164.

[13] C. Wendelstein, 'Zur Schadenshaftung für "Erfüllungs"- Gehilfen bei Verletzungen des Integritätsinteresses' [2015] 215 Archiv für die Civilistische Praxis, p. 71.

14 P. Hacker, 'Verhaltens- und Wissenszurechnung beim Einsatz von Künstlicher Intelligenz' [2018] 3 RW Rechtswissenschaft, p. 254.

15 G. Teubner, 'Digitale Rechtssubjekte – Zum privatrechtlichen Status autonomer Softwareagenten' [2018] 218 Archiv für die Civilistische Praxis, p.187 et seq..

16 G. Sartor, 'Contracts in the Infosphere' in: S. Grundmann: European Contract Law in the Digital Age', (Cambridge: Intersentia 2018), p. 272

1.1 Deployment of digital agents for contractual performance

For the sense and purpose of this paper, digital agents mean AI systems like self-learning algorithms[17] or robots[18] with a certain degree of cognitive and autonomous[19] features. Unlike other simple tools, these systems are able to learn from experience and therefore do not follow a typical stimulus-response scheme. They are given goals and will then be trained how to achieve them using examples and feedback. Through this, they are not only executing pre-programmed instructions, but also discover their own solutions and can abstract their learning experiences. To a certain extent, these capacities allow them to perceive, understand, predict and to alter their environment according to their goals.[20] Consequently, their reactions will not always be predictable as they can result from learning process or further development which goes beyond the initial programming.[21]

As digital agents they are already and will be increasingly deployed in different fields to take on tasks which require the ability of an autonomous decision-making and an interaction in an unstructured environment[22] without permanent human assistance and immediate control. Whereas decision algorithms are already used to support or even make medical diagnosis[23], robots could be deployed as service or care robots in the service and healthcare sector.[24] The crucial point here is the transfer of a decision-making power to the AI system.

1.2 Unpredictability as new risk

If the obligor decides to accomplish contract-related tasks with the support of such systems or even delegates the whole performance of his contractual duty to them[25], his

17 H. Dettling, S. Krüger, 'Digitalisierung, Algorithmisierung und Künstliche Intelligenz im Pharmarecht, [2018] Pharmarecht, p 513, 520 et seq.

18 M. Lohmann, 'Roboter als Wundertüten – eine zivilrechtliche Haftungsanalyse', [2017] 2 Aktuelle Juristische Praxis, p.152 et seqq.

19 It is difficult to find a definition of autonomy for the purpose of this investigation: If the standard is too high (autonomy requires all human cognitive capacities), nearly no AI system can be considered autonomous. If the standard is too low, almost all algorithms quailfy as autonomous, G. Sartor, 'Contracts in the Infosphere' in: S. Grundmann: European Contract Law in the Digital Age', (Cambridge: Intersentia 2018), p. 266.

20 G. Sartor, 'Contracts in the Infosphere' in: S. Grundmann: European Contract Law in the Digital Age', (Cambridge: Intersentia 2018), p. 266.

21 H. Zech, 'Liability for Autonomous Systems: Tackling Specific Risks of Modern IT' in: S. Lohsse/ R. Schulze/ D. Staudenmayer, Liability for Artificial Intelligence and in the Internet of Things', (Baden-Baden: Nomos 2019), p. 187 et seqq.

22 M. Lohmann, 'Roboter als Wundertüten – eine zivilrechtliche Haftungsanalyse', [2017] 2 Aktuelle Juristische Praxis, p.154.

23 The American Food and Drug Administration has just permitted a medical device with image-analysing algorithm for.3 The system is the first device authorized for marketing that makes a screening decision without the need for a physician to also interpret the results. U.S. Food & Drug Administration (FDA), 'FDA permits marketing of artificial intelligence-based device to detect certain diabetes-related eye problems', (11 April 2018), https://www.fda.gov/newsevents/newsroom/pressannouncements/ucm604357.htm.

24 For a categorisation of different robots and their application fields see M. Lohmann, 'Roboter als Wundertüten – eine zivilrechtliche Haftungsanalyse', [2017] 2 Aktuelle Juristische Praxis, p.155 et. seqq.

25 G. Sartor, 'Contracts in the Infosphere' in: S. Grundmann: European Contract Law in the Digital Age', (Cambridge: Intersentia 2018), p. 264

responsibility for damages under the current legal framework is not clear at this stage. Whereas he would be held liable if he did not adequately maintain and monitor the system and therefore had breached his duties of care, his liability would be questionable if the damage was only a result of machine learning processes.[26] By deploying technical systems with a certain degree of cognitive capacities one will face a new type of risk that is inherent in autonomous decision-making: unpredictability.[27] When comparing risks of AI systems with classic product risks as covered under product liability law unpredictability is the key distinguishing feature. It is the main reason why AI systems cannot be considered as simple tools operating for their user.

2. Extending the scope of Section 278 BGB to digital agents?

Concerning German contract law, the difficulty of covering this new scenario can be traced back to one of its basic structural principles: The German Civil Code does not provide a standard regulating the contractual liability of the obligor for damages caused by things he was using to perform his obligation. The existing contractual liability rules only address human behaviour. They presuppose a behaviour of the debtor himself that then could be considered as breach of duty.

Against this backdrop the general idea to extend the scope of Section 278 to certain technical systems is not new. Initial discussions go back to the 1950's starting with simple automatic tools[28] and had a revival when computers[29] were introduced for private use. Unlike today the approach then was to attribute classic product risks like unrecognisable technical failure of systems to the obligor even when he had maintained and supervised it sufficiently. Ultimately, one was trying to overcome the same structural principles of contractual liability law as mentioned above but for another class of risks.[30] However, the introduction of intelligent systems with the ability of autonomous decision-making sheds a new light on the basic idea that the deployment of technical systems could be comparable to the risks of the deployment of humans.

2.1 How to review?

The review of the standard comprises two parts: a legal ("could") one and a normative ("should") one. In order to provide a clear structure all key aspects are divided into discussion parameters. This paper will only outline some extracts of one parameter within in the legal part of the analysis namely the criterions of the standard itself. There are mainly two elements that are considered problematic regarding a shift of its scope: legal capacity and the requirement of fault of the agent.

2.2 Legal capacity as application requirement

[26] The liability of the manufacturer will not be subject of this paper.
[27] G. Teubner, 'Digitale Rechtssubjekte – Zum privatrechtlichen Status autonomer Softwareagenten' [2018] 218 Archiv für die Civilistische Praxis, p.174.
[28] M. Wolf, 'Schuldnerhaftung bei Automatenversagen' [1989] Juristische Schulung, p. 899-902.
[29] M. Brunner, 'Zum Risiko für Computerfehlleistungen bei der Abwicklung von Verträgen. Der Computer als Erfüllungsgehilfe', (Kiel: 1970).
[30] P. Hacker, 'Verhaltens- und Wissenszurechnung beim Einsatz von Künstlicher Intelligenz' [2018] 3 RW Rechtswissenschaft, p. 249.

The official heading of Section 278 reads “Responsibility of the obligor for third parties”. The standard itself describes them as “legal representatives” and “persons” the debtor uses to perform a contractual duty. To date, the concept of “person” means natural or legal persons, thus legal subjects with the ability to bear rights and duties. Therefore, one can argue that legal capacity is a mandatory prerequisite to fall under the term “agent” and therefore under the scope of Section 278. As a result, the direct application of Section 278 on technical systems would not be possible.

In order to overcome the current lack of legal capacity one could create a special status for certain systems as electronic persons. The implications of this idea are already being discussed intensively both in the philosophical[31] and legal academic discourse. The discussion comprises a wide spectrum of opinions on how to approach the possible incorporation of certain AI systems as legal entities. Ultimately, this reflects the general controversy on how to determine the concept of legal capacity as one of the fundamental issues of (German) civil law. There can be identified two main approaches to this ontological question: a normative one and a functional one. According to some voices the decision has to be made based on anthropocentric arguments. In their opinion, legal capacity should be granted to AI systems that are sufficiently similar to human beings. Therefore, they are facing questions like “can these systems have a free will” or “do they have something like a conscience”.[32] In contrast, others advance a more functional approach emphasising that legal capacity is by no means limited to natural person as the concept of legal persons shows.[33] According to them, AI systems should be granted legal capacity if it seems useful considering the purpose of the legal standard in question. Instead of focussing on potential similarities between natural persons and AI systems, this pragmatic comprehension of legal capacity allows to differentiate between certain degrees of autonomy of each system and to introduce them into legal transactions step by step. Moreover, it provides the flexibility that is necessary to consider the variety of systems and their individual features.[34]Since the possible implementation of electronic persons is envisaged in the EU-Parliament’s resolutions[35] the initial academic discourse has been brought to a new level.

Based on the preferred functional approach, it has to be examined if the use of an AI system touches the objective of Section 278 and if yes which extent is to be required. To determine if a system leads to personnel risks in the sense of Section 278 one has to carefully analyse its features and the respective application field. For example, for a decision-algorithm deployed for medical diagnosis one would have to ask whether there is still the need for a physician to also interpret the results.

2.3 Fault of the agent

[31]See A. Matthias, ‘Automaten als Träger von Rechten’, (Berlin: Logos-Verlag 2008).
[32]J. Schirmer, ‘Rechtsfähige Roboter?’ [2016] 13 JuristenZeitung, p.661 et seqq.
[33]G. Teubner, ‘Digitale Rechtssubjekte – Zum privatrechtlichen Status autonomer Softwareagenten‘ [2018] 218 Archiv für die Civilistische Praxis, p.163 et seqq.
[34] J. Schirmer, ‘Rechtsfähige Roboter?’ [2016] 13 JuristenZeitung, p.663 et seqq.
[35] “(…) the most sophisticated autonomous robots could be established as having the status of electronic persons responsible for making good any damage they may cause (…)”, European Parliament,‘European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))‘, 16 Februar 2017, http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.pdf, p. 18.

Section 278 aims to attribute behaviour and fault of the agent to the obligor. Again, it is questionable whether fault as concept can be transferred to AI systems. One can advance this issue from two directions: The first is a "standard-related" one. It starts by taking a closer look on fault as criterion within the standard itself and on how it can be determined. From a technical legal perspective, fault generally presupposes a reference point in form of a behaviour requirement.[36] In Section 278 this reference point is a breach of a contractual duty of the obligor. As this contractual duty does not and cannot affect the third person as non-contractual party, fault of the agent can only have a fictitious character. In other words, fault is determined on the basis of an "as-if" view.[37] In order to attribute fault to the obligor it is asked whether he would be held liable if he had acted the same way as the (human) agent deployed by him. This approach was designed for human agents, but does it also work for digital agents? One could consider applying it to AI systems and ask whether the obligor would be liable if he had acted like his digital agent. While a theoretical replacement might be conceivable if the activity of the system imitates a human activity (e.g. service or healthcare robots who serve some food or help patients to get up), it seems difficult where it does not perform tasks like humans or at least not according to its outward appearance [38:] Could a decision-making algorithm be subject to an "as-if" view? Here the answer is not straightforward and requires a more detailed study of the function and working procedure of the system in question.

The second approach is more "system-related" as it attempts to find an equivalent for fault in the sense of Section 278 instead of trying to adjust concepts of human agents to digital agents. It aims to interpret fault in a way that is more oriented towards the systems themselves. An idea is to stick with the "as-if" view but to compare the digital agent in question with a similar system being deployed in the same field of activity and to ask whether it would have behaved differently than the system that caused the damage.[39] However, this leads to two follow-up problems: So far there are no technical standards in form of harmonised rules for the training of AI systems what makes it challenging to find a similar system to compare them. Even if it existed, it would be difficult to implement an "as-if" view due to their individual learning abilities.[40]

3. Other discussion parameters

Next to the investigation of some selected criterions of Section 278 other discussions parameters have to be addressed in order to answer the question of applicability raised above. This involves, for instance, the analysis of alternative legal instruments to cover the identified liability gaps in contractual relations. One could, like some argue, develop broader duties of care to handle those new cases. But besides the fact that the nearly independent performance of tasks is just the innovative part of the systems, it will be difficult to keep them

[36]P. Buck, 'Wissen und juristische Person', (Tübingen: Mohr Siebeck 2001), p.34.
[37]P. Hacker, 'Verhaltens- und Wissenszurechnung beim Einsatz von Künstlicher Intelligenz' [2018] 3 RW Rechtswissenschaft, p. 262.
[38]J. Heuer-James, K. Chibanguza, B. Stücke, 'Industrie 4.0 – vertrags- und haftungsrechtliche Fragenstellungen', [2018] Betriebsberater, p. 2830.
[39]J. Günther, 'Embodied Robots – Zeit für eine rechtliche Neubewertung' in M. Gruber/ J. Bung/ S. Ziemann, 'Autonome Automaten: Künstliche und artifizielle Agenten in der technisierten Gesellschaft, (Berlin: 2014), p. 164.
[40]P. Hacker, 'Verhaltens- und Wissenszurechnung beim Einsatz von Künstlicher Intelligenz' [2018] 3 RW Rechtswissenschaft, p. 264.

on a reasonable level and to determine their extend. Another discussion parameter will comprise an economic view. It needs to be discussed on whether treating systems as agents would create an economic incentive to deploy them. As Section 278 has a sort of equivalent[41] in tort law the possible implications on the relations of the standards also have to be considered. Furthermore, the investigation will have a look on the approaches in other EU member states and outline how their contract law is able to cope with risks of autonomous systems.

Conclusions

Law has always been challenged by the pace of technology change. The basic questions in this context are not new but have to be discussed anew. Concerning AI systems, this involves identifying and examining key standards in each legal framework as part of a general review on existing rules. This also means to develop and indicate new interpretations of terms which used to be exclusively reserved for human beings. This paper tried to give an example of how a profound investigation on a standard would need to look like. It advocates to open up traditional concepts for AI systems with a certain degree of autonomous and cognitive features based on functional approaches. However, it showed that even when applying functional approaches there remains a constant difficulty to decide on when and how AI-systems can be compared with human behaviour.

Bibliography

1. M. Kloepfer, 'Technik und Recht im wechselseitigen Werden', (Berlin: Duncker & Humblot 2002).
2. M. Ebers, S. von Lingen, 'RAILS and GRUR in Conversation with Sharad Ghandi', (26 November 2018), Robotics & AI Law Society (RAILS), https://ai-laws.org/2018/11/ai-is-the-most-profound-technology-created-by-mankind/.
3. European Parliament,'European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))', 16 Februar 2017 (27 January 2017), http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.pdf.
4. G. Teubner, 'Digitale Rechtssubjekte – Zum privatrechtlichen Status autonomer Softwareagenten' [2018] 218 Archiv für die Civilistische Praxis 155-205.
5. C. Wendelstein, 'Zur Schadenshaftung für "Erfüllungs"-Gehilfen bei Verletzungen des Integritätsinteresses' [2015] 215 Archiv für die Civilistische Praxis 70-106.
6. P. Hacker, 'Verhaltens- und Wissenszurechnung beim Einsatz von Künstlicher Intelligenz', [2018] 3 Rechtswissenschaft 243-288.
7. J. Schirmer, 'Rechtsfähige Roboter?' [2016] 13 JuristenZeitung 660-666.
8. M. Lohmann, 'Roboter als Wundertüten – eine zivilrechtliche Haftungsanalyse', [2017] 2 Aktuelle Juristische Praxis, 152-162.
9. J. Günther, 'Embodied Robots – Zeit für eine rechtliche Neubewertung' in: M. Gruber/ J. Bung/ S. Ziemann, 'Autonome Automaten: Künstliche und artifizielle Agenten in der technisierten Gesellschaft, (Berlin: 2014), 155-169.

41 Section 831 BGB regulates the 'liability for vicarious agents'.

10. G. Sartor, ‘Contracts in the Infosphere’ in: S. Grundmann: European Contract Law in the Digital Age’, (Cambridge: Intersentia 2018), 263-278.
11. U.S. Food & Drug Administration (FDA), ‘FDA permits marketing of artificial intelligence-based device to detect certain diabetes-related eye problems’, (11 April 2018), https://www.fda.gov/newsevents/newsroom/pressannouncements/ucm604357.htm.
12. M. Brunner, ‘Zum Risiko für Computerfehlleistungen bei der Abwicklung von Verträgen. Der Computer als Erfüllungsgehilfe’, (Kiel: 1970).
13. P. Buck, ‘Wissen und juristische Person’, (Tübingen: Mohr Siebeck 2001).
14. A. Matthias, ‘Automaten als Träger von Rechten’, (Berlin: Logos-Verl. 2008).
15. J. Heuer-James, K. Chibanguza, B. Stücke, ‘Industrie 4.0 – vertrags- und haftungsrechtliche Fragenstellungen’, [2018] Betriebsberater, 2819-2832.
16. H. Zech, ‘Liability for Autonomous Systems: Tackling Specific Risks of Modern IT’ in: S. Lohsse/ R. Schulze/ D. Staudenmayer, Liability for Artificial Intelligence and in the Internet of Things’, (Baden-Baden: Nomos 2019), p.187-201.
17. H. Dettling, S. Krüger, ‘Digitalisierung, Algorithmisierung und Künstliche Intelligenz im Pharmarecht, [2018] Pharmarecht, 513-522.
18. M. Wolf, ‘Schuldnerhaftung bei Automatenversagen‘ [1989] Juristische Schulung, 899-902.

ELECTRICALLY POWER-ASSISTED CYCLES (EPACs) AFTER THE EUROPEAN COMMISSION'S REFIT REVIEW AND PROPOSAL TO AMEND DIRECTIVE 2009/103/EC

Olga Shevchenko[1]

Abstract

In 21st century technological development never takes a break and progress itself is growing rapidly. The society reacts to the occurrence of new technologies, in particular while the usage of the above-stated technologies ends up in sharp conflicts. Regardless the type of technological product and the area where the latter is allocated, whenever the usage of new technologies produces a conflict it must be the case of a precise and qualitative legal regulation addressing the most accurate solution.

In 2018, after the number of changes occurred within the motor insurance sector, European Commission admitted the necessary to include electrically power assisted cycles (EPACs) within the scope of the motor third party liability regulation. The regulation of e-bikes in terms of the Motor Insurance Directive would be a wrong step at the European Union level due to the environmental, social, both human and financial resources reasons. At this stage, it is inevitably important to distinguish alternative transport, which must be accurately regulated at the European Union level from the one that shall remain untouched in terms of the legal intervention for the purposes of motor third party liability regulation.

High technologies and technological progress are not always connected with inevitable necessity to provide with the legal regulation in particular field. Instead, both human and financial resources should be concentrated on the dimension of areas where conflicts are hardly or even impossible to be solved without imperative intervention of the qualitative legal regulation.

Keywords: Electrically power assisted cycles (EPACs), motor third party liability, Motor Insurance Directive, technological development.

Introduction

During the recent years particular outstanding changes occurred within the motor insurance sector. Some of them should be considered as the outcomes of the legal interpretation at the European Union level, others as technological progress stimulating the development of alternative transport. Besides the ultimate aim for which alternative transport was manufactured, there is a number of inevitable connections between the products put into the free circulation at the common market and instruments seeking to regulate conflicts, which might appear as a consequence of the usage of the alternative transport. There is an

[1] Olga Shevchenko, Master degree in International and European Union Law from Vilnius University, currently a PhD candidate, Faculty of Law, Private Law department at Vilnius University. Research Interests: Private Law, Insurance Law, Artificial Intelligence (AI) and Fraud Prevention. Email: olga.shevchenko.vu@gmail.com

accurate example of motor third party liability regulation and challenges, which technological progress have brought:

1. Autonomous vehicles (AVs) and Connected autonomous vehicles (CAVs) as a classic example of the result of technological development and which are necessary to be regulated by law.
2. Electrically power assisted cycles (EPACs) is a one more example of technological progress, which nevertheless must remain untouched in terms of a legal intervention for the purposes of the motor third party liability regulation.

It is inevitably important to determine not only the legal area where technological development takes place, but there is also a necessity to invest in both human and financial recourses in order to provide with the legal regulation of the concerned matter. Accordingly, the sector which consists of the AVs and CAVs entering the European Union market must be considered as a new developed product, which closely interacts with the range of the legal areas, such as motor third party liability regulation, product liability regulation and data protection. The analysis of the foreseeable conflicts as well as the ones which have already taken place might occur and it leads to the conclusion that legal regulation is inevitable in terms of both AVs and CAVs entering the market.

Motor Insurance Directive (MID)[2] addresses the uniform regulation of the motor third party liability (MTPL) within the European Union. Despite the number of developments performed in that area, there are still particular uncertainties existing within the regulation of motor third party liability among different member states. Whenever there is a claim for an uncertain regulation under the European Union legal act, national judicial authorities might refer to the Court of Justice of the European Union (hereinafter CJEU) bringing a disputable issue for further interpretation. Following the above-stated procedure, the Court of Justice of the European Union provided with an absolutely new interpretation of a concept 'vehicle' for the purposes of the Motor Insurance Directive within its Judgment *Damijan Vnuk v Zavarovalnica Triglav d.d. (Vnuk)*[3].

Vnuk judgment should be considered to be a breakpoint of the previous Motor Insurance Directive application. The judgment has changed the essential terms of the MID broadening the scope of the 'vehicle' and 'use of a vehicle'. Following the *Vnuk* judgment in particular, the broadened scope of a 'vehicle', European Commission provided with the Inception Impact Assessment (hereinafter REFIT review)4 addressing upcoming and necessary re-consideration of the Motor Insurance Directive and also including electrically power assisted cycles (EPACs) within the scope of a 'vehicle' for the purposes of the MID. It must be admitted that EPACs do not provoke any conflicts (oppositely to the AVs and CAVs) that would address the necessity to proceed with the legal regulation of the concerned issue at a new level, such as motor third partly liability regulation. Coming back to the classic laws which have been qualitatively developed within the last decades, it should be noticed that all conflicts which have already taken place and the ones foreseeable in future including the interaction with the electrically power assisted cycles are the subject to be regulated by civil tort law (in terms of a domestic law of each member state).

[2] European Parliament and Council Directive (EC) 2009/103 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability [2009] OJ L 263.
[3] Damijan Vnuk v Zavarovalnica Triglav d.d., Case C-162/13 [2014] ECLI:EU:C:2014:2146.
[4] European Commission Inception Impact Assessment 'REFIT review of the Motor Insurance Directive' [2017[Q4 2017 Ref. Ares/2017/3714481.

Bearing in mind a divergent view upon the technologies which are entering the market, there is a necessity (1) to provide with the outside of the scope of the Motor Insurance Directive regulatory solution with regard to the electrically power assisted cycles (EPACs) as a product of technological development. It is also essential (2) to provide with the possible outcomes which might occur as a consequence of EPACs' direct inclusion within the scope of a 'vehicle' for the purposes of the Motor Insurance Directive.

1. Inclusion of the EPACs into the scope of a 'vehicle'[5]: existing risks

The European Cyclists' Federation (hereinafter ECF) provided with its ECF Position Paper on Motor Vehicle Insurance Directive. It[6] states that within the REFIT review the European Commission should exclude electrically power assisted cycles (EPACs) from the scope of the 'vehicle' for the purposes of the Motor Insurance Directive for a number of reasons, including the fact that EPACs are not motorized vehicles, since they are operated without constant power, by means of no pedal or power. Moreover, the direct inclusion of EPACs within the scope of a 'vehicle' for the purposes of the MID will provide with the sufficient impact on the decrease of the number of cyclists, whereas might affect both environmental and health issues.

In accordance with the European Cyclists' Federation Paper, the inclusion of the EPACs into the scope of the motor third party liability regulation will cause "[b]urdens on regulatory authorities, confusion amongst millions of riders, and a patchwork of regulations and rules across the EU".[7] Moreover, the majority of e-bikers possess either personal or travel insurance, which might arise the double-compensation cases and even fraudulent acts towards the reception of double-indemnification. The inclusion of the EPACs will require to amend not only the Motor Insurance Directive itself, but also to establish a new act guiding the member states in the concerned subject-matter. Besides, it will require from competent bodies of the member states to fully re-consider a motor insurance sector.

In May 2018, European Commission provided with the Proposal (hereinafter Proposal)[8] to amend Directive 20019/103/EC as a consequence of the *Vnuk* judgment along with the further *Rodrigues de Andrade* C-514/16[9] and *Torreiro* C-334/16[10] cases clarifying

[5] This statement shall be considered as inclusion of the electrically power-assisted cycles into the scope of a 'vehicle' for the purposes of the Motor Insurance Directive.

[6] C. Woolsgrove, European Cyclists' Federation 'ECF Position Paper on Motor Vehicle Insurance Directive' [2017]. Retrieved August 19, 2018 from <https://www.google.lt/url?sa=t&rct=j7q=7esrc=s7source=web&cd=107ved=0ahUKEwiTwDetcPYAhVIKyw KHRCEAW0QFghxMAk7url=https%3A52F52Fecf.com%2Fsite%2Fecf.com%2Ffiles%2FInsurance%2520Position%2520Paper_2017_final%2520draft.docx&usg=AOvVaw2Ke4K1v6kQnjS7yj6RZiai>.

[7] C. Woolsgrove, European Cyclists' Federation 'ECF Position Paper on Motor Vehicle Insurance Directive' [2017]. Retrieved August 19, 2018 from <https://www.google.lt/url?sa=t&rct=j7q=7esrc=s7source=web&cd=107ved=0ahUKEwiTwDetcPYAhVIKyw KHRCEAW0QFghxMAk7url=https%3A52F52Fecf.com%2Fsite%2Fecf.com%2Ffiles%2FInsurance%2520Position%2520Paper_2017_final%2520draft.docx&usg=AOvVaw2Ke4K1v6kQnjS7yj6RZiai>.

[8] European Commission Proposal for a Directive of the European Parliament and of the Council amending Directive 2009/103/EC of the European Parliament and the Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to ensure against such liability [2018] COM 336 final.

[9] Isabel Maria Pinheiro Vieira Rodrigues de Andrade, Fausto da Silva Rodrigues de Andrade v José Manuel Proença Salvador, Crédito Agrícola Seguros — Companhia de Seguros de Ramos Reais SA, Jorge Oliveira Pinto Case C-514/16 [2017] ECLI:EU:C:2017:908.

the scope of a 'vehicle' and 'use of a vehicle' for the purposes of the Directive. Analysing the Proposal, it becomes clear that the empowered institution added only Article 1a, the so-called 'use of a vehicle', leaving the shield for further uncertainties, having broadened the scope of a 'vehicle' itself.[11]

In case European Commission insists on the EPACs inclusion into the scope of a 'vehicle' for the purposes of the Motor Insurance Directive in the light of the CJEU practice in future, all e-bikes within the European Union territory without compulsory insurance might become illegal. ECF states that such a regulation might become a huge error having its effect on a healthy, naturally friendly class of transport, even though European Commission stated that there will be no effect in respect to the environmental and health consequences. Therefore, ECF is seeking to keep EPACs out of scope of the 'vehicle' for the purposes of the Motor Insurance Directive having a maximum continuous rated power of less than or 250 W in accordance with the Regulation 168/2013[12].

For instance, in the light of the broadened scope of a 'vehicle' in the *Vnuk* judgment, the UK government, within the REFIT review[13] of the Motor Insurance Directive, has insisted on the omission of the electric bicycle as a class of vehicles, since in no way an electric motor device in the absence of an engine and without being mechanically propelled can be treated as a vehicle. Naturally, the necessity of obliging cyclists to pay *premium* in terms of compulsory motor third party liability insurance would break a domestic policy which promotes the development of this class of alternative transport instead of a classic vehicle (passenger car).

The ECF pointed out that since the EPACs had already been excluded from the European Community Motor Vehicle Type Approval in accordance with the Directive 2007/46/EC[14], thus, it is another reason why it is imperative to keep the one out of the scope of the 'vehicle' for the purposes of motor third party liability regulation. E-bike is a subject included into the bicycle classification in the majority of the European Union member states, whereas such an alternative transport is named as 'a pedal cycle' instead of 'a vehicle', and the rider is called 'a cyclist', but not 'a driver'.

It has to be said that in order to make a firm decision whether to include EPACs into the scope of the motor third party liability regulation or to keep the previous status of e-bikes (as a class of alternative transport out of scope of a 'vehicle'), the consequences of road collisions must be analysed at first. As an outcome of the regular collision involving a vehicle and an e-bike, a rider will be seriously injured in nine cases out of ten, while the driver of a passenger car might suffer light injuries or none at all. In case an e-bike is involved into a

---

[10] José Luís Núñez Torreiro v AIG Europe Limited, Sucursal en España and Unión Española de Entidades Aseguradoras y Reaseguradoras (Unespa) Case C-334/16 [2017] ECLI:EU:C:2017:455.

[11] This statement shall be considered strictly within the frames of the European Commission Proposal without prejudice to further frameworks established after the Proposal.

[12] European Parliament and Council Regulation (EU) 168/2013 on the approval and market surveillance of two- or three-wheel vehicles and quadricycles [2013] OJ L 60.

[13] Road Safety, Standards & Services Director B. Rimmington, 'REFIT review of the Motor Insurance Directive' [2017] (ARES 2017) 3714481, Retrieved September 15, 2018 from <https://www.google.lt/url?sa=t&rct=j&q=7esrc=s7source=wev7cd=27ved=0ahUKEwjRyuHOiL_YAhUC66QKHaQHBAgQFggvMAE&url=http%3A%2F%2Fec.europa.eu%2Finfo%2Flaw%2Fbetter-regulation%2Ffeedback%2F6729%2Fattachment%2F090166e5b48b83b1_cs&usg=AOvVaw0EZAiOOp4Nx_CVZH1fcJ>

[14] European Parliament and Council Directive (EC) 2007/46 establishing a framework for the approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles (Framework Directive) [2007] OJ L 263.

collision with a heavy truck, the former might have injuries incompatible with life, while a truck's driver, perhaps, will not have any personal injuries at all. For instance, in accordance with the statistics data published on the UK governmental database portal, per billion vehicle miles, 1,160 pedal cyclists are killed or seriously injured, in comparison to 25 car drivers.[15] Bearing in mind the above-stated statistics and the data addressing the accidents with the participating of classical cyclists, it has to be said that the collisions involving e-bikes might cause even harder injuries due to the higher speed EPACs operate. It appears that an e-bike rider shall be the subject of additional safeguard coverage rather than a policyholder that must not just keep themselves safe, but to monetary disbenefit from the established policy. Additional safeguard measures minimizing the number of fatal crashes including riders should be established. While it is an easier aspect with the classic cycles in terms of the establishing of additional side roads suitable for riders, the e-bikes roads should be considered as the ones, which are more complicated to achieve. Side roads for EPACs must be free of pedestrians at any time in order to avoid possible injuries which might occur in case an e-bike rider collides with a pedestrian. Bearing in mind the speed limits integrated into the e-bikes technology, roads illuminating possible contacts with either pedestrians or classic cyclists shall be constructed.

Technological development inquires additional supervision and decisions in particular cases. EPACs and their inclusion into a free circulation on the common market must be considered as a new duty to be put on each member state in order to ensure a safety level of riding. Direct inclusion of the electrically power assisted cycles into the scope of a 'vehicle' for the purposes of the Motor Insurance Directive will not solve initial danger to riders' health and life.

2. Foreseeable consequences

Electrically power assisted cycles, as a class of alternative transport, are not included into the scope of a 'vehicle' for the purposes of the Directive 2006/126/EC[16] on driver licenses. For the purposes of the Directive 2006/126/EC the 'power-driven vehicle' is "[a]ny self-propelled vehicle running on a road under its own power, other than a rail-borne vehicle"[17], which is create to some extent a threshold for particular classes of alternative transport (such as EPACs that are not self-propelled under their own power), which cannot be covered for the purposes of the above-mentioned Directive. It should be emphasized that EPACs have maximum of 250 W of power limitation, that is, as a matter of fact, might be achieved by riders operating a classic bicycle without any additional assistance. The European Committee for Standardization (CEN)[18] confirmed that an electrically power assisted cycle is a class of alternative transport with the pedal assist that is accelerating up to 25 km/h and it must be considered as a bicycle. At the same time bicycles were never considered as a vehicle neither within the REFIT review nor in the light of the CJEU jurisprudence. Oppositely, bicycles as a type of transport and cyclists themselves are

[15] United Kingdom Department for Transport statistical data on casualties involved reported road accident (RAS30) 'RAS30070: Relative risk of different forms of transport' [2016]. Retrieved February 10, 2019 from <www.gov.uk/goverment/statistical-data-sets/ras30-reported-casualities-in-road-accidents>

[16] European Parliament and Council Directive (EC) 2006/126 on driver licenses [2006] OJ L 403.

[17] European Parliament and Council Directive <…>.

[18] European Committee for Standardization, Cycles – Electrically power assisted cycles – EPAC Bicycles [2017] EN 15194:2017, 00333036. Retrieved September 20, 2018 from <https://standards.cen.eu/dyn/www/f?p=204:110:0::::FSP_PROJECT:39396&cs=16DF8E47F41EAC1DBC86BEAA129F6C67C>

considered as highly protected subjects under both valid motor third partly liability law and jurisprudence addressing road traffic collisions.

In the majority[19] of the European Union member states cyclists are considered as a special category of victims (or privileged)[20], hence entitled to a higher protection level (in some cases unless the gross negligence is proved). For instance, in accordance with the strict liability rules in France, in case a road traffic collision involves a cyclist, the latter will be always entitled to receive a full compensation with regard to the non-pecuniary losses only. Even though cyclist's liability might be proved, the latter will be still a subject who receives a full compensation with regard to the personal injuries claim. However, in case the third party was able to prove that a cyclist intended to commit a suicide (or has committed suicide), the first party shall be exempt from any liability at all. It has to be said that a French example provides with one of the stickiest rules with regard to the motorised transport involved into the road traffic collision with a cyclist. At the same time in Germany, in case a cyclist found liable for causing a traffic accident, the former is still entitled to claim for a compensation. However, the amount might also vary with regard to the negligence/gross negligence level, e.g. overtaking manoeuvre (1/3) performed by cyclist during the left turn manoeuvre (2/3) performed by a car driver.[21] It has to be said that within the above-mentioned example of the German court practice, the District Court (Landgericht Saarbrücken) has also confirmed that e-bikes must be considered as bicycles in a legal sense and in no way to be classified as motor vehicles.

In the Netherlands, strict liability is integrated within the Article 185[22] of the *Wegenverkeerswet*, where it has to be said that 'strict liability' as the term does not apply; instead it is more likely to be interpreted as a 'duty to cover losses sustained by cyclist'. The mechanism does not automatically put the motorised driver 100% liable, as a threshold procedure applies. In case a cyclist made no mistake, the liability will pass to a motorised driver in full. However if the first party proves that a cyclist made a mistake, the liability might be 50% split. In case the driver of a vehicle did not commit any mistake, the liability is still can be 50% split if a cyclist is over the age of 14. Otherwise, (when a cyclist is under the age of 14) the driver of a vehicle will be held 100% liable for the accident, unless the former is able to prove that a cyclist under the age of 14 caused the collision on purpose. Naturally, appears the issue whether the cyclist of the electrically power assisted cycle will be equalized to the driver of a vehicle; and in this case whether it shall be considered as annulment of the previously existed privileges to cyclists (French, German and Dutch

[19] Such member states as France, the Netherlands, Belgium, Germany, Denmark, Sweden and Norway has introduced strict liability system along with the privileges to both cyclists and pedestrians at the high level. The rest of the European Union member states have also integrated particular strict liability rules within the domestic law, however at the lower level. The only Romania, Cyprus, Malta, Ireland and United Kingdom have not integrated strict liability system with regard to the incidents involving cyclists into the domestic law.

[20] 'Special categories of victim' also indicated within the Motor Insurance Directive in its Article 12 with the same title 'special categories of victim'. In accordance with the Article 12 (3) "[T]he insurance referred to in Article 3 shall cover personal injuries and damages to property suffered by pedestrians, cyclists and other non-motorised users of the roads who, as a consequence of an accident in which a motor vehicle is involved, are entitled to compensation in accordance with national civil law". Accordingly, cyclists are granted the status of special category of victims in the light of both Motor Insurance Directive and domestic motor third party liability law of the majority of the EU member states.

[21] Keine Einstufung von E-Bikes als Kraftfahrzeug, Das Landgericht Saarbrücken, Urteil vom 15.11.2013 - 13 S 107/13.

[22] Artikel 185, Hoofdstuk XII. Civiele aansprakelijkheid. Wet van 21 april 1994, houdende vervanging van de Wegenverkeerswet (Wegenverkeerswet 1994 WVW). BWBR0006622.

examples) or we shall consider e-bikes cyclists totally divergent from the cyclists of the classic bicycles. In terms of the first case scenario, cyclists will be removed from the provisions with regard to the special victims' category. In such a case, it shall be considered as a worsen regulation with regard to the sensitive category of victims. In the light of the second case scenario, where cyclists of the electrically power assisted cycles are strictly distinguished from the cyclists of the classical bicycles, it shall be considered as a discriminatory measurement.

The ECF has provided with the statement that European Commission is now challenging the natural choice of the individuals to travel with a cycle instead of a classic vehicle (passenger car). European Commission's position in this matter shall be considered as a will to establish imperative *premium* to be paid for the compulsory motor third party liability insurance. Bearing in mind that there are millions of EPACs, which have already been sold throughout the European Union, it might also result in a significant non-compliance causing a huge range of incidents involving uninsured transport. In general, the imposition of an obligation to purchase an insurance policy for such classes of alternative transport as e-bikes in the nearest future will lead to the decision to insure also classic bicycles.

Naturally, people are favouring bicycles instead of vehicles while travelling short distances. Accordingly, individuals will prefer a classic vehicle (passenger car) instead of an e-bike for a long distance trip. In case European Commission (or any other empowered European Union institution) ever again in future will insist on the imposition of compulsory insurance for classes of alternative transport such as e-bikes, individuals would probably prefer a vehicle to a bicycle in order to avoid double charges for insurance. Despite the fact that insurance *premium* for an e-bike is hardly to be as much expensive as for the rest of the vehicles, individuals will be willing to avoid paying twice. In case individuals changed alternative transport, such as an e-bike to a vehicle, the number of vehicles on roads would obviously increase bringing new numbers into the road traffic collisions' statistics.

Only two member states such as Malta and Northern Ireland have put strict restrictions on the usage of the electrically power assisted cycles so far providing for the burden to purchase compulsory insurance. Thus, we can observe the outcome, namely a huge decrease in the EPACs sales from 84% in 2012 down to 15% in 2015.[23] That can be foreseen as a future of the rest of the European Union member states in case a class of alternative transport (EPACs) will be included into the scope of a 'vehicle' for the purposes of the Motor Insurance Directive.

Inclusion of e-bikes into the scope of a motor third party liability regulation at the European Union level might invoke the burden of additional administrative actions to be taken at the domestic level, as well as increase in bureaucracy. Here, Germany is in the possession of approximately 3,6 million of the electrically power assisted cycles. In accordance with the statistics data[24] that was 40 % of EU e-bikes up to 2015 while 2016

[23] C. Woolsgrove, European Cyclists' Federation 'ECF Position Paper on Motor Vehicle Insurance Directive' [2017]. Retrieved August 19, 2018 from <https://www.google.lt/url?sa=t&rct=j7q=7esrc=s7source=web&cd=107ved=0ahUKEwiTwDetcPYAhVIKyw KHRCEAW0QFghxMAk7url=https%3A52F52Fecf.com%2Fsite%2Fecf.com%2Ffiles%2FInsurance%2520Position%2520Paper_2017_final%2520draft.docx&usg=AOvVaw2Ke4K1v6kQnjS7yj6RZiai>

[24] Bicycle industry in Europe, Vehicles & Road Traffic, Figure 'Distribution of electrically powered assisted cycle (EPAC) sales in the European Union (EU-28) in 2015 by country' [2015] Retrieved October 3, 2018 from <https://www.statista.com/statistics/5 61566/epac-sales-in-the-european-union-eu-28-by-country/>

sales data[25] shows that 605 000 EPACs were sold up to July 2017 keeping Germany on the first position with the total 36%. The inclusion of electrically power assisted cycles into the scope of a 'vehicle' would mean the necessity to register and license all cycles circulating within the state, which might lead to the burden of an additional huge amount of both material and human resources.

Each step at the European Union level requires a particular number of both human and financial recourses within each member state must reflect its high justification (for instance, proofs that particular legal requirements might decrease the number of further undercompensated victims of road traffic collisions). Analysing the case with regard to the inclusion of the electrically power assisted cycles into the scope of a 'vehicle' for the purposes of the motor third party liability regulation, it has to be said that no justification has been found.

In the light of the feedbacks[26] published within the official European Commission's website it became clear that the majority of the member states through particular representatives have expressed their negative position and firm disagreement with regard to the inclusion of e-bikes into the scope of a 'vehicle' for the purposes of the Motor Insurance Directive. Until this day, in particular 14 October 2018, there are 530[27] feedbacks available within the field addressing REFIT review in general, where 82 feedbacks do not concern electrically power assisted cycles, 3 respondents provided with the consent position, other 2 (respondents from Belgium and Finland) agreed upon the *status quo* approach to develop further regulation and the rest 443 respondents[28] are strongly against the inclusion of the e-bikes into the scope of the motor third party liability regulation at the European Union level.

For instance, French Insurance Federation provided with its consent with regard to the inclusion of all new electric classes of alternative transport into the scope of a 'vehicle', hence within the motor third party liability regulation in terms of the Motor Insurance Directive. However, the one has reminded European Commission that a particular class of transport, such as 'pedelecs'[29] cannot be considered as a vehicle for the purposes of the Motor Insurance Directive. Here, French Insurance Federation has called to a strict necessity to distinguish 'pedelecs' from the electric class of alternative transport.

On the other hand, Association of Mutual Insurers and Insurance Cooperatives in Europe (AMICE) Belgium provided with the recommendation addressing European Commission to follow *status quo* approach with regard to all electrically assisted transport, including electrically power assisted cycles. Here, such an approach might be the case when it does not concern a victim's right to compensation. Since motor insurance liability aimed to

[25] Confederation of the European Bicycle Industry (CONEBI), 'European Bicycle Market. 2017 Edition. Industry & Market Profile (2016 statistics)' [2017]. Retrieved October 10, 2018 from <http://asociacionambe.es/wp-content/uploads/2014/12/Europea n-Bicycle-Industry-and-Market-Profiles-2017-with-2016-data..pdf>

[26] European Commission's website-Feedbacks: 'REFIT review of the Motor Insurance Directive' [2018]. Retrieved October 14, 2018 <from https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3714481/feedback_en?p_id=237387>

[27] Chart of feedbacks sorted by topic and expressing either "for" or "against" position of respondents. Feedbacks are taken from European Commission's website – Feedback received on: REFIT review of the Motor Insurance Directive.

[28] Respondents from the EU member states: France, Germany, United Kingdom, The Netherlands, Sweden, Czech Republic, Bulgaria, Hungary, Spain, Italy, Portugal, Belgium, Luxembourg, Greece, Croatia, Malta, Switzerland, Finland, Slovakia, Slovenia, Poland, Austria, Ireland, Lithuania, Latvia, Estonia, Romania.

[29] French Insurance Federation 'Position Paper referring to REFIT Review of the Motor Insurance Directive' [2018] EU Transparency Register No. 5149794935-37.

ensure the right to compensation itself, *status quo* approach might only worsen victims' status provoking huge delays while awaiting for a particular solution. Bearing in mind that power cycles belong to the same class of vehicles as motorcycles, the Motor Insurers' Centre of Finland together with the Finance Finland believe that power cycles shall be included into the scope of a 'vehicle' for the purposes of the Motor Insurance Directive, however, power cycles[30] should be strictly distinguished from the pedal assisted cycles[31].

3. E-bikes regulation at the European Union level

After precise evaluation of the European Commission's Proposal, on 28th January (2019) European Parliament has provided with the Report (hereinafter Report)[32] on the proposal amending Directive 2009/103/EC. In accordance with the Amendment 23[33] of the Report, electrically power assisted cycles (or e-bikes), as well as other classes of alternative transport should be considered as outside the scope of a 'vehicle' for the purposes of the Motor Insurance Directive as long as those remain outside the scope of the Regulation (EU) 2018/858[34], Regulation (EU) No 167/2013[35] or Regulation (EU) No 168/2013. European Parliament justifies the decision taken with regard to the electrically power assisted cycles as a class of alternative transport which serves for the purposes of better environmental conditions. It has to be said that European Parliament also justified the decision, as e-bikes are hardly to cause significant losses in terms of both material damages and personal injuries. In the light of the drafted Recital 3 (a)[36] it shall be considered disproportionate to impose additional monetary burden on e-bikes riders. However, it has to be noticed that European Parliament keeps identifying electrically power assisted cycles as "some motor vehicles".

It should be mentioned that electrically power assisted cycles shall be ultimately finalized as a subject which can not be related to the motor third party liability regulation. Despite the fact European Parliament considered the previous researches in the concerned

[30] Power cycles that are equal or less power rated than 250 W with the speed that does not exceed 25 km/h.

[31] Motor Insurers' Centre of Finland 'Joint statement of Finnish Motor Insurers' Centre and Finance Finland regarding Proposal for a Directive amending Directive 2009/103/EC' Feedback reference F13288 [2018] Transparency register number 7328496842-09.

[32] European Parliament Report on the proposal for a directive of the European Parliament and of the Council amending Directive 2009/103/EC of the European Parliament and the Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to ensure against such liability [2018] COM/2018/0336.

[33] European Parliament Report <…>, Article 2 1(a) "[T]his Directive shall only apply to the vehicles covered by Regulation (EU) 2018/858, Regulation (EU) No 167/2013 or Regulation (EU) No 168/2013. This Directive shall not apply to vehicles that are intended exclusively for use in the context of participation in a competitive sport activity, or in related sport activities, within a closed area".

[34] European Parliament and the Council Regulation (EU) 2018/858 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC [2018] OJ L 151.

[35] European Parliament and the Council Regulation (EU) No 167/2013 on the approval and market surveillance of agricultural and forestry vehicles [2013] OJ L 60.

[36] European Parliament Report on the proposal for a directive of the European Parliament and of the Council amending Directive 2009/103/EC of the European Parliament and the Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to ensure against such liability [2018] COM/2018/0336. Recital 3 (a) "[S]ome motor vehicles such as electric bicycles and segweys are smaller and are therefore less likely to cause significant damage to persons or property than others…".

subject matter, hence placed the e-bikes outside the scope of the Motor Insurance Directive, it does not necessarily mean that this issue will never appear again. Accordingly, this Contribution serves for the purposes to put a strict boarder between the motor third party liability and electrically power assisted cycles, especially in terms of new developments such as AVs and CAVs requiring all attention of the law-making power at motor insurance sector have been placed in the common market.

While confirming that an e-bike shall not be treated as a 'vehicle' for the purposes of the Motor Insurance Directive, European Parliament has left the unsolved issue with regard to the further safeguard measures in that concern. It is not enough just to keep the alternative transport outside the scope of the motor third party liability coverage. Instead, it is the case where particular supplementary actions, not necessarily directly connected to the regulatory measures, have to be taken. The inclusion of electrically power assisted cycles within free market circulation should be treated as a technological development, which must be assisted along with the supplementary actions. Those steps shall ensure a safe usage of e-bikes for all riders, drivers and pedestrians. Seeking to minimize both pecuniary and non-pecuniary losses sustained by riders, drivers or pedestrians, it is important to keep regular traffic away from e-bikes (such as construction of a separate tracks including particular upgrades for the ones which have already been constructed for classic bicycles). Having been analysed in the previous sections for the purposes of this contribution, e-bikes shall be granted not just separate status of a class of alternative transport that falls outside the scope of a 'vehicle' for the purposes of motor third party liability regulation, but shall be supported by integrated safeguard measures, which might prevent traffic collisions.

Keeping EPACs away from both traffic roads and sidewalks does not solve the issue with regard to the particular accidents, which might take a place when other classes of alternative transport intersect. For instance, the rapid growth in electric scooters sales in the common market has already changed the traffic in the majority of the European Union member states. Electric scooters are fast enough and it also makes them a class of transport difficult to brake on time, which finally might cause losses. At the same time, electric scooters are small enough and it becomes rather difficult to notice them on time in order to prevent a collision. It must be admitted that Lithuania is one of the examples of the countries where sales in an electric scooters sector have grown significantly during the last years. As a result, the particular social interrogations have been made in order to find out whether cyclists consider electric scooters to be an obstacle or not. In accordance with the statements prepared by the respondents, electric scooters shall be considered as a class of alternative transport challenging a current situation between public traffic and side walks. Electric scooters have a negative effect on the cyclists usage of tracks as they are operated on high speeds (scale addressing tracks for classes of alternative transport only), hence in case of a collision the losses are usually more significant in comparison to the ones caused by an accident between two cyclists. Taking into account the size of electric scooters it is usual that cyclists are unlikely to notice them in order to avoid a collision. Accordingly, keeping electrically power assisted cycles in the right place (simply away from both drivers and pedestrians) cannot be considered as a safety measures solution, instead it is necessary to ensure safety usage of all classes of alternative transport in order to prevent collisions while such means of transport intersect. Due to the above-mentioned reason new tracks which are wider and which will serve a larger number of users, for classes of alternative transport shall be either constructed or upgraded.

It has to be said that years ago people could hardly imagine separated tracks serving for the purposes of cyclists' safety rides. It might be a case that current developments have led to the same necessity to introduce new actions with regard to the safety measures.

Technological progress does not necessarily mean an absence of additional actions to serve for the purposes of that particular progress. Hence, in case the particular product of technological progress enters the marker, the society must be ensured that all safety measures are also guaranteed. Otherwise, it might be a claim that the particular product of technological development is not worth entering into a free circulation in the common market. Taking into account the overall progress we have reached in 21 century, legal intervention cannot remain as classic as it used to be. It is imperative to integrate non-standard decisions of regulation for the purposes of non- standard developments. Accordingly, considering its status as a class of alternative transport, EPAC requires alternative actions for the purposes of a qualitative maintenance of technological progress.

Conclusions

High technologies and technological progress itself do not always mean inevitable necessity to provide with the legal regulation in a particular field. Instead, both human and financial resources should be concentrated on the dimension where conflicts are hardly or even impossible to be solved without the necessary intervention of the qualitative legal regulation.

Oppositely to both European Commission's REFIT review and Proposal, electrically power assisted cycles (EPACs or e-bikes) must remain outside the scope of a 'vehicle' for the purposes of the Motor Insurance Directive seeking to avoid further member states losses of both material and human resources, commercial insurance collapse as well as social, environmental, bureaucratic outcomes.

The tracks which serve the classes of alternative transport shall be either constructed or upgraded illuminating possible intersects with either pedestrians or vehicles. Once neither public traffic roads nor sidewalks are suitable for electrically power assisted cycles (as well as for other classes of alternative transport), there is a top agenda to proceed with the construction of additional tracks that shall ensure safety measures and minimize the number of injuries and fatal collisions.

Technological development inquires additional supervision and decisions in particular cases. EPACs and the inclusion of such a class of alternative transport into a free circulation must be considered as a new duty to be put on each member state in order to ensure a safe level of riding. Although the inclusion of e-bikes into the scope of a 'vehicle' for the purposes of the Motor Insurance Directive will not decrease initial danger to riders' health and life, the maintenance of particular safety measures will do.

Taking into account the overall progress we have reached in 21 century, legal intervention cannot remain as classic as it used to be. It is imperative to integrate non-standard decisions of regulation for the purposes of non- standard developments. Electrically power assisted cycles, as a class of alternative transport, requires alternative actions for the purposes of a qualitative maintenance of technological progress.

Bibliography

1. Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles

and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC. OJ L 151.

2. Regulation (EU) No 167/2013 of the European Parliament and of the Council of 5 February 2013 on the approval and market surveillance of agricultural and forestry vehicles. OJ L 60.

3. Regulation (EU) No 168/2013 of the European Parliament and of the Council of 15 January 2013 on the approval and market surveillance of two- or three-wheel vehicles and quadricycles. OJ L 60.

4. Directive 2009/103/EC of the European Parliament and of the Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability. OJ L 263.

5. Directive 2007/46/EC of the European Parliament and of the Council of 5th September 2007 establishing a framework for the approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles (Framework Directive). OJ L 263.

6. Directive 2006/126/EC of the European Parliament and of the Council of 20 December 2006 on driver licenses. OJ L 403.

7. European Parliament Report on the proposal for a directive of the European Parliament and of the Council amending Directive 2009/103/EC of the European Parliament and the Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to ensure against such liability. COM/2018/0336.

8. European Commission Proposal for a Directive of the European Parliament and of the Council amending Directive 2009/103/EC of the European Parliament and the Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to ensure against such liability. Brussels [2018] COM(2018) 336 final.

9. European Commission. Inception Impact Assessment. REFIT review of the Motor Insurance Directive [2017] Q4 2017. Ref. Ares(2017)3714481.

10. French Insurance Federation. Position Paper referring to REFIT Review of the Motor Insurance Directive. EU Transparency Register No. 5149794935-37 of 24 July 2018.

11. Motor Insurers' Centre of Finland. Joint statement of Finnish Motor Insurers' Centre and Finance Finland regarding Proposal for a Directive amending Directive 2009/103/EC. Feedback reference F13288. Transparency register number 7328496842-09.

12. Wet van 21 april 1994, houdende vervanging van de Wegenverkeerswet (Wegenverkeerswet 1994 WVW). BWBR0006622.

13. *José Luís Núñez Torreiro v AIG Europe Limited, Sucursal en España and Unión Española de Entidades Aseguradoras y Reaseguradoras (Unespa).* Judgment of the Court (Sixth Chamber) of 20 December 2017, Case No. C – 334/16, ECLI:EU:C:2017:455.

14. *Isabel Maria Pinheiro Vieira Rodrigues de Andrade, Fausto da Silva Rodrigues de Andrade v José Manuel Proença Salvador, Crédito Agrícola Seguros — Companhia de Seguros de Ramos Reais SA, Jorge Oliveira Pinto*. Judgment of the Court (Grand Chamber) of 28 November 2017, Case No. C – 514/16, ECLI:EU:C:2017:908.

15. *Damijan Vnuk v Zavarovalnica Triglav d.d.* Judgment of the Court (Third Chamber) of 4 September 2014, Case No. C – 162/13, ECLI:EU:C:2014:2146.

16. *Keine Einstufung von E-Bikes als KraftfahrzeugDas*, Landgericht Saarbrücken, Urteil vom 15.11.2013 - 13 S 107/13.

17. C. Woolsgrove, European Cyclists' Federation 'ECF Position Paper on Motor Vehicle Insurance Directive' [2017]. Retrieved August 19, 2018 from https://www.google.lt/url?sa=t&rct=j7q=7esrc =s7source=web&cd=107ved=0ahUKEwiTwDetcPYAhVIKywKHRCEAW0QFghxMAk 7url=https%3A52F52Fecf.com%2Fsite%2Fecf.com%2Ffiles%2FInsurance%2520Po sition%2520Paper_2017_final%2520draft.docx&usg=AOvVaw2Ke4K1v6kQnjS7yj6R Ziai

18. Road Safety, Standards & Services Director B. Rimmington, 'REFIT review of the Motor Insurance Directive' [2017] (ARES 2017) 3714481, Retrieved September 15, 2018 from https://www.google.lt/url?sa=t&rct=j&q=7esrc=s7source=web7cd=27ved=0ahUKEwj RyuHOiL_YAhUC66QKHaQHBAgQFggvMAE&url=http%3A%2F%2Fec.europa.eu% 2Finfo%2Flaw%2Fbetterregulation%Ffeedback%2F6729%2Fattachment%2F090166 e5b48b83b1_cs&usg=AOvVaw0EZAiOOp4Nx_CVZH1fcJ

19. European Committee for Standardization, Cycles – Electrically power assisted cycles – EPAC Bicycles [2017], EN 15194:2017, 00333036. Retrieved September 20, 2018 from https://standards.cen.eu/dyn/www/f?p=204:110:0::::FSP_PROJECT:39396&cs=16D F8E47F41EAC1DBC86BEAA129F6C67C

20. Bicycle industry in Europe, Vehicles & Road Traffic, Figure 'Distribution of electrically powered assisted cycle (EPAC) sales in the European Union (EU-28) in 2015 by country'. Retrieved October 3, 2018 from https://www.satista.com/statistics/561566/epac-sales-in-the-european-union-eu-28-by-country/

21. Confederation of the European Bicycle Industry (CONEBI), 'European Bicycle Market. 2017 Edition. Industry & Market Profile (2016 statistics)' [2017]. Retrieved October 10, 2018 from http://asociacionambe.es/wp-content/uploads/2014/12/European-Bicyle-Industry-and-Market-Profile-2017-with-2016-data..pdf

22. United Kingdom Department for Transport statistical data on casualties involved reported road accident (RAS30). RAS30070: Relative risk of different forms of transport, Great Britain [2016] Retrieved February 10, 2019 from www.gov.uk/goverment/statistical-data-sets/ras30-reported-casualities-in-road-accidents

23. European Commission's website – Feedback received on: REFIT review of the Motor Insurance Directive. Retrieved October 14, 2018 from https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3714481/feedback_en?p_id=237387

THE ROLE OF SEMANTIC WEB IN THE MANAGEMENT OF LEGAL DATA

Victor Terekhov[1]

Abstract

Modern Web is the most important source of legal information: it contains legislative texts, case-law, doctrine, drafts and outdated laws from all over the world. The amount of such materials keeps growing with time, while their availability to wide audience presents a significant problem as it remains hard to find, process, analyze and systematize them. This leads to an 'information deficit' paradox: despite there being plenty of relevant data, it is at times impossible to make proper use of it. One of the possible solutions is the further development of Semantic Web – an extension of the current Internet structure relying on logical concepts and correlations between events, and making use of specific ontologies. The application of such technologies in the legal field may permit faster and more precise search, easier reasoning, storage and use of data as well as automatic resolution of disputes by relying on the previous case-law systematized in a machine-understandable format.

Keywords: Semantic Web, Legal Data, Linked Open Data, Legal Knowledge Interchange Format (LKIF), smart applications, e-government

Introduction

The modern World Wide Web (WWW) is a great source of information in both general and specialized fields (including the legal domain). Speaking of the latter, one may find texts of binding legal instruments, judicial cases of various jurisdictions (resolved and in progress), drafts, soft law, outdated and historic sources ranging from the *Manusmriti* and *Hammurabi Code* to the American Declaration of Independence to the present-day blockchain and eCommerce regulations, proposed amendments and, last but not least, doctrine. All of these may be united under the common term of 'legal knowledge', since it does not differentiate between the status (binding/nonbinding), jurisdiction or type of the document, but rather underlines that it contains certain information pertaining to the law.[2] Most of these materials are available worldwide in common formats and may be accessed free of charge. In fact, our generation appears to be in the best position in terms of access to legal data: relevant information is at our fingertips and does not require visiting libraries or purchasing printed

[1] PhD in Civil Procedure, Master Degree in International and EU Law Vilnius University. Currently a lecturer of European Private Law and European Civil Procedure at Vilnius University. Recent research interests include comparative law, legal technology (Legal Tech) and online dispute resolution. E-mail: victor.terekhov@tf.vu.lt

[2] P. Casanovas, N. Castellas et al. 'An Ontology-Based Decision Support System for Judges' in: 'Law, Ontologies and the Semantic Web: Channeling the Legal Information Flood' (Amsterdam, IOS Press 2008) 167.

copies of the documents. The Web is, without doubt, the largest repository of legal data,[3] and it keeps growing.

The main beneficiaries of such situation are 'law professionals': judges, arbitrators, public prosecutors, notaries, attorneys and judicial clerks, however ordinary citizens wishing to know better their rights and remedies can also make use of data stored in the Web. In fact, access to legal information is nowadays treated as a fundamental element of democracy, since, on the one hand, we do not excuse liability due to the lack of knowledge of applicable law and, on the other hand, we demand that such laws be precise and clear, so that an average individual can grasp their meaning and learn of his/her rights and obligations.[4]

The potential of the Web as a source of legal information is undisputed throughout the world. In many countries it even becomes common practice to treat publication of newly adopted statutes on an official website of the governmental institution as an official promulgation,[5] and it is hard not to see it as such since Internet tools are accessible to more citizens than paper-based newspapers or journals which were previously used for the same purpose.

At the same time, there are some problems associated with Web as a source of legal information. Firstly, with all its petabytes of data,[6] Internet presents a vast 'ocean' of water where the relevant information constitutes just a small landmass ('island'). It is not easy to find exactly what you are looking for. Secondly, the Web has a lot of 'junk files': irrelevant, broken, infected, or simply incomplete and inaccurate. That sometimes casts doubt on its ability to serve as a reliable source of legal knowledge to consult with. Professionals need an instrument of high accuracy as often the lives of other individuals depend on their reasoning, and the latter may not be arbitrary. Citizens and companies also want more clarity as to their legal status, available rights, imposed obligations and procedures to follow. That is not what they get when different web portals cannot agree on such important issues as the amount of tax to be paid, full list of the documents needed to register a company or the method used by the Border Service to count how many days an individual has spent in the country in order to obtain a right to claim permanent residence there. It is not exactly legal certainty that people want: they simply want correct answers to the questions posed, and they want them to appear within the first lines of search results in Google or Bing.

This paper tries to show what can be done within the legal domain to improve the situation. The idea behind the changes is not new – it is that of Semantic Web, which was first mentioned by Sir Tim Berners-Lee back in 1994 and stands for a virtual space where most of the tasks are performed by mutually communicating machine algorithms (software agents), while humans just rely on their work.[7] This system is based on some new and recently popularized formal languages and builds strong ontologies for its sectors of application. In the legal field the deployment of such technologies can bring faster and qualitatively better search results, automation of some comparative analysis and reasoning

[3] E. Francesconi, 'On the Future of Legal Publishing Services in the Semantic Web' [2018] 10(6) Future Internet 48.
[4] E. Francesconi and G. Peruginelli, 'Integrated Access to Legal Literature through Automated Semantic Classification' [2008] 17 Artificial Intelligence and Law 31.
[5] In that way it is treated, inter alia, in the Russian Federation, see: Federal Law no. 289-FZ [2011] http://www.consultant.ru/document/cons_doc_LAW_120715.
[6] According to Live Counter (https://www.live-counter.com/how-big-is-the-internet), at the time of preparation of this paper (14 April), the size of the Internet in Petabytes was 14.964.536 (1 petabyte = 10^{15} bytes).
[7] L. Yu, 'A Developer's Guide to the Semantic Web' (Berlin: Springer 2014) 3-5.

tasks and, to some extent, even autonomous and automatic decision-making in particular cases (fines for traffic violations, IP rights management, solution of monetary claims, etc.).

It must be observed that this paper is written from the position of the lawyer (not a computer engineer or a philologist trained to work with natural language constructions). This presupposes that the question posed by the author is 'in what way the Semantic Web can contribute to the law and the daily routine work of the lawyers with the legal sources', while answering the question of 'how exactly that may be done in terms of available programming tools' remains outside the reach of the research. Here the author cannot but note the necessity of integrated multidisciplinary approach to law in the XXI century and effective collaboration between professionals of legal, IT and (last, but not least) linguistic fields of science and practice.

1. Classic Web and its drawbacks

The first stage of the WWW evolution was marked by static information. It was based on simple pages that contained text, images and embedded videos and had their own Uniform Resource Locators (URLs) to be accessed. This was also known as Web 1.0 or 'documentary web'. Most users were consumers rather than creators of the content. At the beginning of the XXI century the mankind saw a move towards Web 2.0, the main feature of which was heavy reliance on social networks (Facebook, LinkedIn, Twitter) and open interaction between independent users. Users also started to actively generate content, which could be pictures of cats and memes, but on the other hand, scholar articles, commentaries to statutes, case analyzes and model acts.[8] At the same time the Web has become more exposed to the threat of 'fake information'.[9] If the content can be generated by anyone, you cannot immediately trust it, as you do not know the aim and motives behind the will to share that information and the fact of whether a person is acting in good faith. Thus, despite being the largest repository of information in all domains (including legal), Web cannot be trusted unconditionally, as many of the publications are not specifically checked for consistency and may be manipulated by the website owner in his own interest.[10] In some situations, it may even take place unintentionally: with purely legal issues that happens when the website contains an outdated or incomplete version of the statute, or an act matching a totally different jurisdiction. The only possible exception (when you can trust what you see) is a situation where you deal with an official page of the relevant governmental or international institution.

In most cases though the quest for finding relevant information starts with the search portal (such as Google or Bing). These services have complex searching tools that help us find and look through the documents. However, there is one major limitation – all of the searching algorithms rely on keyword matching, so that they provide you with documentary search results that contain exactly the same words and phrases you entered in the searching box.

[8] J. Breuker, P. Casanovas et al. 'The Flood, the Channels and the Dykes: Managing Legal Information in a Globalized and Digital World' in: 'Law, Ontologies and the Semantic Web: Channeling the Legal Information Flood' (Amsterdam, IOS Press 2008) 10.

[9] S. Mo Jang and J. K. Kim, 'Third Person Effects of Fake News: Fake News Regulation and Media Literacy Interventions' [2018] 80 Computers and Human Behavior 295-296.

[10] T. Bascik, 'Web sémantique: Quelles perspectives pour l'information juridique?' [2014] 19(1) Lex Electronica 27.

This is not bad when you are sure about what you are looking for. At the same time, more often you experience certain problems trying to get what you want. To begin with, words forming the keywords may be polysemic and homonymous, may have synonyms, acronyms and abbreviations or just be used with different meanings depending on the content. Thus, the words 'business', 'trader' or 'entrepreneur' are used in different EU acts on consumer protection to describe the 'stronger' party to a contractual relation. Some words, on the contrary, can be polysemantic and mean different things (e.g. 'arbitration court' in Russian law means a judicial institution that resolves disputes of economic nature between companies and/or individual entrepreneurs, but in most other states an 'arbitration' is seen as a form of alternative dispute resolution that takes place outside courts and is conducted by specialized individuals or institutions). Computer software can do little to help in clarification of the search, as it just provides a list of queries matching the data entered by the user. As S. Walter and M. Pinkal note, sometimes it is possible to use Boolean operators (AND, OR, NOR) in addition, but this again has to be done by the user.[11] In sum, we shall be very precise with our search queries, otherwise we will either get an enormous list of unwanted and irrelevant documents or an empty result.

The first of these situations leads to an 'overload' of irrelevant information in the Internet.[12] A user will get hundreds of documents with only several of them really having relevance to his query. A typical example is the search for 'appeal proceedings' where the person intends to find out their special features in civil procedure. However, the system may present in response documents that relate to criminal procedure, out-of-court dispute resolution, or the information on the correct area of law, but of totally different jurisdiction (e.g. Italy instead of France). The latter situation may occur due to several reasons. Some pages do not appear in the results as they do not match the keywords entered by the user or are used in a different form. Yet other places are hidden, being located in the deep Web or some professional network. A number of sources are totally impenetrable and untraceable – like images, audio/video files, zipped archives, databases information, scanned PDF documents.

Modern searching engines are also not very helpful when we need something beyond the mere text of the document. Lawyers, for example, may be interested in the following related information:

- Which edition of law [L] of [yy.mm.dd] was in force on [yy.mm.dd]?

- Which law would recognize the contract between the parties [A] and [B] as valid?

- Which law governs the legal status of company [A], a [LLC]?

- Which remedies against a [businessman] may a [consumer] use in [country A]?

- Which laws are changed or annulled by the law [X]?

As you may imagine, it is hardly possible to ask question like these to a general-purpose searching engine. Although some of them may be answered by carefully reading the text, this is not something that can be presented to us at once by the search engine.

We must also remember that users are interested in particular norms, rather than full documents. Thus, people wishing to conclude a contract for the lease of dwellings (Chapter

[11] S. Walter and M. Pinkal, 'Definitions in Court Decisions – Automatic Extraction and Ontology Acquisition' in: 'Law, Ontologies and the Semantic Web: Channeling the Legal Information Flood' (Amsterdam, IOS Press 2008) 95.
[12] A. Lamandini, 'Semantic Web' [2011] 6(1) Ricerche di Pedagogia e Didattica 2-3.

XXXI of Lithuanian Civil Code[13]) will be interested in norms related to that contract and some general rules for contract law, but not the other parts of the instrument.

A big problem is also lack of real connection between separate documents in the Web. Hyperlinks are intended to be used by the humans, not the machines. That is why a broken link (a well-known 404 error) presents a fatal thing that a computer cannot fix on its own.

Consequently, the search phase is only a first step in the intellectual work of a law professional – the next stage is processing and analyzing of these results where the person in charge picks necessary documents in order to apply them in his case. The last (third) stage will be actual reasoning with the help of information duly obtained.[14] It must be observed that computers only help users during the first stage, while the second and the third are totally left to human operators. They have to invest sufficient time and effort in completing these tasks which until now was almost taken for granted.

The reason the computers do so little to assist humans lies in the nature of the Web. Its main tool is the Hypertext Markup Language (HTML) which describes in its elements (known as *tags*), how the page shall be structured, e.g. which part of it must be treated as a heading, paragraph, image, embedded video and so on. However, this information only instructs user browser how to display content. Meanwhile, it does not help computers to understand the *contents* of a page. Whether the text displayed constitutes a draft version of the Declaration of Independence of the USA, a binding EU Regulation on Data Protection (GDPR) or an apple pie recipe – the machine will just treat it as a sequence of zeroes and ones. Computer programs and algorithms cannot share and perform tasks on such data. The only thing they can help us with is the actual search, but even here they are far from perfect.

Of course, there is a number of commercial databases and web services specifically designed for legal researchers. They have more 'intellectual' searching tools and the possibility to perform advanced searches, indicating authority, date of adoption of the legal instrument, its type and serial number, etc. It can give a better result when compared with mainstream solutions and even provide for a possibility to answer some of the questions specified above. However, there are also many important drawbacks. Firstly, such databases are for professional use only and even lawyers need preliminary practice before mastering them. This cannot be compared to general-purpose searching tools that are familiar to all Internet-users. Secondly, the databases are paid, which limits access to them of general society, including unemployed, migrant workers, poor and other socially vulnerable people. Thirdly, they have significant jurisdictional limitations. Thus, Westlaw and Lexis only provide data on major western jurisdictions. Such systems as 'Garant' and 'Consultant Plus' contain great collection of Russian and Post-Soviet laws, but are practically unknown elsewhere in the world and are never used in reasoning there. Moreover, one of the limitations of proprietary databases is their reliance on patented technology which makes it almost impossible to add new blocks without the agreement of the right holder. Consequently, they remain limited to what has been included to the database by the company's employees.

2. Semantic Web and its solutions for the legal sector

[13] Lietuvos Respublikos Civilinis Kodeksas (Civil code of the Republic of Lithuania) [2000] Valstybės žinios 74-2262.
[14] G. Shankhdhar, V.K. Singh and M. Darbari, 'Legal Semantic Web – a Recommendation System' [2014] 7(3) International Journal of Applied Information Systems 31-32.

One of the possible solutions to the problems named above is the progressive development of what is known as Semantic Web. It is not considered a different kind of Internet, but rather an extension of the latter. While the original Web was known as 'Web of documents', this one presents 'Web of data'.[15] In essence, it is a project of World Wide Web Consortium (W3C) to promote common data formats and exchange protocols. The general idea is that the Internet can be used to share not only the information, but also the *meaning*. In that way web pages and other materials distributed over the network will become understandable by the machines, and the latter will gain ability to perform various functions upon them (read, process, analyze, store, compare, use in equations and deliver them to end-users).[16] This project seems to partially solve the problem of information overload in the Internet, as it assigns a more active role to computers, allowing them not only to conduct a more thoughtful and thorough search, but also to assist lawyers and other seekers of legal knowledge at a later stage (analysis and reasoning). Full implementation of the semantic technologies will lead us to Web 3.0, a next stage in its progressive evolution.

The central concept of the project is '*semantics'*, which in linguistics stands for an area of study devoted to the meaning of words and phrases. Currently, the Web provides meaning only to the human-reader, not to the machine. The latter needs an instruction in a formalized, instead of a natural language. Such languages, indeed, have been created and implemented in different sectors.

The first example is eXtensible Markup Language (XML), which complements classic HTML and also relies on *tags*.[17] Unlike the latter, this language does not influence the way humans see the page, but provides commands for the computers. Its tags refer to objects, persons and relations between them. It may include such statements as <author>, <title>, <year>, <price> and many others. Moreover, it allows nesting, i.e. one element can be placed within the other, thus becoming its 'child' and acquiring relation with its 'parent'. With the above-mentioned tags that may happen when all of them are united together under a common tag of <book>. A great feature of XML language is that it allows users to define tags of their own, so that they can take advantage of all the peculiarities of their informational needs. We clearly see that XML may be used to describe legal concepts – parliamentary statutes (which all have their titles, reference numbers, sections and subsections and, of course, valid and outdated redactions). XML may also describe people (parties to a contract), places (jurisdiction, country of origin of a product) and more abstract things. At the same time, this language just puts meta-annotations to existing blocks of text – it does not do anything with them on its own.[18] In order to perform certain tasks on the data, there must be an additional application instructed to use it in a prescribed way.

Another important technology of Semantic Web is Resource Description Framework (RDF). It is a methodology, or a data model, for conceptual description or modelling of information in the Web through the use of different syntax notations and data serialization formats. In essence, it is used to describe objects (resources) and relations between them. This one indeed helps to catch semantic meaning of the data and represent it in an XML-based syntax. It also relies on specialized vocabularies defined by the users. This is done with the help of special RDF Schemas. RDF allows making statements about various

[15] Semantic Web [2018]: https://www.w3.org/standards/semanticweb/
[16] A. Patel and S. Jain, 'Present and Future of Semantic Web Technologies: a Research Statement' [2019] International Journal of Computers and Applications (https://doi.org/10.1080/1206212X.2019.1570666).
[17] C. Fong, 'What is the Semantic web?' [2011] 30 TALL Quarterly 13.
[18] Introduction to XML [2019] https://www.w3schools.com/xml/xml_whatis.asp

concepts in expressions of the form *subject-predicate-object* (known as *triples*). Such statements may be found in most legal texts, including Art. 25 of Lithuanian Constitution: "[e]veryone shall have the right to have his own convictions".[19] "Everyone" here is a subject, "shall have the right to have" is a predicate and "his own convictions" is an object. This statement in its formalized form may be understood by the software agent, which draws the relationship between the subject and the object. It must be noted that RDF is not intended for the human eye, just for the machine.

The last part of Semantic Web is Web Ontology Language (OWL) which is used to standardize the definition of real-world concepts. The main notion here is that of ontology, a term coming from philosophy and meaning identification in the most general terms of the kinds of objects that virtually exist and ways of their description. An ontology is an explicit and formalized specification of conceptualizations.[20] OWL can help to describe properties and classes, relations between classes (e.g., disjointness, cardinality, equality, symmetry). The relationships also need to include hierarchy of classes. In practice, ontology shall consist of a finite list of terms and the relationships between them. These terms have to be the most important concepts of a given area. The core notions in Law include: norm, case, person, agent, role, status, responsibility, property, etc. What is important here is that the general notions established by the ontology are shared for the whole domain and will still do their job even if different terminology is used.

The following example from Civil Procedural Law[21] demonstrates application of the named technologies to the legal sphere:

<p>Natural and legal entities may be parties to a civil procedure: plaintiff

<!DOCTYPE rdf:RDF [<!ENTITY law "http://domain.tld/otherpath/law#" >]>

<owl:Class rdf:ID="Plantiff">

<rdfs:subClassOf rdf:resource="#Person"/>

</owl:Class> <owl:inversOf>

<owl:ObjetcProperty rdf:ID="Defendant"/>

</owl:inversOf>

or defendant

<!DOCTYPE rdf:RDF [<!ENTITY law «http://domain.tld/otherpath/law#» >]>

<owl:Class rdf:ID="Defendant">

<rdfs:subClassOf rdf:resource="#Person" />

</owl:Class>

<owl:inversOf>

<owl:ObjetcProperty rdf:ID="Plaintiff"/>

[19] Lietuvos Respublikos Konstitucija (Constitution of the Republic of Lithuania) [1992] Valstybės Žinios 33-1014.

[20] T. Gruber, 'A Translation Approach to Portable Ontology Specifications" [1993] 5 Knowledge Acquisition 199.

[21] Lietuvos Civilinio Proceso Kodeksas (Code of Civil Procedure of Lithuania) [2002] Valstybės žinios, 36-1340 (Art. 41(1)).

</owl:inversOf>

</p>

This code makes explicit statements about 'plaintiff' and 'defendant', marking them up for the software agents to be noticeable, and showing to which class the two belong and what is their relation towards each other. There is no doubt that in practice it will be necessary to perform more complex work by trying to establish meaningful connections between more than two persons and objects in real life (companies, state institutions, rights and legal titles, etc.).

Together the three named components will enable more effective structuring, publication and referencing to legal documents and consequently will save time and money of those working with the legal data. Semantic technologies will enable cooperation between the computer and human beings at all stages of the legal research. There may be two possible scenarios for such work: interaction between machine and human (M2H), where the computer program will help to clarify the searching issues and present the most relevant result. Another option is machine-to-machine (M2M) operation, where separate programs (software agents) will exchange data to solve a certain problem.

In practice we see some specific projects, developing semantic technologies for the legal sector. One of the most prominent in Europe is the Legal Knowledge Interchange Format (or, LKIF), which was developed by ESTRELLA project and intends to establish uniform standards for representing and interchanging data on law, judicial cases and governmental policy.[22]

Another feature of the Semantic Web is its intended decentralization: there are clear intentions to move away from quasi-monopolistic position of Google and Facebook to the status quo where there is no need to depend on any major organization for the Web to function properly.[23] Private parties will not only create content (as it happens in Web 2.0), but also fill it with meaning. Such concept as Linked Open Data helps to implement this desire as it allows to publish structured data and provide for cross-references through hyperlinks. Each resource has its unique Uniform Resource Identifier (URI) and can be accessed from outside and contain its own links to other resources and objects.

3. Prospects of the semantic technologies

As was noted from the very beginning, the first thing where Semantic Web can do its job is the searching mechanisms. With content enhanced by semantic annotations it will be easier for machines to understand search queries and present an optimal result. In fact, specialists hope that instead of getting a set of hyperlinks to follow in response for your question typed into a search box, computers will be ready to propose a final and definite answer.[24] In many situations significant computing power will have to be used in order to perform a statistical query. You may ask the computer to find out how many states still retain the death penalty, or where in the world you will get the highest fine for driving drunk. These examples may present a special interest to academics, but other law professionals also may benefit from them. Thus, a judge can consult a specialized database in order to get an

[22] Th. Gordon, 'An Overview of the Legal Knowledge Interchange Format' in: 'Business Information Systems Workshop' (Berlin, Springer 2010) 240-241.
[23] J. Mailland, 'The Semantic Web and Information Flow: a Legal Framework' [2010] 11(2) North Carolina Journal of Law and Technology 269.
[24] E. Francesconi, Ibid., 49.

insight of which punishment to choose for the criminal, by comparing his case with previous convictions for similar offences. Attorneys will be able to better help their clients if all the details of the problem will be taken into consideration and a full list of applicable statutes, regulations and case-law will be delivered by a software agent.

The other important thing is to keep the existing databases up-to-date, so that you will get the law in force instead of some old and irrelevant edition. However, the outdated versions shall not be simply put aside as in many instances they present an interest for the lawyer (the solution of the case may depend on the act that was in force on a certain date). For that reason, it must be easy enough to get a correct redaction just by giving the computer an exact date. Again, this may be done only by supplementing the relevant document with the necessary time tags.

Semantic Web can also contribute to the establishment of more advanced data-management systems. Since RDF and OWL permit us to define subjects and assign various roles to them, it becomes possible to determine who has access to particular documents and their parts. This is quite promising for working with classified information and even trade or state secrets, so that only a duly authorized person may view the corresponding file. Another available feature is permission to modify and update content. If that is given to a limited number of actors, it increases the credibility of the system and allows other users to rely on the data contained therein. As we may access a certain legal rule from any application using semantic technologies, it is extremely relevant for us, where does this rule come from. Where the author and source are encoded together with the rule, we have no reasons to worry and question its authority.

Some other ways in which Semantic Web can be useful are provided in legal literature. Thus, P. Casanovas et al. speak about an ontology-based decision support system for young judges (*Iuriservice*). Its necessity is justified by a number of problems that inexperienced judges of their first appointment may face while performing their functions. They have numerous questions, most of which are of para- or meta-legal nature (Which procedures to follow? How to document an interim decision?). Most of them may be answered by their more experienced colleagues. However, the latter do not usually have enough time to do that, or may already be retired. Consequently, *Iuriservice* tries to combine all the wisdom in a sort of database with restricted access. The judges will be able to ask direct questions in natural language and get the response in it from the machine. Behind the curtain is a complex process of finding and matching the relevant question with the most probable and appropriate answer.[25]

A semantic approach to copyright management is presented by R. García and R. Gil. In their article the authors speak of a system that would help people establish the copyright conditions for their content. OWL-based technologies would allow checking if a certain action is granted by a specific license, as well as incorporating penalties for copyright violation directly into the system.[26]

Within a sector of private law software agents can look through a vast collection of previously drafted contracts and propose a set of terms that will mutually benefit the two parties entering into a particular relationship. It will do so basing its solution on law and

[25] P. Casanovas, N. Casellas and J-J. Vallbé, 'An Ontology-Based Decision Support System for Judges' in: 'Law, Ontologies and the Semantic Web: Channeling the Legal Information Flood' (Amsterdam, IOS Press 2008) 165.

[26] R. García and R. Gil, 'Copyright Licenses Reasoning using an OWL-DL Ontology' in: 'Law, Ontologies and the Semantic Web: Channeling the Legal Information Flood' (Amsterdam, IOS Press 2008) 161-162.

regulations, previous practice and usages. In certain situations of B2B relationships the contracts can even be concluded automatically if certain conditions are satisfied.

Finally, semantic technologies may be important for online dispute resolution. They can both assist the judge in reaching a decision on the matter and do the job instead of him in an automatic fashion. While a human in charge of resolving a dispute may be able to consult tens or hundreds of cases, the machines can do much better. The only problem is that modern judgments and arbitration awards do not usually have the most suitable from. They all have similar structure, but the reasoning part, where the competent authority cites legal norms and applies them to the exclusion of the others is more creative and cannot be as easily reduced to simple equations. That is why semantic technologies can help solve all the nuances of a dispute if it is a repeating and standard problem (late payments, non-enforcement of monetary obligations, etc.), but will be of less importance in cases with wide judicial discretion where decision is rather based on intuition than an analysis of previous practices.

4. Challenges for the Semantic Web

Common problems include vast amount of data that is not already in relevant formats. There are also many imprecise concepts in law, such as 'unpleasant emotional experiences' (which are elements of non-pecuniary damage in Civil Law)[27] or 'impeccable reputation' as a precondition for a person to become a judge.[28] In fact, law is not 'black and white' and has many nuances. Quite difficult will be to conceptualize the fundamental principles (such as 'fair trial', 'equality', 'rule of law') which are rather abstract and subject to controversy in doctrine as well as in practice when it comes to their precise meaning.

Another big problem is that there is no universal standard for development. Instead, several projects are run side-by-side in different institutions and they are poorly coordinated. What happens is that their end results suit only marginal policy goals and do not change the whole picture. At the same time, it may be presumed that such situation is common for transition and experimentation period and in the end, we will combine all the best solutions into the uniform standards of future Web 3.0 (or, even 4.0).

A frightening issue was revealed by J. Mailland, according to whom the situation where the Semantic Web is built from the bottom-up (by private individuals putting tags on the information) gives more opportunities to representatives of the Western nations. They are in a better position to impose familiar linguistic, cognitive and ideological frames as universal norms, while the rest of the world may be left behind.[29] The same author also fears the increased possibilities of censorship when all the information in the Web is 'labelled' with semantic tags.[30]

Conclusions

[27] Lietuvos Respublikos Civilinis Kodeksas (Civil Code of the Republic of Lithuania) [2000] Valstybės žinios 74-2262 (Art. 6.250).
[28] Lietuvos Respublikos Teismų įstatymas (Law on Courts of the Republic of Lithuania) [1994] Valstybės žinios 46-851 (Art. 22).
[29] J. Mailland, Ibid., 285.
[30] Ibid., 286.

As was shown in this paper, Semantic Web is a promising solution to the problems faced by law professionals and ordinary citizens while dealing with information overload in the vast expanses of the Internet. It is not as easy as it may seem, since requires additional and complicated work on establishing relations between concepts and ontology-based vocabularies. A big dilemma is that lawyers generally are not perfect at Web-technologies, while IT specialists know little about fundamental legal concepts and the relations between them. Another significant issue is the lack of uniformity with the development of Semantic Legal Standards for the Web. Akoma Ntoso, NormeInRete, LexML, MetaLex, LexDania and the others function independently (although consult each other from time to time), pursue different goals and used their own modifications of the standard XML/RDF/OWL technologies. In the long run there is a possibility of their integration, but now it seems that each of the projects is only capable of solving small problems identified by their leaders. At the same time, the very idea of introducing legal meaning to the world of the Internet and making the machines smart enough to help us with daily routine and really complex cases is brilliant and requires universal support.

Bibliography

Articles:

1. Bascik T., 'Web sémantique: Quelles perspectives pour l'information juridique?' [2014] 19(1) Lex Electronica.
2. Breuker J., Casanovas P. et al., 'The Flood, the Channels and the Dykes: Managing Legal Information in a Globalized and Digital World' in: 'Law, Ontologies and the Semantic Web: Channeling the Legal Information Flood' (Amsterdam, IOS Press 2008).
3. Casanovas P., Castellas N. et al., 'An Ontology-Based Decision Support System for Judges' in: 'Law, Ontologies and the Semantic Web: Channeling the Legal Information Flood' (Amsterdam, IOS Press 2008).
4. Casanovas P., Casellas N. and Vallbé J-J., 'An Ontology-Based Decision Support System for Judges' in: 'Law, Ontologies and the Semantic Web: Channeling the Legal Information Flood' (Amsterdam, IOS Press 2008).
5. Fong C., 'What is the Semantic web?' [2011] 30 TALL Quarterly.
6. Francesconi E., 'On the Future of Legal Publishing Services in the Semantic Web' [2018] 10(6) Future Internet.
7. Francesconi E. and Peruginelli G., 'Integrated Access to Legal Literature through Automated Semantic Classification' [2008] 17 Artificial Intelligence and Law.
8. García R. and Gil R., 'Copyright Licenses Reasoning using an OWL-DL Ontology' in: 'Law, Ontologies and the Semantic Web: Channeling the Legal Information Flood' (Amsterdam, IOS Press 2008).
9. Gordon Th., 'An Overview of the Legal Knowledge Interchange Format' in: 'Business Information Systems Workshop' (Berlin, Springer 2010).
10. Gruber T., 'A Translation Approach to Portable Ontology Specifications" [1993] 5 Knowledge Acquisition.

11. Lamandini A., ‘Semantic Web’ [2011] 6(1) Ricerche di Pedagogia e Didattica.
12. Mailland J., ‘The Semantic Web and Information Flow: a Legal Framework’ [2010] 11(2) North Carolina Journal of Law and Technology.
13. Mo Jang S. and Kim J.K., ‘Third Person Effects of Fake News: Fake News Regulation and Media Literacy Interventions’ [2018] 80 Computers and Human Behavior.
14. Patel A. and Jain S., ‘Present and Future of Semantic Web Technologies: a Research Statement’ [2019] International Journal of Computers and Applications (https://doi.org/10.1080/1206212X.2019.1570666).
15. Shankhdhar G., Singh V.K. and Darbari M., ‘Legal Semantic Web – a Recommendation System’ [2014] 7(3) International Journal of Applied Information Systems.
16. Walter S. and Pinkal M., ‘Definitions in Court Decisions – Automatic Extraction and Ontology Acquisition’ in: ‘Law, Ontologies and the Semantic Web: Channeling the Legal Information Flood’ (Amsterdam, IOS Press 2008).
17. Yu L., ‘A Developer’s Guide to the Semantic Web’ (Berlin: Springer 2014).

Legal acts:

18. Federal Law of the Russian Federation no. 289-FZ [2011] http://www.consultant.ru/document/cons_doc_LAW_120715.
19. Lietuvos Respublikos Konstitucija (Constitution of the Republic of Lithuania) [1992] Valstybės Žinios 33-1014.
20. Lietuvos Respublikos Civilinis Kodeksas (Civil code of the Republic of Lithuania) [2000] Valstybės žinios 74-2262.
21. Lietuvos Civilinio Proceso Kodeksas (Code of Civil Procedure of Lithuania) [2002] Valstybės žinios, 36-1340.
22. Lietuvos Respublikos Teismų įstatymas (Law on Courts of the Republic of Lithuania) [1994] Valstybės žinios 46-851.

Internet sources:

23. How Big is the Internet? Live Counter (https://www.live-counter.com/how-big-is-the-internet).
24. Introduction to XML [2019] https://www.w3schools.com/xml/xml_whatis.asp
25. Semantic Web [2018]: https://www.w3.org/standards/semanticweb/

WILL INTERNET PLATFORMS BECOME NEW STATES OF DIGITAL ECONOMY?

Laurynas Totoraitis[1]

Abstract

A decade ago new type of business model reinvented the way people shop online, book their holidays or order a ride. Online platforms established in the fields of commerce, entertainment and social media and made up a platform economy with new legal challenges unthinkable at that time and still underestimated.

In order to establish fully functioning Digital Single Market European Commission initiated a draft regulation which would regulate such platforms, provide legal certainty and fairness to business users within the EU. The initiative is analyzed in this article.

Keywords: platform economy, digital single market.

Introduction

The most significant platform operators are established in the United States and various countries of Asia, whereas only 4% of market capitalization is held by EU-based platforms.[2] However, this leaves a lot of room for innovation and business opportunities for EU corporate users using such intermediaries to sell their products and services online. For instance, European app developers share 30% of global revenue in most popular application distribution platforms.[3]

In previous years various challenges relating to platform economy were identified.[4] For instance, social media platforms raise social, legal and economic risks which involve (i.) forcing decision upon users or (ii.) protection of information provided to the platform. Users barely know that platforms analyze scrolling patterns, filter private messaging, account deletion does not remove data completely. Platforms use a practice of tying with other services, personal data is not portable etc.[5]

By recognizing that business owners (vendors, service providers, sellers) do not have enough market power to negotiate on terms and agreements, European Commission

[1] PhD candidate, Vilnius University Faculty of Law, research in the field of legal tech and cyber law.
[2] European Commission. Communication from the Commission to the European Parliament, THe Council, The European Economic and Social Committee and the Committee of the Regions. Online Platforms and the Digital Single Market Opportunities and Challenges for Europe. Available at https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-288-EN-F1-1.PDF, p.3
[3] WILLIAMSON, B., CHAN Y. S., WOOD, S. A policy toolkit for the app economy — where online meets offline. Available at https://plumconsulting.co.uk/policy-toolkit-app-economy/, p. 10
[4] European Commission. Communication from the Commission to the European Parliament, THe Council, The European Economic and Social Committee and the Committee of the Regions. Online Platforms and the Digital Single Market Opportunities and Challenges for Europe. Available at https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-288-EN-F1-1.PDF, p. 7 – 12.
[5] GEBICKA, A., HEINEMANN, A. Social Media & Competition Law. World Competition 37, no. 2 (2014), p. 158-164.

suggests making platform economy a more competitive environment by limiting powers of platforms themselves. In February 2019 the European Commission published a proposal for a Regulation of the European Parliament and of the Council on Promoting Fairness and Transparency for Business Users of Online Intermediation Services (hereinafter the Regulation of the Platforms). The analyzed regulation is supposed to create fair, predictable, sustainable and trusted legal framework in a business-to-platform relationship. It is important to ensure that comparable digital services would compete on a level field. Also, policy maker seeks to ensure that online platforms act responsibly. It is true that access to information is a value and a freedom worth protecting, however some types of information (adult content, fake news, hate and crime provoking) should be controlled and access restricted for some users (children etc.[6]). Research show that search platforms tend to be concentrated or form into monopolies, therefore regulatory intervention is welcome and necessary[7].

The proposed Regulation of the Platforms should cover a part of unfair business practices, such as unilaterally changing terms and conditions without necessary notification period, terminating business accounts without proper investigation or an effective right to an appeal and other. Such practices were not covered by existing legal acts in the fields of competition law, [8] and consumer protection law. Guidance on Unfair commercial practices directive was also renewed recently. All of this should contribute to a trust in the platform economy. The regulation ensures that market players have appropriate transparency and appropriate redress measures.

However, how to effectively regulate something that is fast changing and evolving, such as internet-based services? The Commission recognizes this challenge and sets up rules that are rather general and principles-based. The Commission promotes principles-based[9] measures in Digital Single Market regulation. This makes the Regulation of the Platforms a good scientific object of research since content of principles will be elaborated in scientific articles and case law.

The goal of this article is to review proposed regulation on promoting fairness and transparency for business users of online intermediation services and evaluate its main provisions. This goal is achieved by (I.) identifying main challenges business users face in the platform economy; (II.) verifying whether proposed regulation corresponds to and solves these issues.

The author identifies a set of examples which need to be resolved in the platform economy. First of all, review mechanisms are too often manipulated with fake reviews organized by competitors. This reduces trust in the platforms. Secondly, ranking practices are unclear and dependent on profiling of a customer. Lastly, business users are too dependent on changing policies, frivolous copyright claims (sometimes used in bad faith by their competitors). The European Commission conducted a survey where market players expressed their concerns regarding following problems while using intermediation services. First of all, they are deprived of access to valuable data generated in the platform. Secondly,

---

[6] London School of Economics. EU Kids Online. Available at http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/Intheirownwords020213.pdf.

[7] POLLOCK, R. Is Google the Next Microsoft: Competition, Welfare and Regulation in Online Search," Review of Network Economics, De Gruyter, vol. 9(4), p. 1-31.

[8] GEBICKA, A., HEINEMANN, A. Social Media & Competition Law. World Competition 37, no. 2 (2014), p. 149–172.

[9] European Commission. Principles for Better Self- and Co-Regulation. Available at https://ec.europa.eu/digital-single-market/en/news/principles-better-self-and-co-regulation-and-establishment-community-practice.

refusal to grant market access or short-notice terms regarding conditions for market access is an issue. Thirdly, unfairly promoting platforms' own services or products. Lastly, there is a lack of transparency on remuneration, especially with listing practices and use of data.[10]

1. Scope of the Regulation

Platforms act as marketplaces, search engines[11], social media[12] and creative content outlets, application distribution platforms, communications services, payment systems, and platforms for the collaborative economy1. The most recognized examples are Google's AdSense, eBay and Amazon Marketplace, Google Search, Facebook, YouTube, Spotify, Google Play and App Store, PayPal, and Uber or Upwork. Platforms operate in two-sided market[13] where demand that one party has for the product is complementary to the demand that the other party has for the same product.[14] In other words, a customer on one side of the market will be willing to participate to the platform activity only if it is expected that sufficient participation from the other side is.[15]

Some platforms provide doubtful added value to the product but rather are listing sites, such as booking.com. However competitive advantage of such platforms in comparison to local service providers is that they benefit from the economy of scale and network effect which makes the value of the service increase with the number of users.[16] One should bear in mind that other types of intermediation services are extremely concentrated, such as app selling sites (dominated by App Store and Google Play). By collaborating with a platform, a business entity becomes dependent because a significant part of business inquiries come through this intermediary. Intermediaries' business model is based on selling advertisement, registration fees for business users (or sometimes - customers), transaction fees and bundling with information goods.[17]

The Regulation of the Platforms will be significant to online intermediation service providers[18], business users and corporate website users (and their associations) as well as

[10] European Commission. Communication from the Commission to the European Parliament, THe Council, The European Economic and Social Committee and the Committee of the Regions. Online Platforms and the Digital Single Market Opportunities and Challenges for Europe. Available at https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-288-EN-F1-1.PDF, p. 4-5.

[11] Google. Facts About Google and Competition, About Ads. Available at http://www.google.com/competition/howgoogleadswork.html.

[12] COHEN, S., NORTH, Z., PARK, D. The Opportunities and Risks Posed by Social Media for Antitrust Compliance. Available at http://www.bna.com/the-opportunities-and-risks-posed-by-social-media.

[13] BORK, R., SIDAK, G. What does the Chicago School Teach About Internet Search and the Antitrust Treatment of Google? Journal of Competition Law & Economics, Volume 8, Issue 4, December 2012, p. 663–700, SCHMALENSEE R, EVANS, D. Markets with two-sided platforms. In: ABA section of antitrust law (ed) Issues in competition law and policy. p. 667–693/

[14] EVANS, D. The Antitrust Economics of Multi-Sided Platform Markets, 20 Yale Journal on Regulation, p. 328; ROCHET, J.C., TIROLE, J. Platform Competition in Two-Sided Markets, 4 Journal of the European Economic Association 990 (2003).

[15] JULLIEN, B. Two-sided Markets and Electronic Intermediaries. CESifo Economic Studies, Volume 51, Issue 2-3, p. 233-260. Available at https://academic.oup.com/cesifo/article-abstract/51/2-3/233/306461?redirectedFrom=fulltext,

[16] European Commission. Report on the Public Consultation on the Regulatory Environment for Platforms, Online Intermediaries and the Collaborative Economy.

[17] JULLIEN, B. Two-sided Markets and Electronic Intermediaries. CESifo Economic Studies, Volume 51, Issue 2-3, p. 233-260. Available at https://academic.oup.com/cesifo/article-abstract/51/2-3/233/306461?redirectedFrom=fulltext, p. 239

[18] European Commission. Communication Towards a thriving datadriven economy.

specialized mediators[19]. In general, online intermediation service is a platform. Online intermediation services are contractual obligation aimed at facilitating the initiating of direct transaction between business users and consumers, irrespective of whether the transaction is ultimately concluded online or offline. The regulation expressis verbis states that it is not applicable to online advertising serving tools or online advertising exchanges which are not provided with the aim of facilitating the initiation of direct transactions and do not involve a contractual relationship with consumers. They must constitute information society services which is (i.) any service normally provided for remuneration, (ii.) at a distance (service is provided without the parties being simultaneously present), (iii.) by electronic means (the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means) and (iv.) at the individual request of a recipient of services (the service is provided through the transmission of data on individual request)[20].

For instance, services would not be considered as provided at a distance if provided in the physical presence of the provider and the recipient, even if they involve the use of electronic devices such as medical examinations, consultation of an e-catalogue with the customer on site, plane ticket reservation at a travel agency. Also, services are considered not to be provided by electronic means if they have material content even though provided via electronic devices such as ticket dispensing machines, voice telephony. Lastly, television broadcasting services (including on-demand services) or radio broadcasting services are not supplied at the individual request therefore would not be applicable.

In the context of the regulation business user is any person (natural or legal) which uses online intermediation services to offer goods or services to consumers for purposes relating to its trade, business, craft or profession (Article 2). This definition would cover distributors, craftsmen, freelance service providers or any other seller using marketplace platforms. The author believes this definition also covers copyright holders who use subscription based streaming platforms such as Spotify even though consumers use such platforms as a whole – individual licensing or purchase agreement are not made while listening to a particular piece of music on such platforms.

Whereas corporate website user is a similar person but uses websites instead of solely online intermediation services (Article 2). Online search engine means a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found. Internet platforms have reduced or even made obsolete product research costs as there are platforms which instantaneously provide price comparison results.[21]

This is a first attempt to define what is an online platform in a legal act (not considering EC communications or other soft-law material). The definition correctly corresponds with existing legal framework and provides an adequate criterion for a platform. It is technology neutral definition and does not consider the type of services provided but rather the way

[19] European Commission. Press release "Digital Single Market: EU negotiators agree to set up new European rules to improve fairness of online platforms' trading practices" available online europa.eu/rapid/press-release_IP-19-1168_en.htm

[20] Directive (EU) 2015/1535 Of the European Parliament and of the Council Laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, Article 1(1)(b).

[21] GLENN, E., ELLISON S.F. Lessons About Markets from the Internet. Journal of Economic Perspectives, 19 (2): 139-158. Available at https://economics.mit.edu/files/7606, p. 141 – 146.

business is conducted. This makes the Regulation of the Platforms relevant in the years to come.

2. Individual provisions of the Regulation

Alternative dispute resolution schemes. At the moment business users have limited ability to file for a court because of a risk of retaliation (Preamble 4). This might be a correct assumption. Paypal, Amazon, booking.com, Aliexpress and other leading marketplace-platforms have internal dispute settlement procedures among consumers and vendors which made a breakthrough in small claim disputes. Such disputes are settled cheaply and fast by impartial arbitrator (or an artificial intelligence). This scheme is set by the platform operators. However, if a dispute arises between a business user and an online intermediation service operator there are no external institution to resolve a dispute. Business users are obliged to follow terms and conditions drafted by the platform operator which might involve foreign applicable law and seat of arbitration.

Jurisdiction matters have always been a topic of discussion since legislators started to regulate electronic services. Since these services make obsolete physical distances and state borders, traditional territorial (or seat of establishment) approach would not be effective. Therefore, the regulation will be applicable to platform operators without considering their establishment jurisdiction (in a Member State or outside the European Union). However other two conditions are set. First of all, business users or corporate website users are to be established in the Union. Secondly, goods or services have to be offered to consumers located in the European Union at least for part of the transaction. What this means is that a consumer has to be physically located in the Union, but do not need to have his or her place of residence in the Union. Neither has to be a citizen of any Member State. In a case goods or services are offered exclusively to consumers outside the EU the regulation shall not apply (Preamble 7). From the wording of the regulation one can notice that the transaction itself is not necessary, only an intention to sell. These conditions are cumulative, and both must be met. If a business user satisfies both conditions, it can enjoy rights granted by the Regulation of the Platforms.

The Regulation will only be applicable in case the terms and conditions of a contract between business user and platform operator were not individually negotiated. This well corresponds to a current business practice. The European Commission published survey results which showed that business users have no bargaining power therefore all contracts are signed under standard draft.[22] The Regulation also requires that such terms must be drafted in a clear and unambiguous language which is comprehensible by an average business user. Such contracts must not be vague, unspecific or lack detail on important commercial issues. This would fail to provide predictability regarding business relationship (Preamble 13, Article 3).

Research show that terms and conditions are drafted in difficult legalese, 56% consumers indicated that they did not read the terms and conditions of online platforms[23], parts of text is spread across various places in the website. All of this makes it more difficult to comprehend the true meaning of rights and obligations. It is hard to make an informed

[22] European Commission. Report on the Public Consultation on the Regulatory Environment for Platforms, Online Intermediaries and the Collaborative Economy.
[23] European Commission. Special Eurobarometer 447 Report "Online platforms". Available at ec.europa.eu/information_society/newsroom/image/document/2016-24/ebs_447_en_16136.pdf, p. 65.

decision which intermediation service to use if a business user cannot fully understand the contract. This has to change, and proposed regulation contributes to this. Transparency is achieved by providing general terms and conditions in a clear and easily accessible manner even in pre-contractual phase. The Regulation requires that such provisions must be available online and without a requirement to establish business account in the platform.

Speaking about legal certainty, any changes to terms and conditions have to be notified with at least 15-day notice. In all cases such notice must be reasonable and proportionate depending on specific circumstances (Article 3). Therefore, if a change in terms and conditions requires business user to redesign its processes or implement additional measures on product safety, shipping etc. notice period must be prolonged.

The regulation states that provisions annulled by a competent court, will not be binding only on the business user concerned. Non-compliant terms and conditions are not binding on a business user concerned *ex nunc* however the rest of the contract remains valid (Preamble 15). It is worth raising a question whether it was better to bind the provider of intermediation services to annul a specific provision for all users? The author contributes to a EC's chosen model as this creates less legal chaos. Even though business users do not have sufficient market power to negotiate on terms and conditions they are better informed than customers and can challenge individual clauses by their own.

Even though the Regulation of the Platforms grants various rights to business users it is understandable that a platform operator (provider of online intermediation services) should keep its right to remove particular goods or services from the platform or suspend business users' account in general (Article 4). Such grounds must be objective (Article 3(1)(c)). First of all, such decision must be properly provided for a business user in a timely manner. The regulation states that it must be done without undue delay. Secondly, such decision must be specified and elaborated (Article 4). Arguments must be informative enough for business user to evaluate whether it is worth it to challenge the decision in court. Platform operator can take such actions if it identifies items as illegal content.[24] In 2018 EC issued a recommendation on measures to effectively tackle illegal content online which states that provision should be made for mechanisms to submit notices. Those mechanisms should be easy to access, user-friendly and allow for the submission of notices by electronic means. Those mechanisms should allow for and encourage the submission of notices which are sufficiently precise and adequately substantiated to enable the hosting provider concerned to take an informed and diligent decision in respect of the content to which the notice relates, in particular whether or not that content is to be considered illegal content and is be removed or access thereto is be disabled. However, such flagging systems are manipulated by competitors by issuing false reports and giving a competitive advantage.

Ranking. Today's platform economy is based on a principle zero-sum-game where winner takes it all. That is why there are articles trying to analyze particularities of various platforms search engine mechanisms.[25] Consultants provide their expertise to help achieve better search results by optimizing meta-tags[26]. Ranking is essential for good commercial

[24] European Commission, Recommendation (EU) 2018/334 On Measures to Effectively Tackle Illegal Content Online

[25] BORK, R., SIDAK, G. What does the Chicago School Teach About Internet Search and the Antitrust Treatment of Google? Journal of Competition Law & Economics, Volume 8, Issue 4, December 2012, p. 663–700.

[26] Google. Webmaster Tools, Ranking, Available at http://support.google.com/webmasters/bin/answer.py?hl=en&answer=34432; Google. Facts About Google and Competition, About Search, Available at http://www.google.com/competition/howgooglesearchworks.html. Bing Webmaster Central FAQs, at

results in the platform economy. Some claim that Google's ranking methodologies and search algorithms are unfair. Critics have focused on whether Google's ranking of its specialized search results harms competitors and whether Google excludes competitors by limiting access to search inputs.[27]

Coding of such algorithms is a commercial secret because it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question, it has commercial value and is subject to reasonable steps to keep it secret[28]. Proposed Regulation of the Platforms does not infringe the Directive On the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

Besides, providers of online intermediation services publish press releases explaining changes in the algorithms. The regulation provides even more transparency by requiring that platform operators outline the main parameters which determine ranking in advance. First of all, it should be stated how and to what extent ranking mechanisms consider characteristics of a product, relevance of those characteristics for a consumer and design characteristics of the website used by corporate website users (Article 5).

This should contribute to a better predictability and allow business users to compare different platforms to suit their needs. The notion of main parameter refers to any general criteria, processes, specific signals incorporated into algorithms or other adjustment or demotion mechanisms used in connection with the ranking system. The information provided should also include an explanation of possibilities to actively influence ranking against remuneration (Preamble 17). Other types of searchable data include direct response to the query in a form of image, video, map destination, product or real-time news[29].

There are examples when a provider of online intermediation service itself offers certain goods or services to consumers through its own online intermediation services or does so through a controlled business entity (Article 6). In part such practices are captured by competition law. Preamble 19 of proposed regulation states that such competition is allowed per se. In such situations platform operator must act in in a transparent manner and provide a description of any differentiated treatment (legal, commercial or technical) that it might give in respect of goods or services it offers itself. This covers practices such as providing access to any personal or other data which online intermediation service providers collects from its users or which is generated through the provision of those services, ranking or any remuneration charged for the use of a platform and conditions for use of directly connected or ancillary services.

Use of data. It is a cliché to say that data is the currency of digital economy. Value of data is acknowledged in the Regulation preamble 20. General Data Protection Regulation sets strict rules regarding use of personal data. However, it is applicable only to natural

---

8, available at http://www.bing.com/toolbox/home/; Bing. How Bing Delivers Search Results. Available at http://onlinehelp.microsoft.com/en-us/bing/ff808447.aspx

[27] BORK, R., SIDAK, G. What does the Chicago School Teach About Internet Search and the Antitrust Treatment of Google? Journal of Competition Law & Economics, Volume 8, Issue 4, December 2012, Pages 663–700.

[28] Directive (EU) 2016/943 of the European Parliament and of the Council On the Protection of Undisclosed Know-how and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure.

[29] Google. Microsoft and Experts Agree: Search Is Evolving Beyond Links. Available at http://googlecompetition.blogspot.com/2012/09/microsoft-and-experts-agree-search-is.html

persons and not business users. Eurobarometer survey in 2016 on online platforms showed that 72% also considered that online platforms should be regulated to limit the extent to which they display different results to users based on the data collected about their activities.[30] The Regulation of the Platforms sets that business users are provided with a clear description of the scope, nature and conditions of their access to and use of certain categories of data in a proportionate manner. Platform operators have an obligation to provide business users with a clear description of the scope, nature and conditions of their access to and use of certain categories of data.

The regulation sets minimum standards what information must be provided. That is whether platform operator has access to personal or other data which is provided for the use of the platform or which is generated through the provision of those services. Also, whether business user has access to any data provided by that business user in connection to his or her use of services. Lastly, whether business user has access to data (including in aggregated form) generated by other business users and consumers.

Most favorable notion. In 2015 a coordinated investigation against booking.com was made by the French, Italian and Swedish competition authorities. They analyzed price parity clauses which required hotels to offer the same or better room price on the platform in comparison to their own websites or other mediums whether online or offline. The platform argued that there is high risk of free-riding by using platform's infrastructure for promotional reasons[31] but making a reservation without an intermediary. The case was closed by accepting commitments that hotels can offer better deals to loyalty card holders or via offline channels or walk-in bookings.[32]

The proposed regulation states that in some situations a practice to restrict business users to offer goods or services under different conditions through other means than the platform itself (a form of exclusiveness) is allowed. Such restriction should be based on published economic, commercial or legal consideration of for such restriction. First of all, article 8 restricts providing goods or services under different conditions. It is not important whether such conditions are better (i.e. cheaper) or worse for the consumers. This happens when business users have multi-channel sales practice and uses various platforms or his or her own website for sales, business inquiries or reservations. If intermediator is avoided, business user usually received better profit margin as no commission payment is grabbed by the platform. Providers of online intermediation services are interested to collect not only payments, but also collect data of the transaction itself.

Business users might be interested in avoiding such restriction. It can be done by offering some services or goods through one medium, and other through the other. The regulation only allows this restriction to apply for the same goods and services (Article 8). For instance, a hotel may dedicate separate suits to be offered on booking.com and other rooms to be offered for walk-ins. However, this norm is more understood as a transparency obligation rather than setting new requirement.

Internal complaint-handling system. A significant novel in the legal background is article 9 of the regulation which sets up a requirement for intermediation services to set up

[30] European Commission. Special Eurobarometer 447 Report "Online platforms". Available at ec.europa.eu/information_society/newsroom/image/document/2016-24/ebs_447_en_16136.pdf, p. 40.
[31] CAILLAUD, B., JULLIEN B. Chicken & egg: competition among intermediation service providers. Rand J Econ 34, p. 309–328.
[32] COLANGELO M. Parity Clauses and Competition Law in Digital Marketplaces: The Case of Online Hotel Booking. Journal of European Competition Law & Practice, Volume 8, Issue 1, 1 January 2017. Available at https://academic.oup.com/jeclap/article-abstract/8/1/3/2890729, p. 3–14.

an internal dispute resolution system. This should provide business users with an immediate, suitable and effective redress possibilities. Such system should resolve a meaningful part of disputes. The procedure should be more result oriented, flexible and address individual complaints. Moreover, the overall results of disputes resolved ought to be published annually. This raises some doubt why would the same entity change its decision? It is clear that decisions of the same operator will be questioned during such procedures. Then the same operator will be resolving a dispute. This creates a conflict of interest and biased decision making. It is worth noting that small enterprises as stated in Recommendation 2003/361/EC are exempted from this provision. Therefore, such scheme should be considered as medium for cooperation rather than judicial appeal system. Business user will have an opportunity to explain him/herself especially regarding decisions on removing supposedly illegal content.

Mediation. Business users hesitate to file for a court against a platform operator. They fear that either such behavior could lead to a complete retaliation, or contractual jurisdiction is not suitable for them. Therefore, the Regulation of the Platforms also suggests parties to solve their dispute in mediation sessions (Article 10). Platform operators should a priori name mediators with which they trust and commit. Costs of mediation should be covered by the providers of online intermediation services at least by a reasonable proportion of 50 per cent or more of total costs. Such settlements will require specific competence of the mediators who have deep understanding of peculiarities of online intermediation services and business users. Therefore, the Commission is encouraged to establish specialized organizations which would unite such experts.

Moreover, associations and public bodies representing business users or corporate website users are granted a right to file for a court on behalf of a business users itself in a form of collective interest or in the general interest. Codes of conduct are also encouraged. Such documents should be drafted with stakeholders involved and consider specifics of different size enterprises and features of the sector concerned.

Conclusions

Regulation on promoting fairness and transparency for business users of online intermediation services provides a few new rights to business users thus protecting EU-based entrepreneurs against US-Asia based online intermediation service providers. Such rights are described in abstract, principle-based approach as it is common for Digital Single Market legal acts. If adopted the regulation should make European Union a more attractive jurisdiction for e-commerce vendors to establish here. However, this initiative also shows that European Union have lost the competition in the online intermediation service providing market.

The Regulation does not tackle the most troublesome business practices faced by business users, but rather sets an approach so solve those disputes internally or using mediation. If passed, these legal relations probably will not change for the years to come. Therefore, the author wishes the regulation would be more ambitious and put platform operators under stricter obligations. Regulation also lacks detail regarding how active must be an online intermediation service provider to ensure product safety and removal of illegal content. Such and other requirements will be set in other legal acts as this regulation is not comprehensive. It is clear, however, that attention to platforms will continue to increase and legal regulation will become more defined stripping down state-like authority eventually.

Bibliography

1. Bing. How Bing Delivers Search Results. Available at http://onlinehelp.microsoft.com/en-us/bing/ff808447.aspx
2. Bing Webmaster Central FAQs, at 8. Available at http://www.bing.com/toolbox/home/
3. BORK, R., SIDAK, G. What does the Chicago School Teach About Internet Search and the Antitrust Treatment of Google? Journal of Competition Law & Economics, Volume 8, Issue 4, December 2012, Pages 663–700.
4. CAILLAUD, B., JULLIEN B. Chicken & egg: competition among intermediation service providers. Rand J Econ 34, p. 309–328.
5. COHEN, S., NORTH, Z., PARK, D. The Opportunities and Risks Posed by Social Media for Antitrust Compliance. Available at http://www.bna.com/the-opportunities-and-risks-posed-by-social-media.
6. COLANGELO M. Parity Clauses and Competition Law in Digital Marketplaces: The Case of Online Hotel Booking. Journal of European Competition Law & Practice, Volume 8, Issue 1, 1 January 2017, p. 3–14. Available at https://academic.oup.com/jeclap/article-abstract/8/1/3/2890729.
7. Directive (EU) 2016/943 of the European Parliament and of the Council On the Protection of Undisclosed Know-how and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure.
8. Directive (EU) 2015/1535 Of the European Parliament and of the Council Laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, Article 1(1)(b).
9. EVANS, D. The Antitrust Economics of Multi-Sided Platform Markets, 20 Yale Journal on Regulation, 325.
10. European Commission. Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions. Online Platforms and the Digital Single Market Opportunities and Challenges for Europe. Available at https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-288-EN-F1-1.PDF
11. European Commission. Communication Towards a thriving data driven economy.
12. European Commission. Press release "Digital Single Market: EU negotiators agree to set up new European rules to improve fairness of online platforms' trading practices". Available at europa.eu/rapid/press-release_IP-19-1168_en.htm.
13. European Commission. Principles for Better Self- and Co-Regulation. Available at https://ec.europa.eu/digital-single-market/en/news/principles-better-self-and-co-regulation-and-establishment-community-practice.
14. European Commission. Recommendation (EU) 2018/334 On Measures to Effectively Tackle Illegal Content Online.
15. European Commission. Report on the Public Consultation on the Regulatory Environment for Platforms, Online Intermediaries and the Collaborative Economy.
16. European Commission. Special Eurobarometer 447 Report "Online platforms". Available at ec.europa.eu/information_society/newsroom/image/document/2016-24/ebs_447_en_16136.pdf.

17. GEBICKA, A., HEINEMANN, A. Social Media & Competition Law. World Competition 37, no. 2 (2014), p. 149–172.
18. GLENN, E., ELLISON S.F. Lessons About Markets from the Internet. Journal of Economic Perspectives, 19 (2): 139-158. Available at https://economics.mit.edu/files/7606.
19. Google. Facts About Google and Competition, About Ads. Available at http://www.google.com/competition/howgoogleadswork.html.
20. Google. Microsoft and Experts Agree: Search Is Evolving Beyond Links. Available at http://googlecompetition.blogspot.com/2012/09/microsoft-and-experts-agree-search-is.html.
21. Google. Webmaster Tools, Ranking, Available at http://support.google.com/webmasters/bin/answer.py?hl=en&answer=34432.
22. JULLIEN, B. Two-sided Markets and Electronic Intermediaries. CESifo Economic Studies, Volume 51, Issue 2-3, p. 233-260. Available at https://academic.oup.com/cesifo/article-abstract/51/2-3/233/306461?redirectedFrom=fulltext.
23. London School of Economics. EU Kids Online. Available at http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/Intheirownwords020213.pdf.
24. POLLOCK, R. Is Google the Next Microsoft: Competition, Welfare and Regulation in Online Search. Review of Network Economics, De Gruyter, vol. 9(4), p. 1-31.
25. ROCHET, J.C., TIROLE, J. Platform Competition in Two-Sided Markets, 4 Journal of the European Economic Association 990 (2003).
26. SCHMALENSEE R,, EVANS, D. Markets with two-sided platforms. In: ABA section of antitrust law (ed) Issues in competition law and policy. P. 667–693
27. WILLIAMSON, B., CHAN Y. S., WOOD, S. A policy toolkit for the app economy — where online meets offline. Available at https://plumconsulting.co.uk/policy-toolkit-app-economy.

PROHACKTIVE POLICING: POLICE ACCESS TO IT-SYSTEMS IN CRIMINAL INVESTIGATIONS

Lisa Urban[1]

Abstract

Incidences of Cybercrime, i.e. crimes in which computers and the internet are either the target or tool, are rising. Unfortunately, most conventional investigative measures are ineffective against the methods of anonymization and encryption used by cybercriminals. While cybercriminals profit from the cross-border character of the online world, investigators find themselves decelerated by the limits of domestic law and slow interjurisdictional investigative collaboration. To overcome the arising obstacles, the idea of legalizing hacking techniques for police investigations has emerged.

Two tendencies can be observed in this context: investigative measures targeting individuals, mainly for surveillance purposes, and measures targeting online platforms used for illegal activities on the darkweb. Both cases centre around the access to computer systems that usually has to be gained by subverting technical security mechanisms, in other words, by hacking into these systems.

Technically similar, both investigative approaches are today often considered under the same legal framework. Either under the authorization for a search and seizure, or under the conditions of "hacking measures", such as most legislations of EU Member States foresee them. However, in practice, the access to a personal computer device and the access to a web-server expose many differences that also reflect in the legal questions surrounding them.

The following article will try to answer some of the questions arising in this context: What are these investigative measures that include law enforcement's use of hacking techniques? In what do the presented approaches differ? And what legal consequences do these differences bare? Its objective is to lead the way for a clear legal and rhetorical distinction of current practices, in order to allow for legal certainty and comprehensive fundamental rights protection.

Keywords: Cybercrime, Darkweb, Investigative Measures, Hacking-Techniques, Policing

Introduction

The wider public perceives the darknet as a dark alley covering criminals of all kinds in their flourishing activities. Indeed, although the covering coat of darknet-privacy is not as

[1] Lisa Urban is research assistant and PhD student at the University of Luxembourg and the KU Leuven. Her research, funded by the National Research Fund of Luxembourg, focusses on law enforcement's use of hacking techniques in criminal investigations.

opaque as many (also criminals) might think, the darknet is still one of the most challenging fields in modern police investigation. A promising investigative technique adopted to face this challenge is law enforcement's use of hacking techniques to infiltrate computer systems. This article will present and compare two different forms of hacking-investigations.

The darknet is the part of the internet, which users cannot directly view or enter without specific software.[2] In its characteristics, the darknet increases anonymization, making it more difficult for investigators to attach a specific individual to online activities, and vice versa. The most prominent way to access the darknet is by using the TOR network. A simple and free download of the TOR web-browser enables connection to the darknet and a strong privacy protection. TOR uses a combination of multiple servers and a multi-layered encryption system to make the tracking and identification of internet activity as difficult as possible.[3] As communication is usually well encrypted and identification nearly impossible, traditional investigative measures face their limits, especially with regard to the gathering of evidence. The main problems are related to the localization of the web servers, i.e. high capacity computers holding web-sites or internet services,[4] and to the identification of the real persons behind an internet service of a specific online activity. Both difficulties arise due to the strong privacy protection in the darknet. However, locating the web servers is a key condition for investigators to search and seize the data stored on them. As would be the identification of service providers, website operators and clients. Without their identification, investigators have no possibility to request information or user data from the individuals or the companies, who own the servers or offer the services.[5] Hence, all electronic evidence has to be obtained in direct access to the data, i.e. without relying on cooperation with such third parties as an intermediate. Additionally, there is usually no use in requesting content data or to engage in traditional surveillance measures, such as interceptions, as communication is encrypted and therefore of little use for investigators. Taking the amount of resources and time needed for decryption, the only practical approach is to try to gain access on the communications in clear, directly readable text, before encryption and transmission, or after it is decrypted by the intended recipient. Also enquiries into financial transactions are often just as little successful as the beforementioned options[6], since darknet users engaging into serious criminal activities have long migrated from the use of rather traceable cryptocurrencies such as the well-known Bitcoin to much more private and untraceable digital currencies, such as Monero.

To face the challenges posed by the darknet's privacy, investigators are developing new investigative approaches, often resorting to new spectres of application of traditional investigative methods. One new investigative approach is, for instance, the use of hacking techniques, not only to gain access to a computer system, but also to undertake

---

[2] Find a more extensive explanation in: K. Becker, B. Fitzpatrick, 'In the Search of Shadows: Investigating and Prosecuting Crime on the "Dark Web"', United States Attorneys' Bulletin [2018], 41.

[3] https://www.torproject.org/about/history/. (Last access 31.3.2019).

4 The Oxford dictionary defines a web server as "A program that provides and manages access over the web to a collection of websites; (also) a computer or computer system running a program of this kind, especially one on which the websites themselves are stored", https://en.oxforddictionaries.com/definition/web_server (Last access: 31.3.2019).

[5] For instance, even in cases in which administrators of a website have been identified, they will seldomly cooperate with law enforcement and provide information on users. Especially in cases in which their own offered services and business model are illegal.

[6] An enumeration of some of the issues in darknet investigations under German law can also be found in: B. Krause 'Ermittlungen im Darknet – Mythos und Realität' Neue Juristische Wochenzeitschrift (NJW) [2018], 678-681, 679. See also K. Becker, B. Fitzpatrick, 'In the Search of Shadows: Investigating and Prosecuting Crime on the "Dark Web"', United States Attorneys' Bulletin [2018], 43.

surveillance[7] of the systems users. To hack a computer system means to access it by circumventing or overcoming its security mechanisms, e.g. password protection. This can help to overcome most of the beforementioned issues, as it circumvents anonymization efforts undertaken in the darknet.[8] Under the right conditions, law enforcement can use such techniques in order to obtain otherwise encrypted data and information on a person's online activities and real identity.

In this context, direct access, online- or computer surveillance and hacking techniques are often named in one breath. They are also frequently considered under the same legal framework, as national legislations[9] usually authorize a multitude of hacking featured investigative measures under the broad formulation of acts using technical means or devices to access computer systems.[10] Nonetheless, it can be deceptive to generalize the possibilities that hacked access to computer systems provides for surveillance. If hacking-investigations can assume different shapes, and if furthermore these shapes cause very different legal effects, they need to be distinct in order to reflect their impact on fundamental rights. Recent developments in darknet investigations mainly reveal two tendencies of forms in which such measures appear: one consists in accessing web-servers and the other one in the access to personal computer devices, such as smartphones, PCs, etc. While the first option potentially allows to gather information on all users of a particular internet service or website, the second approach has the objective to gather evidence on the activities of one individual. After a short presentation of the two investigative approaches (1.) and in view of this difference, it should be analysed which other differences can be observed between the two forms of hacking investigation (2.). Furthermore, this article will examine how these differences reflect in the legal issues relating to the two phenomena (3.). The scope of this article does not allow for an analysis of the legal questions that each investigative approach poses. It shall rather diagnose some problematic aspects for the purpose of this comparison. If it were to be discovered that the differences between the different hacking techniques are substantial, it could be indicated to establish a clear distinction. This would allow for more clarification on the matter, for a precise debate about such investigative measures and for the establishment of a clear legal classifications and conditions.

1. Presentation of Hacking Investigations

Two tendencies of surveillance schemes that are based on hacking techniques appear dominant in criminal investigations. One investigative measure targets a collective of internet users (a.), while the other one focusses on one specific individual (b.).

a. Collective Surveillance

When investigators are able to locate a server on which a website is stored, they can either conduct an open search and seizure[11] or they could secretly hack into it under the

[7] Surveillance in this context means the secret and remote acquisition of data performed through the access into a computer system.
[8] See detailed explanation intra.
[9] The same considerations are valid for cases in which such investigative tools may be used under provisions originally meant for other ways of obtaining evidence.
[10] See for example formulations in Article 90ter of the Belgian Code of Criminal Procedure, Article 81-1 Luxembourgish Code of Criminal Procedure, Article 706-102-1 French Code of Criminal Procedure.
[11] Under most juridical systems within the EU searches and seizures of servers englobe the right to circumvent its security mechanisms with technical means, i.e. to use hacking techniques to access

legal basis of one of the beforementioned hacking provisions.[12] Once investigators have gained access to the server multiple information can be gathered, and other investigation- and surveillance schemes may be put in place.

The so-called Hansa case is a good example of the extensive possibilities of such an investigation. In this case, Dutch police was able to locate and seize the servers of the Hansa market, the biggest European drug trafficking platform on the darknet at the time. Previous investigations into illegal digital market places had shown that shutting such websites down only led buyers and vendors to migrate to other hidden drug markets[13]. This time, Dutch police decided to gather as much information as possible before closing the Hansa market. Therefore, they used the server-access for an innovative and remarkable storefront investigation in which they took over and operated the Hansa market for one month. Impersonating the web-sites administrators and altering with its codes and functions, law enforcement was thus able to gather a multitude of information on users of the Hansa services. For instance, they logged every user's password, analysed photo metadata and by delaying the automated encryption of messages send on the platform, police were able to save all communications in clear text, allowing for the registration of more than 10.000 home addresses of buyers.[14] Target of the operation was every individual registered on the website and using the offered services.

In the Hansa case, investigators had the advantage that they could rely on the cooperation of the two administrators of the darknet market. Both had been arrested in Germany on the ground of completely unrelated charges and were cooperative. They passed over their credentials for the Hansa platform, permitting to access the servers without the time-consuming use of hacking techniques. However, this kind of investigation can theoretically also be undertaken by circumventing the server's security mechanisms, i.e. with hacking techniques. The developments in the Hansa case, are however a good example for the investigative possibilities that the access to webservers entails.

b. Individual Surveillance

Hacking access to individual computer devices can look similar on first view: In the context of searches and seizures, law enforcement officials can gain physical access to the devices as such, allowing them to see and analyse the data stored on them. When police want to access such a device remotely and secretly in order to undertake certain surveillance schemes, they can do so based on specific provisions authorizing such investigative acts. Such provisions exist already in most of the judicial systems of EU Member States.[15] With the use of malware, usually a trojan, investigators gain access to a

---

stored data. However, this practice is not uncontested. In the context of the access to cellphones, the US supreme court decided in Riley v California (2014) that the search of contents stored on a cell phone required a specific juridical warrant. Jurisprudence of the Dutch supreme court and discussions throughout the EU Member States indicate similar considerations.

[12] See for example Article 90ter of the Belgian Code of Criminal Procedure, Article 81-1 Luxembourgish Code of Criminal Procedure, Article 706-102-1 French Code of Criminal Procedure.

[13] See extensive analysis in: D. Décary-Hétu/ L. Giommoni, 'Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous', Crime Law Soc Change [2017], 55-75.

[14] A good account of the whole investigation can be found in: A. Greenberg, 'Operation Bayonet: Inside the string that hijacked an entire dark web drug market' [2018] Wired, https://www.wired.com/story/hansa-dutch-police-sting-operation/ (Last access: 31.3.2019).

[15] See for example, §100a I 2 and §100b German Code of Criminal Procedure, Article 706-102-1 French Code of Criminal Procedure.

computer or smartphone. Undetected, such access can allow for a number of surveillance activities.[16] For instance, investigators can log all key strokes, i.e. everything typed in on a computer keyboard, and thereby gather written texts and passwords. They can also get a clear view of a person's activities on the device by taking small interval screenshots. This means taking a sort of photo, every 3-15 seconds, showing an exact copy of what is visible on the screen. It is technically also possible to turn on a device's camera or microphone remotely, permitting audio- /video- surveillance of the user and the room he/she is in. The national provisions on hacking techniques vary on the types of surveillance features they allow for.

Using these techniques can allow access not only to the data stored on the device itself, but also to data stored on remote servers, like for example a cloud. It also allows to proof a clear connection between the user and its online aliases, and for a clear reading and logging of messages that throughout their transmission process are encrypted and therefore of no use if just intercepted. Online and offline activities, as well as personal accounts can be monitored.

2. Differences Between the two Approaches

Common feature of the presented investigative measures is the use of hacking techniques to access IT systems. The technique used is similar and has the same objective: circumventing or overcoming security mechanisms. Hence, one could assume at first glance that the legal rules governing the use of hacking techniques in order to access IT systems should be governed by the same legal framework. However, it seems difficult to characterize these investigative measures only on the general permission for law enforcement to use hacking techniques. Once a system was hacked, the investigative measure is rather to be understood as an umbrella concept englobing a diversity of investigative features which in their possibilities differ substantively and lead to different legal considerations.

Primarily the two approaches differ in the number of subjects affected by the investigative measure: while one focusses on a single individual, the other enables the observation of a theoretically unlimited number of persons. In theory, both could be used in repressive as much as in proactive investigations, with the collective surveillance being particularly interesting for proactive policing because of the number of persons potentially targeted. Although illegal market places always allow police to establish a link towards already committed offences that they investigate repressively, such operations rather give access to information that can be used as investigative leads rather than that they allow for the gathering of evidence.

The collective surveillance approach does not only target a potentially high number of internet users, it also involves many more actors than the direct access to an individual computer device. Law enforcement and the investigated suspect are the only mandatory actors for the latter, but additional third parties could be involved. These could consist for example in communication partners of the investigated person, or in a bystander who uses the same computer device as the suspect. Also private companies could become involved in the investigation, for instance, if they voluntarily or compulsory cooperate with the law

[16] See some techniques described in: G. Vaciago/D. Silva Ramalho, 'Online searches and online surveillance: the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings' Digital Evidence and Electronic Signature Law Review [2016], Vol. 13, 89.

enforcement agencies by providing them with vulnerabilities in their IT-systems, which enable the hacking attack. That means, if tech-companies install backdoors or point out security shortcomings in their systems, which allow police to access them.

All these actors could potentially also appear when web-servers are accessed and taken under surveillance. But such investigations often also involve the companies that hold the web-site servers, as well as the administrators and the users of the darknet-service – as they are usually targeted for different legal activities. Such diversity of actors leads to a number of different questions regarding the conflict of jurisdiction, notification, fundamental rights protection and cooperation of law enforcement with third parties, as will be seen in the following.

3. Main Legal Consequences

The outlined differences have an impact on the legal considerations surrounding the use of hacking techniques in criminal investigations. The main legal issues concern sovereignty and jurisdiction (a.), human rights protection (b.), and cooperation with third parties (c.). They all fall back to the different investigative features that each of the investigative measures can imply (d.).

a. Sovereignty and Jurisdiction

Both individual and collective investigative measures have a strong cross-border dimension. Theoretically, technical possibilities allow in both situations direct access to stored data and to real-time surveillance all over the world. It is still under discussion which state should have or assume competence for investigative acts in cyberspace.[17] So far, one could say that EU rules foresee a distinction between the different types of investigative measures: For real time surveillance, the competence depends on the location of the investigated individual, while the competence for investigations targeting stored data should lay with the state(s) in which the data/respectively the company that is holding the data is located.[18] Investigative measures based on hacking techniques can face both features, real time and stored data searches. Not only does this call for a re-evaluation of existing rules for sovereignty and jurisdiction in cyber-investigations, it also reveals an important distinction between the two presented investigative approaches.

In the case of access to an individual computer, law enforcement targets a specific person, who has already been identified and generally located.[19] What they usually cannot predict, is where the data that they will access through the device is located. Data stored in a cloud or on other servers can theoretically be located anywhere in the world. Moreover, tech-companies use to split data packages and store them on different servers all around

[17] C. Conings 'Locating criminal investigative measures in a virtual environment. Where do searches take place in Cyberspace' Belgian Cybercrime Center of Excellence for Trainings, Research and Education: Legal Research Report [2014] 47, 54; published in Dutch in Nullum Crimen [2014] no.1, 1-25.

[18] EU Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, [2000] OJC 197 and Directive 2014/41/EU regarding the European Investigation Order in criminal matters [2014] OJL 130..

[19] Locating the surveillance target on one's territory, usually grants competence for the investigative measure to local authorities, ibid.

the world in order to optimize their transmission processes.[20] If the person and the device were to be located outside the jurisdiction of the investigating agency, mutual legal assistance or (within the EU) a European Investigation Order[21] would have to be requested.[22] Law enforcement agents in the State receiving the request could then gather the evidence under the respective legal conditions. Up to which extent cooperation or at least notification to foreign authorities would also be necessary for the access to the there-stored data, or with respect to affected third parties outside of the initial territory of the investigation, is still to be determined.

In the case of server-surveillance, the situation presents itself the other way around. Here, police are well aware of the location of the data, as the investigation concerns mainly the data stored on the infiltrated server. If the data is stored on their territory, or the company holding the server located there, these authorities could assume competence.[23] They can, however, not be previously aware of the location of all the user of an internationally accessible website. Consequently, it has to be asked whether, when and how foreign authorities have to be asked for authorization or have to be at least notified about the planned or even ongoing investigation. In the example of the Hansa case, Dutch police was the leading law enforcement agency. The seized servers were located in Lithuania, while the observed users were to be found all over Europe. Such a multi-national constellation is typical for investigations based on the hacking access to web-servers.

In any case, it seems problematic to divide the competence for one investigative measure regarding its objective. Aligning the competences for remote access to one country if the measures objective is to gather stored data and to another, when real time surveillance is intended, does not appear practicable.[24]

b. Human Rights Protection and Notification

The protection of fundamental rights holds a prominent position in the context of secret investigative measures. This general rule also applies to hacking investigations. They interfere with the right to privacy, protected by all national constitutions in the EU and by Article 8 European Convention of Human Rights and Articles 7 and 8 of the European Charter of Fundamental Rights. Arguments can be found in pro and in contra of a proportionate justification of such interference for the benefits of criminal investigations.[25] A right balance between the public interest in the fight against crime and the individual's

[20] J. Spoenle, 'Discussion paper: Cloud Computing and Cybercrime Investigations: Territoriality vs. The Power of Disposal' Project on Cybercrime Council of Europe [2010].
[21] Directive 2014/41/EU regarding the European Investigation Order in criminal matters [2014] OJL 130.
[22] Such request for law enforcement cooperation could also be necessary in cases in which the investigative person carries the computer device outside the country, for instance by using one's cellphone or laptop on a weekend trip.
[23] See for example Article 31,32 Budapest Convention on Cybercrime [2004] ETS No. 185.
[24] In Germany, the legal framework regarding the use of hacking techniques does actually foresee a similar separation. Investigative acts oriented towards the gathering of communication content is considered under §100a StPO while the remote search for stored data is authorized under §100b stop, see discussion of problematics in: T. Stadler, 'Zulässigkeit der heimlichen Installation von Überwachunssoftware – Trennung von Online-Durchsuchung und Quellen-Telekommunikationsüberwachung möglich?' MMR [2012], 18-20.
[25] See for example arguments brought forward in the judgements of the German constitutional court, which declared national provisions governing law enforcement's use of hacking techniques unconstitutional twice: BVerfG, [2008] NJW [2008] 822 and BVerfG [2016] NJW [2016] 1781.

interest in the protection of his/her privacy, depends on the exact scope of the national provisions governing such hacking techniques and on the investigative features they authorize (for instance, the use of real-time surveillance via a devices camera and microphone, etc.).

Even without a concrete scope and independent from the exact investigative aspects, one general observation can be made, which distinguishes the individual and collective surveillance schemes. Despite the high number of people affected by collective surveillance schemes, such investigations are vertically much less intrusive of fundamental rights. While hacking into a web server only enables to gather information on one aspect of online activities (in the example of the Hansa investigation only on the activities related to drug trafficking on a darknet market), direct access to personal computer devices discloses the very wide range of personal information that modern society is used to save on their computers, smartphones, clouds and online-accounts. Additionally, law enforcement can engage in particularly intrusive real-time surveillance, which could allow to log conversations and observe the target in his/her online and offline activities, from *Wikipedia* surfing to online-banking. Combining knowledge about an individual's usage of his/her cell phone or laptop with the insights of the data stored on such devices, can give information that covers nearly all spheres of a person's life. Personal data stored on personal computer devices and clouds may date back much longer than user activities on short-dated online platforms. Observing the latter gives, in consequence, only limited insights into a person's life. Targeting personal computer devices, on the other hand, permits to draw of a very complete picture of someone's character, relations and interests and is thus strongly intrusive of the right to privacy.

Human rights protection also depends on the location of the data, the investigated person and the active law enforcement agents. Jurisdiction does not only state which rules govern the investigation, but also where and how affected persons may claim a violation of fundamental rights. For individual surveillance, the investigation will mostly be governed by the legal framework of the country in which the investigated person resides.[26] Usually this will mean that one State's law enforcement agencies will act upon domestic rules, that also govern human rights protection, recourse, etc. Whether the same law enforcement agent could also be authorized to undertake the surveillance on a suspect situated in another European Member State, or even outside the EU is doubtful, at least in cases in which the authorities of the affected State did not agree to such action.

Additional questions of conflict of law concern the location of the stored data, the location of affected third parties and possible cooperation with foreign authorities. In such cases, also the question of notification arises. Recent discussions for the new rules on electronic evidence, for instance, suggest that not all affected persons, foreign authorities or other third parties, like tech-companies, need to be informed about the investigation.[27] Not even ex-post. Nonetheless effective remedies for alleged fundamental rights' violations are largely dependent on due information of the holder of the affected rights and the domestic

[26] Also in cases in which a EIO was issued, see Article 9, Directive 2014/41/EU regarding the European Investigation Order in criminal matters, 1 May 2014, OJL 130.

[27] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final, 2018/0108 (COD). See critic on the missing obligation to notification in: T. Christakis, 'E-Evidence in the EU Council: The Key Issue of when one Member State can Review the Requests from Another', Cross-Border Data Forum [2018], https://www.crossborderdataforum.org/e-evidence-in-the-eu-council-the-key-issue-of-when-one-member-state-can-review-the-requests-from-another/ (Last access, 11.4.2019).

authorities. Without adequate information about the interference with one's rights, one cannot effectively challenge the underlying measures.[28] As the concerned persons are usually also best suited to claim any privileges (professional secrets, immunities etc.) that they may have, notifications are of particular importance in this regard.

These observations are even more valid in the case of collective surveillance schemes, in which investigators are generally not able to locate or identify the targets prior to the observation. Users of a specific internet service will usually be situated all over the world, or at least all over the EU, with only a limited number of users in the country from which law enforcement is acting. A large part of the investigation will therefore rely on cooperation with the authorities of other States. Whether cooperation or authorization to undertake the surveillance measures and notifications are always sought in practice, is doubtful.

With a multiplicity of unidentified internet users targeted by an investigative measure, the question of conflict of law and the effectivity of fundamental rights protection becomes even more essential. Where can an individual, subject to such measures, seek recourse? Which law governs the execution of the measure? Will the affected person or the State authorities be notified? For yet another reason comprehensive notification appears crucial in such cases: since police are also not able to identify the individuals, who will be affected by the measure, beforehand, they cannot consider any possible privileges either. However, the observed person or the domestic authorities may find themselves in a better position to intervene and protect privileges.

c. Cooperation and Third Parties

Whenever law enforcement receives direct access to data that is usually stored by tech companies, i.e. access without the need to ask those companies to hand data over, the question arises whether such companies should work together with law enforcement and implement vulnerabilities in their system. Vulnerabilities are weaknesses within a software or computer system, which can be exploited to access the system. So far, there is no obligation for companies to provide vulnerabilities for law enforcement, but although this would imply a substantive decrease in security of the affected systems, the topic is on the table.[29]

Cooperation with companies in the context of hacking investigations can also be an issue from other angles. For instance, for the question up to which extent private companies have to be informed about vulnerabilities/ security breaches found by police or other third parties, or about law enforcement's access to data stored on their servers. In cases in which police infiltrates a web server, the provider, that is the company running the service, will often be aware of the investigation. Can companies be obliged to respect the secrecy of the investigation in this kind of situations? Can companies be obliged to give law enforcement access to data or information?[30] Also in cases in which their contract with the client states that they would disclose any data-

[28] Klass and Others v Germany, Application no. 5029/71 [1978]; Zakharov v Russia, application no. 47143/06 [2015].

[29] As many States lack the resources and technologies for elaborated hacking tools, they would often outsource the actual technology behind the attack, i.e. the technical enabling of the access to the computer system to specialized private companies. A prominent example is the Italian enterprise "Hacking Team", see http://www.hackingteam.it/ (Last access 9.4.2019)

[30] Recent international developments, like the CLOUD Act in the US and the proposal for an e-evidence Regulation in the EU, indicate that such legal obligations for companies are on the rise. It is however doubtful, up to which extent private companies would be willing to comply if such obligations existed all around the world, including in countries less respectful of the rule of law and human rights.

or cooperation request made by law enforcement?[31] This leads to the more general question of the rules that actually govern the cooperation of private companies with law enforcement agencies in these situations. Not least when it is about cooperation with a foreign company.

The need for cooperation with privates is stronger in the case of surveillance of a web server, as cooperation with the provider is essential here and as more actors are involved in general. Nonetheless, both situations pose similar legal questions.

d. The Measures/Features involved

Considerations regarding the differences between the two approaches to hacking-surveillance fall back to the different investigative possibilities they open. On the one hand, access to a personal computer device technically permits searches for on- and offline data, real-time surveillance of communications as well as on- and offline activities and even audio-video surveillance. Access to a web server on the other hand, as in the example of the Hansa case, enables cyber infiltration, storefront undercover operations and also the interception of messages and logging of private data attached to online accounts.

The investigative features involved are therefore very different. In both cases, however, it is not easy to legally classify the techniques used. Partially, these practices are legal grey-zones and not yet particularly envisaged by provisions. Some hacking activities simply fall under the national definitions (or practices) of search and seizures and the hacking provisions, although little is known about the additional investigative features such authorizations permit to undertake.

Conclusion

It is challenging to consider the two kinds of access that hacking techniques provide to computer systems under the same legal framework. Rather, both approaches appear to call for a particular legal framework, englobing the legal considerations that they imply.

Differences arise particularly in the context of the complexity of considerations regarding jurisdiction and human rights protection. Many of the questions arising are in the end defined by the technological features actually executed by law enforcement in the development of their investigation. However, the differences that characterize both investigative approaches and especially the strong interference of human rights that accompany individual hacking techniques, call for a specific legal framework with conditions adequately protecting human rights. As national legal frameworks governing hacking techniques in criminal investigations do not foresee such a distinction until now, it would be desirable to engage into a fruitful legal discussion of possible distinctions and rhetorical precisions.

Bibliography

[31] Some companies include privacy guarantee in their business model. They assure clients contractually that they would not disclose any information/ data about their clients and that they would not cooperate with Government authorities of any kind.

1. A. Greenberg, '*Operation Bayonet: Inside the string that hijacked an entire dark web drug market*' [2018] Wired, https://www.wired.com/story/hansa-dutch-police-sting-operation/

2. B. Krause '*Ermittlungen im Darknet – Mythos und Realität*' Neue Juristische Wochenzeitschrift [2018], 678-681

3. C. Conings '*Locating criminal investigative measures in a virtual environment. Where do searches take place in Cyberspace*' Belgian Cybercrime Center of Excellence for Trainings, Research and Education: Legal Research Report [2014] 43-71; published in Dutch in Nullum Crimen [2014] no.1, 1-25

4. D. Décary-Hétu/ L. Giommoni, '*Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous'*, Crime Law Soc Change [2017], 55-75.

5. D. Kipker, '*Vom Staatstrojaner zum staatseigenen Bundestrojaner – Die Evolution einer Überwachungssoftware*', ZRP [2016], 88-89

6. G. Heißel '*Überwachung und Ermittlung im Internet*' [2016]

7. G. Vaciago/D. Silva Ramalho, '*Online searches and online surveillance: the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings*' Digital Evidence and Electronic Signature Law Review [2016], Vol. 13, 88-96

8. J. Neithercutt '*Introduction to Tactical Hacking: A Guide for Law Enforcement*' [2016]

9. J.J. Oerlemans '*Investigating Cybercrime*' [2017]

10. J. Spoenle, '*Discussion paper: Cloud Computing and Cybercrime Investigations: Territoriality vs. The Power of Disposal*' Project on Cybercrime Council of Europe [2010].

11. K. Becker, B. Fitzpatrick, '*In the Search of Shadows: Investigating and Prosecuting Crime on the "Dark Web*"', United States Attorneys' Bulletin, January 2018, 41-47

12. S. Hilley '*Trojan horse powers for the police*' Digital Investigation [2007], Vol. 4, 56-58

13. T. Christakis, '*E-Evidence in the EU Council: The Key Issue of when one Member State can Review the Requests from Another'* Cross-Border Data Forum [2018], https://www.crossborderdataforum.org/e-evidence-in-the-eu-council-the-key-issue-of-when-one-member-state-can-review-the-requests-from-another/

14. T. Stadler, '*Zulässigkeit der heimlichen Installation von Überwachungssoftware – Trennung von Online-Durchsuchung und Quellen Telekommunikationsüberwachung möglich*?' MMR [2012], 18-20

15. W. Ziebarth 'Online-Durchsuchung' [2013]

THE CHALLENGES AND PERSPECTIVES FOR AN EFFECTIVE MERGER CONTROL IN DIGITAL MARKETS

Fasoula Vasiliki[1]

Abstract

Digital markets can be found in new entrepreneurial concepts, such as digital platforms, that may sometimes disrupt competition, but also in more traditional industries, such as the agrochemical sector, that are being transformed in order to meet the needs of a more sophisticated consumer in the global era of the digital industrial revolution. In rapidly changing innovative and very dynamic markets, many legal and economic experts are focusing on the adaptability of the actual substantial and procedural tools provided by European and national merger control provisions to effectively assess notified concentrations in the above mentioned markets as shown by recent cases *Dow/Dupont, Bayer/Monsato, Apple/Shazam, Microsoft/LinkedIn, Facebook/WhatsApp, Facebook/Instagram*. Some national legislators have already proceeded to an amendment of their national laws so that they can include specific provisions for digital markets. Although in the Commission's view, after a public consultation in 2016, there was no need for a "*digital amendment*" to the current European merger regulation, as most of the mergers in digital markets fall under national scrutiny, some "*digital guidelines*" would be beneficial for the European digital industry at large and the national competition authorities.

Keywords: merger control, innovation, digital markets, substantive assessment

Introduction

The design of competition policy has an impact on legislation and decision making process not only at a European but also at a national level for the Member States. The effectiveness of existing tools in order to achieve competition policy's objectives, or even the necessity to review them, is challenged each time competition policy is faced with major changes in the market environment and radical modifications of global business models or even major geo-political developments.

After the Lisbon Treaty, competition is included in the objective of the internal market under Article 3(3) of the Treaty on the Functioning of the European Union (TFEU).[2] The Lisbon Treaty removed the wording of article 3(1) (g) of the Treaty Establishing the European Community (EC Treaty) which stipulated that the activities necessary to achieve the objectives of the Community included "*a system ensuring that competition in the internal market is not distorted*" from the part of the European Treaties declaring the Union's

[1] PhD candidate in Private Law, University Paris II Panthéon-Assas, Institut de recherche en droit des affaires (IRDA) - EA 3047, with a dissertation on "Essai sur l'intégration de considérations non concurrentielles en droit des concentrations" [Study on the integration of non-competition considerations in merger control]. ATER in Private Law at the University Paris Nanterre. Research interests: Competition Law, Law & Economics, Business Law, Contract Law. Email: vicky_fasoula@hotmail.com

[2] Art. 3(3) TFEU: "[…] The Union shall establish an internal market. It shall work for the sustainable development of Europe based on balanced economic growth and price stability, a highly competitive social market economy, aiming at full employment and social progress, and a high level of protection and improvement of the quality of the environment. […]", Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union - Consolidated version of the Treaty on the Functioning of the European Union - Protocols - Annexes - Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007 - Tables of equivalences [2012] OJ C326/1.

objectives and transferred it to Protocol No 27 on the internal market and competition,[3] annexed to the Treaty on European Union (TEU) and the TFEU. The significance of the Protocol is to preserve the exclusive legislative powers of the Union in regards to competition policy on the basis of Article 352 TFEU (ex-article 308 EC),[4] which is also the legal basis for the adoption of the EU Merger Regulation (EUMR)[5] and to present fair and undistorted competition as a means to serve the objective of the internal market and not as an end in itself. The case law of the Court of Justice of the European Union (CJEU) has established that the Protocol forms a constitutive part of Article 3(3) TEU on the Union's objective of internal market.[6]

The system of European competition law provisions, including anti-competitive agreements, dominant market positions, merger control and state aid has a variety of objectives: assuring market integration, guarantying economic freedom of individuals in the market place which reflects the influence of ordoliberalism in the shaping of European competition law provisions,[7] enhancing the consumer welfare[8], providing economic efficiency.[9] It only follows that the objectives of merger control is to keep a distortion-free competition in the market that allows new suppliers to entry and that concentrations do not harm the consumer welfare.[10]

During the Conference "*Shaping competition policy in the era of digitalization*" organised by the European Commission on January 17, 2019, the Director General of the Commission's Directorate-General for Competition (DG COMP) stated that in merger control "*the application of some of the existing theories, legal texts, analytical methods and investigative procedure needs to be reconsidered to ensure that they adequately address new phenomena*".[11] The reason is that the unpredictability of dynamic markets and the evaluation of elements with no price formation invalidate the traditional economic models used in merger assessment that are based precisely on price formation. At a national level, the competition authorities faced with mergers in digital markets are increasingly relying on the input of internal documents provided by or demanded from the merging entities and in quantitative methods of economic analysis, expanding the traditional standards so that they can take into account the dynamic change of markets or the no-price considerations in

[3] Protocol n°27 on the internal market and competition, [2008] OJ C115/309 stipulates that: "THE HIGH CONTRACTING PARTIES, CONSIDERING that the internal market as set out in Article 3 of the Treaty on European Union includes a system ensuring that competition is not distorted, HAVE AGREED that: To this end, the Union shall, if necessary, take action under the provisions of the Treaties, including under Article 352 of the Treaty on the Functioning of the European Union ".

[4] J.Drexl, 'Competition law as part of the European Constitution', in 'Principles of European Constitutional Law', A.von Bogdandy & J.Bast, eds, (München: Hart Publishing 2010, 2nd edn).

[5] Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (the EC Merger Regulation) [2004] OJ L24/1 which amended and replaced the first Council Regulation (EEC) No 4064/89 of 21 December 1989 on the control of concentrations between undertakings [1989] OJ L395/1.

[6] Konkurrensverket v TeliaSonera Sverige AB, Case C-52/09 [2011] ECLI:EU:C:2011:83; Solvay SA v European Commission, Case C-109/10 P [2011] ECLI:EU:C:2011:686.

[7] C. Mongouachon, 'L'ordolibéralisme : contexte historique et contenu dogmatique' [2011] Concurrences n°4 70 ; D. Hildebrand, 'The role of economic analysis in the EC competition rules' (The Hague : Kluwer Law International 2009 3rd edn).

[8] As previous Commissioner for Competition Policy, Joaquin Almunia stated in « Competition –What's in it for consumers? », speech of 24 November 2011, "consumer welfare is the cornerstone, the guiding principle of EU competition policy".

[9] L. Parret, 'The multiple personalities of EU competition law: time for a comprehensive debate on its objectives', in D. Zimmer ed., 'The goals of competition law' (Cheltenham: Edward Elgar 2010).

[10] W. Frenz, 'Handbook of EU Competition Law' (Berlin: Springer-Verlag 2016).

[11] European Commission, Conference 'Shaping competition policy in the era of digitisation' (Brussels 2019), http://ec.europa.eu/competition/scp19/

digital innovative markets.[12] They also developed an assessment based on a theory of harm based on data protection considerations, similar to the one applied for mergers with a strong innovation, R&D, element and are working on amendments of national merger control legislation.

1. Challenges in the identification of the transactions in the digital dynamic markets that fall under merger control scrutiny

Not all transactions between firms fall under an *ex ante* merger control assessment. Most European jurisdictions apply a turnover threshold for identifying the transactions that fall under merger control provisions. The scope of application of the EUMR depends on financial thresholds as well. The European Commission has exclusive jurisdiction for mergers between firms with a combined worldwide turnover of at least €5 billion and a turnover within the European Economic Area of more than €250 million for each of them.[13] In this way, mergers can be assessed in a single procedure, and don't have to go through a number of different procedures in individual EU countries (the "one stop shop" principle). If the merging parties have more than two-thirds of their European turnover in one and same EU country, the merger is examined by the competition authority of that country because the latter is better placed than the Commission to examine its potential effects. If the above-mentioned criteria are not met, the transactions may fall under the jurisdiction of national competition authorities according to national merger control legislation.

The firms concerned are the undertaking(s) acquiring sole, or joint control and the undertaking over which control is being acquired. For the purpose of calculating the turnover of the undertaking(s) acquiring control, the turnover relating to all entities belonging to the group must be considered.[14] The emergence of transactions between undertakings in the digital industries has put into question the effectiveness of the turnover thresholds. In these sectors, the acquired company might play a competitive role, hold commercially valuable data, or have considerable market potential for other reasons despite having generated such a turnover so far that cannot meet the turnover thresholds and can go on undetected by the competition authorities. This debate has intensified since *Facebook/WhatsApp*,[15] which fell below the EU turnover thresholds. As a result of this, the European Commission carried out a consultation on the merger review process, inviting comments on the introduction of a value-based threshold.[16]

A similar debate in Germany has led to the introduction of a new merger control threshold. This allows high-value transactions were the merging companies must have a combined aggregate worldwide turnover of more than 400 million Euros. At least one of the companies must have a turnover of more than 25 million Euros and another of more than 5 million Euros in German. Previously, the deal would not have been notifiable because the target's revenues were less than 5 million Euros. In addition, there are legal exemptions for

[12] P. Dechamps, I. Fanton, 'The economics of dynamic markets : a focus on merger control' in D. Gerard, E. de Rivery, B. Meyring (eds) 'Dynamic markets, dynamic competition and dynamic enforcement : The impact of the digital revolution and globalisation on competition law enforcement in Europe' (Bruxelles : Bruylant 2018).

[13] Article 1 of the EUMR.

[14] For the specificities of the calculation of the so called 'undertakings concerned for the purposes of jurisdictional thresholds, see J.F. Bellis et alii, 'Merger Control: Jurisdictional Comparisons' (London: Sweet & Maxwell 2011).

[15] Facebook/WhatsApp, Case No COMP/M.7217, Commission Decision C(2014) 7239 final, [2014] OJ C417/57.

[16] European Commission, Consultation on Evaluation of procedural and jurisdictional aspects of EU merger control, consultation period from 07.10.2016 until 13.01.2017, http://ec.europa.eu/competition/consultations/2016_merger_control/index_en.html

companies or markets whose size is considered to be of minor importance from a macroeconomic view.[17] German competition law appears to be particularly concerned about transactions in the digital industry involving companies with a low turnover but a large potential for innovation, such as *Facebook/WhatsApp* which did not trigger a notification filing in Germany at the time. Following the example of Germany, Austria has also amended its Cartel and Competition Law Amendment Act 2017 (KartG). The new thresholds in the merger control system aim to meet the demands of an ever more dynamic economic world, and to cope with the challenges of advancing digitisation and the interlinking of the economy and society. The criterion of the transaction value of a merger is introduced as an additional, subsidiary threshold in the form of § 9 para. 4 KartG. This means that mergers involving the acquisition for a high price of companies or assets that are (still) generating low sales can be reviewed from the perspective of competition law. The aim of this threshold is thus to identify those cases where there is an imbalance between previous sales and transaction price that can be viewed as an indicator of innovative business ideas with significant market potential.[18] The two national competition authorities of Germany and Austria published, jointly, Guidelines on the value thresholds but their scope may be limited to the specifications of the two countries economic structure and corporate law.[19] At the same time, the French competition authority is planning to present new merger Guidelines within the year 2019, following a public consultation, where an *ex post* merger control in the markets that may not meet the turnover thresholds may be possible for a limited period of time after the conclusion of the concentration.[20]

2. Challenges in the identification of the relevant market in assessing transactions in the digital dynamic markets

The Commission's appraisal of concentrations is based on the definitions and standards accepted by the substantive test under article 2(2), (3) of the EUMR, called SIEC test. It examines if the notified transaction "*would significantly impede effective competition, in the common market or in a substantial part of it, in particular as a result of the creation or strengthening of a dominant position*." The same test is used by the national competition authorities to scrutinise transactions that fall under their jurisdiction. The Commission has published guidelines to provide guidance to the market operators as well as to national competition authorities and jurisdictions regarding substantive issues in the assessment of horizontal mergers[21] and non-horizontal ones.[22] In economic theory, there is no single concept that defines the notion of "*effective competition*". The Commission's decisional

[17] Act against Restraints of Competition (Competition Act – GWB) in the version published on 26 June 2013 (Bundesgesetzblatt (Federal Law Gazette) I, 2013, p. 1750, 3245), as last amended by Article 1 of the law of 1 June 2017 (Federal Law Gazette I, p. 1416), 9th amendement, http://www.gesetze-im-internet.de/englisch_gwb/englisch_gwb.html

[18] Organisation for Economic Co-operation and Development (OECD), Directorate for Financial and Enterprise Affairs, Competition Committee, 'Annual Report on Competition Policy Developments in Austria-2017' DAF/COMP/AR(2018)32.

[19] Bundeskartellamt (German competition authority), Bundeswettbewerbsbehörde (Austrian competition authority), 'Guidance onTransaction Value Thresholds for Mandatory Pre-merger Notification (Section 35 (1a) GWB and Section 9 (4) KartG)', [2018] https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Leitfaden/Leitfaden_Transaktionsschwelle.pdf?__blob=publicationFile&v=2

[20] French Competition Authority, 'Réforme du droit des concentrations et contrôle ex post', http://www.autoritedelaconcurrence.fr/doc/note_controle_expost.pdf

[21] Guidelines on the assessment of horizontal mergers under the Council Regulation on the control of concentrations between undertakings [2004], OJ C31/5.

[22] Guidelines on the assessment of non-horizontal mergers under the Council Regulation on the control of concentrations between undertakings [2008], OJ C265/7.

practice regarding in the evaluation of mergers has been consistently focusing on the effects of the concentration on the position of consumers, excluding the producers, therefore rejecting the total welfare criterion in favour of the consumer welfare one,[23] within the relevant market of the transaction. The Notice on Market Definition defines a relevant product market as comprising all those products and/or services which are regarded as interchangeable or substitutable by the consumer, by reason of the products characteristics, their prices and their intended use. Product market definition involves analysing demand-side substitution and supply-side substitution.[24] Its purpose is to define possible competitive constraints over the products or services relevant to the transaction. The competition authorities and the Commission, use the small but significant non-transitory increase in price test (SSNIP) that tries to predict the behaviour of the consumers if prices for the product or service increased permanently by 5-10% as a result of the merger.

Such an approach, based on price value, works well in traditional markets where the products or services are relatively stable, and where prices are almost the only competitive factor. In dynamic and innovative markets, however, the standard approach to market definition presents some difficulties. Mainly, innovative and dynamic markets tend to exhibit strong competition dimensions other than just price. Many online services are available for free, there is a no-price value. Instead of prices, the *Facebook/WhatsApp* and *Microsoft/LinkedIn*[25] mergers privacy and data security were considered as key parameters of competition in digital market for consumer communications. The Commission recognised data privacy as a competition parameter because privacy and security are "*becoming increasingly valued*" by consumers, that privacy "*can be taken into account in the competition assessment to the extent that consumers see it as a significant factor of quality*" and indicated that "*data privacy was an important parameter of competition between professional social networks on the market, which could have been negatively affected by the transaction*". At the same time, the Commission limited that statement to the specificities of the merging undertakings hence not allowing data privacy to become a permanent parameter for other digital markets.[26] In *Facebook/Instagram*,[27] the British Office of Fair Trade examined a transaction where Instagram had zero turnover, through the lens of competitive constraints on photo app space and supply of online display advertising, with no reference to data privacy. At the same time, the OFT recognised an international dimension of the photo app space market but a national one in regards to online advertising. Indeed, the standard approach to market definition risks defining in a static, narrow way the dynamic and innovative markets new products or even new markets are created and cannot always be predicted. Without a rigorous framework for markets serving the innovating process, the national authorities may define the relevant markets narrowly, which can lead to an excessive intervention and to market inefficiency.

[23] In paragraph 8 of Guidelines on the assessment of horizontal mergers and in paragraph 10 of Guidelines on the assessment of non-horizontal merges, we find that « Effective competition brings benefits to consumers, such as low prices, high quality products, a wide selection of goods and services, and innovation. Through its control of mergers, the Commission prevents mergers that would be likely to deprive customers of these benefits by significantly increasing the market power of firms ».

[24] Commission Notice on the definition of relevant market for the purposes of Community competition law [1997] OJ C372/5, paras 7, 26.

[25] Microsoft/LinkedIn, Case M.8124, Commission Decision C(2016)8404 final, [2016].

[26] S. Esayas, 'Data privacy in European merger control: critical analysis of Commission Decisions regarding privacy as a non-price competition' [2019] ECLR 2019, 40(4).

[27] Facebook/Instagram, OFT's Decision on the Anticipated acquisition by Facebook Inc of Instagram Inc ME/5525/12.

3. Challenges in the identification of the most appropriate toolkit for assessing mergers in digital dynamic markets

In traditional markets, the consumer welfare criterion prevails over price discrimination and reduction of production costs for the merging parties in order to clear a notified transaction. If a merger harms consumer welfare, it must be prohibited. However, there has not been an objective measure of how much of a reduction must there be noted for a merger to be prohibited. Merger control uses the counterfactual method for its forward-looking approach. This method is a comparison to the market situation without the merger with a situation where the merger occurs, and determines which situation may impede the effective competition. The counterfactual is effective when markets are in some kind of steady state and actual market conditions are considered a good predictor of future market conditions, taking into account some adjustments of simple market dynamics.[28] Mergers in markets where technology evolves rapidly require a prediction of the technological pace going forward and the likely winners and losers, even absent the transaction. Innovative markets in the digital economy were business models are based on the use of consumer data raise even more issues, as whole markets can be completely replaced by new ones in a short timeframe, thus making the assessment more speculative.[29]

Most of the tools that are available for understanding market outcomes arising from mergers are static, and focus on expected price changes or reduction in quality, innovation or choice of products and services. Competition authorities rely on evidence provided by the merging parties and on quantitative investigative techniques in order to predict the consumer welfare harm in the relevant markets affected by the merger. [30] In order for the Commission to make an overall assessment of the merger, the Commission uses the information provided by the merging parties through the notification form (Form CO) and questionnaires or costumer surveys, past information costumer preferences on prices and costs, internal documents provided by the parties or obtained during a surprise inspection of the merging undertaking's premises.[31] Other evidence that can be used may be provided by third parties like competitors, customers, suppliers of the merging undertakings, through public invitations to comment on a notified transaction or responses to written requests for information.[32] As the Commission is trying to find patterns in the markets in order to facilitate the prediction of the post-merger effects on prices, it may also rely on direct evidence of the conduct and performance of suppliers and economic firms in the market and on econometric techniques. The CJEU has established that there is no hierarchy between technical and non-technical evidence and that "*it is the Commission's task to make an overall assessment of what is shown by the set of indicative factors used to evaluate the competitive situation. It is possible, in that regard, for certain items of evidence to be prioritised and other evidence to be discounted*".[33] The examination of that evidence and the associated reasoning is subject to judicial review of legality of Commission's decisions on concentrations.

---

[28] P. Papandropoulos, 'The implementation of an effects-based approach under article 82: Principles and applications' in I. Kokkoris, I. Lianos (eds), 'The Reform of EC Competition Law: New Challenges' (Alphen aan den Rijn: Kluwer Law International 2010).

[29] C. Rusu, A. Looijestijn, M. Veenbrink, State of the art and prospective Directions in the Digitalisation of economic law', in C. Rusu, A. Looijestijn, M. Veenbrink (eds) 'Digital Markets in the EU' (Oisterwijk : Molf Legal Publishers 2018).

[30] A. Lindsay, A. Berridge, 'The EU Merger Regulation : substantive Issues', (London : Sweet&Maxwell, 5th ed. 2017).

[31] Article 13 of the EUMR.

[32] DG Competition, Best Practices on the Conduct of EC Merger Control Proceedings, para 27

[33] Deutsche Börse AG v European Commission, Case T-175/12 [2015] ECLI:EU:T:2015:148, para 133.

In recent decisional practice, competition authorities have considered the effect of consolidation on innovation and investment from two different perspectives: as a theory of harm, and as a dynamic efficiency. On the one hand, in traditional markets authorities have often evaluated the mergers between two innovators can undermine the incentives and ability of the merging parties to continue innovating. In such sectors, authorities have adopted a strict approach to the assessment, leading to concerns of over-enforcement in the area usually by the demand of heavy remedies. On the other hand, in digital markets authorities have often accepted that consolidation in innovation will produce large welfare benefits in the long run. In these cases, there is an open debate about whether lack of enforcement *ex ante* through merger control, because of the transactions that could not meet the turnover thresholds for merger scrutiny led to more stringent enforcement *ex post* through antitrust investigation leading up to heavy fines that could have been avoided; this would apply for example in the case of Google, that has allegedly abused dominant position in some markets years after having been allowed to acquire DoubleClick and Youtube.[34]

When assessing innovation in traditional but dynamic markets the theory of harm is severely appreciated. In the *Dow/DuPont*[35] merger in the agrochemical sector the Commission was concerned that the merger would reduce innovation both in improving existing products and in bringing new ones to the market. Commission found that the merged entity would have lower incentives and a lower ability to innovate than Dow and DuPont did separately, and the merged entity would be likely to cut back on the amount it spent developing innovative products. The decision was criticised as proof of over-enforcement in a sector where the entry of new firms is high unlikely due to the immense sunk costs[36] on infrastructure and licences needed.[37] In the *Bayer/Monsato*[38] mega merger in the same agrochemical sector, there were horizontal, vertical and conglomerate effects in the seeds markets, in crop protection products in the domain of digital agriculture. Both firms had overlapping activities in digital farming, disposing high capabilities in landing innovation and R&D technological platforms on smart farming value chains using free public data on agriculture combined with private data collected by farmers in order to provide farmers with package solutions to maximise theirs fields' capability. The effects of the merger would probably increase prices that would harm smallholder farmers. In the period 2000 - 2010, European farmers faced increases in prices of seeds and planting stock by 30%.[39] Despites the remedies on that case, the agrochemical sector remains highly concentrated with steadily increasing prices.

When assessing innovation in purely digital markets, the increased concentration on the digital space has been treated more favourably by the competition authorities. They refrain from demanding any remedies from the firms in order for the concentration to be compatible with the internal market. A number of mergers in the digital space have been found not to be problematic and in several cases authorities have even considered that innovation made anticompetitive effects less likely. In the *Apple/Shazam* case,[40] the value of the use of the data was not problematic because of their replicability by other means of

[34] G. Accardo et alii, 'Internet and Antitrust : An overview of EU and national case law [2018] Concurrences n°87105.
[35] Dow/Dupont, Case M.7932, Commission Decision C(2017) 1946 final [2017] OJ C356/60.
[36] Sunk costs are the costs the firm cannot recuperate if it decides to exit the market in a short period of time after entering it.
[37] G. Federico, 'Horizontal mergers, innovation and the competitive process', JECP [2017] vol. 8, n.10.
[38] Bayer/Monsato, Case M.8084, Commission Desicion C(2018)1709 final [2018] OJ C459/61.
[39] I.Lianos, D.Katalevsky, 'Merger activity in the factors of protection of segments of the food value chain-Acritic on assessment of the Bayer/Monsato Merger', Policy Papers Series 2017/1, Center for Law, Economics and Society (CLES), London, Faculty of Law, UCL.
[40] Apple/Shazam ; Case M. 8788, Commission Decision C(2018) 5748 final [2018] OJ C417/61.

digital communications, therefore, they were not offering a competitive advantage that could foreclose the market to potential competition from new entrants. In other cases, the Commission has noted that high market shares of the parties might turn out to be ephemeral in fast-growing sectors characterised by frequent market entry and short innovation cycles.[41] For example, in *Facebook/WhatsApp*, the Commission noted that the high market shares of the parties were not a cause for concern, due to the innovative and fast-growing nature of the consumer communications sector. Among the evidence supporting this decision, the Commission cited the example of BlackBerry, which previously held a significant market position but lost importance with the emergence of multi-platform apps once Android and iOS devices gained a large share of the smartphone market.

Conclusion

In competition law enforcement, digital markets are also described as dynamic markets or innovative markets. They have been "disrupting" the traditional legal and economic standards used in the assessment of transactions that do not involve digital markets and there are strong indications that they may be the future of the European industry. The Commission refused to proceed to a "digital amendment" of the current European merger control. Therefore, the national competition authorities are forced to take their own initiatives, if and when assessing these markets, without any guiding by the Commission that may in long term harm the development of an integrated European industry facing global competition. Creating a specific framework for the evaluation of the many different varieties of digital markets that exist in different kinds of traditional or "new-born" industries, or even promoting an *ex post* merger control could provide legal security to potential new entrants in the market and more reliable economic evidence. Finally, a precise framework would also allow for the courts to proceed to an effective judicial review of the Commission's reasoning in decisions regarding merger control, including decisions on remedies, guarantying the legitimacy of the Commission's powers.

Bibliography

1. A. Lindsay, A. Berridge, 'The EU Merger Regulation: substantive Issues', (London : Sweet&Maxwell, 5th ed. 2017).
2. Act against Restraints of Competition (Competition Act – GWB) in the version published on 26 June 2013 (Bundesgesetzblatt (Federal Law Gazette) I, 2013, p. 1750, 3245), as last amended by Article 1 of the law of 1 June 2017 (Federal Law Gazette I, p. 1416), 9th amendement, http://www.gesetze-im-internet.de/englisch_gwb/englisch_gwb.html
3. Apple/Shazam ; Case M. 8788, Commission Decision C(2018) 5748 final [2018] OJ C417/61.
4. Article 13 of the EUMR.
5. Bayer/Monsato, Case M.8084 [2018] OJ C459/61, Commission Desicion C(2018)1709 final.
6. Bundeskartellamt (German competition authority), Bundeswettbewerbsbehörde (Austrian competition authority), 'Guidance onTransaction Value Thresholds for Mandatory Pre-merger Notification (Section 35 (1a) GWB and Section 9 (4) KartG)', [2018]

[41] A. de Streel, 'Big Data and market power 'in D. Gerard, E. de Rivery, B. Meyring (eds) 'Dynamic markets, dynamic competition and dynamic enforcement : The impact of the digital revolution and globalisation on competition law enforcement in Europe' (Bruxelles : Bruylant 2018).

https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Leitfaden/Leitfaden_Transaktionsschwelle.pdf?__blob=publicationFile&v=2

7. C. Mongouachon, 'L'ordolibéralisme : contexte historique et contenu dogmatique' [2011] Concurrences n°4 70

8. C. Rusu, A. Looijestijn, M. Veenbrink, State of the art and prospective Directions in the Digitalisation of economic law', in C. Rusu, A. Looijestijn, M. Veenbrink (eds) 'Digital Markets in the EU' (Oisterwijk : Molf Legal Publishers 2018).

9. Commission Notice on the definition of relevant market for the purposes of Community competition law [1997] OJ C372/5, paras 7, 26.

10. Commissioner for Competition Policy, « Competition –What's in it for consumers? », speech of 24 November 2011, "

11. Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union - Consolidated version of the Treaty on the Functioning of the European Union - Protocols - Annexes - Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007 - Tables of equivalences [2012] OJ C326/1.

12. Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (the EC Merger Regulation) [2004] OJ L24/1 which amended and replaced the first Council Regulation (EEC) No 4064/89 of 21 December 1989 on the control of concentrations between undertakings [1989] OJ L395/1.

13. D. Hildebrand, 'The role of economic analysis in the EC competition rules' (The Hague : Kluwer Law International 2009 3rd edn).

14. Deutsche Börse AG v European Commission, Case T-175/12 [2015] ECLI:EU:T:2015:148, para 133.

15. DG Competition, Best Practices on the Conduct of EC Merger Control Proceedings, para 27

16. Dow/Dupont, Case M.7932, Commission Decision C(2017) 1946 final [2017] OJ C356/60

17. European Commission, Conference 'Shaping competition policy in the era of digitisation' (Brussels 2019), http://ec.europa.eu/competition/scp19/

18. European Commission, Consultation on Evaluation of procedural and jurisdictional aspects of EU merger control, consultation period from 07.10.2016 until 13.01.2017,
http://ec.europa.eu/competition/consultations/2016_merger_control/index_en.html

19. Facebook/Instagram, OFT's Decision on the anticipated acquisition by Facebook Inc of Instagram Inc ME/5525/12.

20. Facebook/WhatsApp, Case No COMP/M.7217, Commission Decision C(2014) 7239 final, [2014] OJ C417/57.

21. French Competition Authority, 'Réforme du droit des concentrations et contrôle ex post', http://www.autoritedelaconcurrence.fr/doc/note_controle_expost.pdf

22. J.F. Bellis et alii, 'Merger Control: Jurisdictional Comparisons' (London: Sweet & Maxwell 2011).

23. G. Accardo et alii, 'Internet and Antitrust : An overview of EU and national case law [2018] Concurrences n°87105.

24. G. Federico, 'Horizontal mergers, innovation and the competitive process', JECP [2017] vol. 8, n.10.

25. Guidelines on the assessment of horizontal mergers under the Council Regulation on the control of concentrations between undertakings [2004], OJ C31/5.

26. Guidelines on the assessment of non-horizontal mergers under the Council Regulation on the control of concentrations between undertakings [2008], OJ C265/7.
27. I.Lianos, D.Katalevsky, 'Merger activity in the factors of protection of segments of the food value chain-Acritic on assessment of the Bayer/Monsato Merger', Policy Papers Series 2017/1, Center for Law, Economics and Society (CLES), London, Faculty of Law, UCL.
28. J.Drexl, 'Competition law as part of the European Constitution', in 'Principles of European Constitutional Law', A.von Bogdandy & J.Bast, eds, (München: Hart Publishing 2010, 2nd edn).
29. Konkurrensverket v TeliaSonera Sverige AB, Case C-52/09 [2011] ECLI:EU:C:2011:83
30. L. Parret, 'The multiple personalities of EU competition law: time for a comprehensive debate on its objectives', in D. Zimmer ed., 'The goals of competition law' (Cheltenham: Edward Elgar 2010).
31. Microsoft/LinkedIn, Case M.8124, Commission Decision C(2016)8404 final, [2016].
32. Organisation for Economic Co-operation and Development (OECD), Directorate for Financial and Enterprise Affairs, Competition Committee, 'Annual Report on Competition Policy Developments in Austria-2017' DAF/COMP/AR(2018)32.
33. P. Dechamps, I. Fanton, 'The economics of dynamic markets : a focus on merger control' in D. Gerard, E. de Rivery, B. Meyring (eds) 'Dynamic markets, dynamic competition and dynamic enforcement : The impact of the digital revolution and globalisation on competition law enforcement in Europe' (Bruxelles : Bruylant 2018).
34. P. Papandropoulos, 'The implementation of an effects-based approach under article 82: Principles and applications' in I. Kokkoris, I. Lianos (eds), 'The Reform of EC Competition Law: New Challenges' (Alphen aan den Rijn: Kluwer Law International 2010).
35. Protocol n°27 on the internal market and competition, [2008] OJ C115/309
36. S. Esayas, 'Data privacy in European merger control: critical analysis of Commission Decisions regarding privacy as a non-price competition' [2019] ECLR 2019, 40(4).
37. Solvay SA v European Commission, Case C-109/10 P [2011] ECLI:EU:C:2011:686.
38. W. Frenz, 'Handbook of EU Competition Law' (Berlin: Springer-Verlag 2016).

CAN GOOD LAW BE TRUE TO SCIENCE? THE CASE OF RELIGIOUS FEELINGS IN POLISH CRIMINAL LAW

Julia Wesołowska[1]

Abstract

This text uses a Polish regulation which penalizes the offence of religious feelings as a conceptual anchor to theorize on the possibility of a future, science-based law. The objective is not so much to render the legal protection of religious feelings scientifically sound, but rather to use that example to identify and explore potential problems, threats and perspectives associated with building law based on science. Such a futurist vision, reconstructed from the bits and pieces of knowledge from precedent cases, commentaries, and controversial innovations, is no less distant than it is interesting. Reflecting on a possibility of science- and technology-based law affords a fresh perspective and uncovers implicit assumptions and intuitions.

Keywords: religious feelings, neurolaw, future law, Polish law, law and science

Introduction

Article 196 of the Polish Penal Code states: "Who offends the religious feelings of others by publicly insulting an object of religious worship or a place of religious worship, is liable to pay a fine, have his or her liberty limited, or be deprived of his or her liberty for up to two years"[2]. This regulation is one of the most controversial and troublesome parts of Polish law; despite an ongoing debate in the legal doctrine and several Highest Court rulings, Polish legal actors are still unsure as to how interpret it. Much of this confusion stems from the fact that the regulation uses the term "religious feelings". While some scholars treat it as a conventional phrase and a sort of an umbrella term for convictions and ideology, others yet are convinced of the psychological dimension of religious feelings. They produce various hypotheses concerning the nature of religious feelings: their object, duration, intensity, and the people who can experience them. However, their conception is wildly unrealistic when compared even to soft psychological knowledge, and even more so – to cognitive neuroscience's discoveries.

The law we use still for the most part appears to rely on folk psychology. However, the neuroscientific revolution, or the "cognitive turn"[3], continues to enter legal systems. Convictions are overturned and sentences mitigated based on brain scans. Intelligent algorithms are used to predict whether the offender should be released on bail. These seemingly small instances are nevertheless progressing at a rapid pace: between 2005 and

1 Julia Wesołowska is a PhD Candidate in the Philosophy of Law and Legal Ethics Department at the Jagiellonian University (Cracow, Poland). Her main research interest are emotions in law. Other academic interests include broader reflection at the intersection of cognitive science and law.

2 The Republic of Poland, The Act of June 6, 1997 – Penal Code [1997] Journal of Laws of the Republic of Poland 1997 no. 88 item 53.

3 S. Pinker, 'The Cognitive Revolution' [2011] Harvard Gazette, accessed at: https://news.harvard.edu/gazette/story/2011/10/the-cognitive-revolution.

2012, the number of cases involving neuroscientific evidence more than doubled[4]. In what way could we punish someone in an increasingly neuroscience- and technology-reliant society for, say, the offence of religious feelings? To illustrate: imagine that a hundred years from now, a technocratic, advanced society lands back on Earth after a catastrophic event. As fate would have it, they land back in Poland. A scrap of the old order is preserved: among ruins, there lies a part of Polish Penal Code with its article 196. Imagine that the new humans, perhaps as a tribute to their ancestors, decide to implement and exercise this law. The question that governs this work is: how would they go about that? In other words: how would the Polish regulation fare in such a world, with all its constituents, among which are neuroscience replacing our folk psychology and technology creeping in place of formal procedures. What would 'Religious Feelings Law 2.0' look like and what would it entail?

To do that, we must identify how we can link the current regulation with its prospective development and the problems that provokes. Therefore, I propose a twofold structure of the text, each one build around a leading question. The first part of the text examines the "How?" of Law 2.0 by introducing technical and procedural aspects of such modification. Namely, it looks into the technologies and tools which are (or will be) at our disposal and how would they be used in reinterpreting the regulation at hand. Among others, it asks questions about determining the nature and occurrence of religious *feelings* (and offence thereof), the possibility of a computer legal decision maker, and the ways in which technology could facilitate the detection of the offence. The second part would focus on the "So what?" of Law 2.0 by reflecting on deeper theoretical issues brought about by the use of tools and technologies described in part one. In other words, it reflects on jurisprudential, moral and societal issues resulting from the reinterpretation of law in a futuristic world. What is of interest are the possible new meanings assigned to crucial legal notions, such as *intent*, *free will*, or *punishment*. The text ends with a short conclusion, which attempts to answer the question: Would Law 2.0 still be law? Would it be good law? What challenges result from the attempt to adapt scientifically-based regulations and what could be possible solutions?

1. The "How" Of Law 2.0

In this part I investigate the techniques and tools which could contribute to creating and implementing the 'Religious Feelings Law 2.0'. Three such aspects are analysed: firstly, cognitive neuroscience and its use in law; secondly, computer programs performing legal functions and, in this way, replacing some parts of the legal process, and finally, the computer judge as an alternative to the classic court. The question behind this part of my work is: how would law look like if we used new programs and techniques to refine it?

As for now, neuroscientific tools are used in law mainly to demonstrate that the brain of the offender malfunctions[5]. However, in the future they could be used to assess whether a breach of law – in this case, an offence to religious feelings – occurred. To do this, such tools would have to be able to detect religious feelings, or religious emotions in a first place. This function, however, entails the need to detail what is meant by the term, i.e. the interpretation of central terms: feelings and emotions. This can vary depending on the theoretical framework one assumes. For example, Antonio Damasio reserves the term

4 G. Miller, 'The Brain Gets Its Day in Court' [2016] The Atlantic, accessed at: https://www.theatlantic.com/science/archive/2016/03/neurolaw-brain-scans-court/471615.

5 D. W. Denno, 'The Myth of the Double-Edged Sword: An Empirical Study of Neuroscience Evidence in Criminal Cases' [2015] 56 B.C.L. Rev. 493.

'emotions' for "non-conscious processes mapped in the body and brain in response to emotionally competent stimuli"[6], and what he calls feelings, that is conscious and distinct experiences of anger, joy etc. most of today's neuroscientist would term emotions. Curiously, Polish law uses the term 'feelings' much like Damasio, meaning, in fact, instances of various emotional experiences connected with religion.

After what is meant by feelings is clarified, we need to search for their specifically religious variety, and attempt to operationalize them and map them to biological constituents. There is no doubt that feelings in themselves have no specific 'variations' - at least not ones that can be neurologically analysed, so thought of *sui generis* religious emotions must be abandoned[7]. Law 2.0's best hope would be to turn towards the neuroscience of religious experience in its affective and cognitive entirety. As Polish doctrine currently restricts the protection of the regulation to religious people (personal history and self-reports are used as a criterium), perhaps in the new legal framework neuroimaging could serve as a proof that a person is religious, i.e. capable of a religious experience. McNamara tentatively maps out the neuroanatomy of a religious self to operationalize religiosity for empirical testing: "Deep to the temporal lobes and within the limbic system are two structures that are particularly important for the Self: the hippocampus and the amygdala."[8] An activation in these areas in confrontation with religious imagery or text could be the neurological indicator of a person having religious feelings, which would eliminate the need for looking into personal history or relying on self-reports.

Law 2.0 then needs to find an operational way to determine that the offence to religious feelings occurred. In this case, it would be most productive to distinguish emotions provoked by an offence or an insult: according to Poggi and D'Errico, the emotional 'definition' of feeling offended entails "humiliation, anger, bitterness, sadness, rancor, the feeling of being misunderstood, impotence, and annoyance"[9]. What would need to be proven in our scenario is that such feelings have arisen as a result of experiencing an insult to one's religion. Here, the following approach could work: rather than structural neuroimaging, one might observe the physiological response of the subjects (heart rate, skin conductivity, temperature, perspiration, and/or facial muscle movements) during an exposure to a given stimulus. In other words, if everyone was equipped with a small device measuring some of the above-mentioned parameters, and if they were able to show that spikes in them (associated with appropriate emotions) correlated temporally with the supposed offence of religious feelings, we would be provided with valuable evidence. Keeping these sorts of records, however, raises serious question about the right to privacy and to avoid self-incrimination. Physiological fingerprint pointing to anger could be indicative of committing other transgression: a suspect's emotions could betray them. Furthermore, as studies of the fingerprint approach are being conducted, detecting particular kinds of emotions could prove more challenging[10].

6 T. A. Maroney, 'Law and Emotions: The proposed taxonomy of an emerging field' [2006] 30 Law Hum Behav 119, p. 124.

7 A. Taves, 'Ascription, attribution, and cognition in the study of experiences deemed religious' [2008] 38 Religion 125, p. 125.

8 P. McNamara, 'The Neuroscience of Religious Experience' (New York: Cambridge University Press 2009) 64.

9 I. Poggi, F. D'Errico, 'Feeling Offended: A Blow to Our Image and Our Social Relationships' [2018] 8 Frontiers in psychology 2221, p. 2223.

10 E.H. Siegel et.al, 'Emotion Fingerprints or Emotion Populations? A Meta-Analytic Investigation of Autonomic Features of Emotion Categories' [2018] 4(144) Psychological Bulletin 343.

Not only neuroscience, but also computer technology could prove useful in applying article 196 of the Polish Penal Code in the future. It could be possible to create a computer program which would detect the clues that an offence to religious feelings occurs. Such technology could be inspired by the algorithm COMPAS which aided United States judges in deciding the probability of recidivism and the advisability of pre-trial release[11]. COMPAS is said to use statistical analysis in order to compare the markers in the case at hand with the database to help determine the probability of recidivism or escape from custody. How it could work in our case? Imagine that we have a powerful AI algorithm. We could program it so it would associate certain kinds of data (e.g. visual or text inputs) as offensive. Such a database could start with programming based on evidence from past trials (e.g. images and phrases determined to insult religious feelings). This could be supplemented with empirical trials determining the statistical probability of certain content being offensive to religious sentiments. In the best case, deep learning would enable the AI to take this basis and teach itself about the kinds of visual and language inputs that are prone to offending religious feelings, and in case of detection of such kind of stimuli it would be able to alert to the possibility of committing a crime and later serve as proof.

The above reflections indicate that 'Religious Feelings Law 2.0' would alter also the job profile of lawyers. Not only computer algorithms could replace expert witnesses, as in the case of COMPAS, also the most important decision-makers in the courtroom – judges and where applicable, juries, would face new demands. After the implementation of Law 2.0, the evidence would consist of brain scans and neurophysiological data, next to (or instead of) photographs and testimonies. These new kinds of evidence necessitate a new kind of interpretation. To ensure a just verdict, a judge would have to correctly infer facts from raw results and turn them into norms. This involves a creation of an *ad hoc* theory of mind, i.e. the hypotheses about connection between brain and behaviour, which often proves problematic. In this case, the intent to offend emotions or lack thereof, as well as the hurt feelings, would have to be coordinated by judge with hard data. One solution to this problem – aside from training legal professionals in neuroscience and philosophy of mind – is to bypass the middle step and infer directly from neuroimaging results to law. In line with the increasing workplace automation predicted by some visionaries, these tasks could be delegated to a new kind of judges – ones not of flesh and blood (and often, human mistakes) but digital ones[12].

The computer judge is a subject of a long debate both in the scientific community and the general public[13]. The famous research citing judges dishing out stricter sentences when they are hungry[14] or juries' decisions being influenced by upsetting evidence[15] is for some authors a proof of the inability of a human mind to escape its own emotions and dispassionately deliver justice. Powerful AIs using algorithms to analyse the evidence and perform legal syllogisms are proposed as an alternative. The main problem with the computer judge is the question if one needs to be human, or more specifically – possess a kind of cognitive apparatus that is typical to humans, including feelings, to be a good judge.

11 A. Dike, 'Would You Trust an Artificially Intelligent Expert?' [2017] National Law Review, accessed at: https://www.natlawreview.com/article/would-you-trust-artificially-intelligent-expert.

12 'Artificial intelligence is coming for both judges and defendants' [2018] New York Post, accessed at: https://nypost.com/2018/01/31/artificial-intelligence-is-coming-for-both-judges-and-defendants.

13 A. D'Amato, 'Can/Should Computers Replace Judges?' [1977] 11 Georgia Law Review 1277.

14 Z. Corbyn, 'Hungry Judges Dispense Rough Justice' [2011] Scientific American, accessed at: https://www.scientificamerican.com/article/hungry-judges-dispense-rough-justice.

15 D. Bright, J.Goodman-Delahunty, 'Gruesome Evidence and Emotion: Anger, Blame, and Jury Decision-Making' [2006] 30 Law and human behavior 183.

Feelings, conceived normally as obstacles to fully rational and dispassionate thinking, are what disqualifies human judge in comparison with a computer one, at least in the view of most. Polish law is again an outlier, as the commentators of article 196 postulate that empathy in the courtroom is necessary for proper protection of religious feelings. Currently, much of Polish doctrine demands an expert opinion for the determination whether an offence to religious feelings occurred, with one reservation – some request that the expert should be able to experience them herself[16]. Employing a computer judge would eliminate the need to empathize with religious feelings of the plaintiff, replacing self-reports and folk-psychology with highly specialized data – that is, unless we learn to program emotions on machines.

2. Thinking About Law with Mind in Mind

The unalienable part of drafting and applying law is to describe what happens when it is broken and enforce these consequences. The analysed article is situated in the Polish Penal code. That means that in each instance of applying this law, *intent* and *responsibility* is to be determined and *punishment* is to be dealt in accordance with theories of criminal law. These categories and theories are very old and deeply ingrained into the fabric of not only law, but also society. However, these assumptions are now being undermined by neuroscience stepping into the courtroom. This new presence is marked not only by new techniques and tools – the use of such methods comes with a more fundamental shift below the surface. There are many voices that the marriage between law and neuroscience, dubbed *neurolaw*, has a potential to transform most fundamental assumptions of legal system, and the goal of this part is to theorize on this impact with regards to Law 2.0 and the Polish regulation.

The discussion about the consequences of Law 2.0 should start with analysing the transformative potential of neurolaw – an attempt should be made to extrapolate the theorists' comments to reflect about possible consequences. What is meant by neurolaw is most typically the use of brain imaging evidence as a mitigating factor in criminal proceedings. In an increasing number of cases, this leads to less severe punishments for criminals. This in turn provokes public debates and warnings against a "brain overclaim syndrome"[17] and neural reductionism or determinism. These are the phenomena that could potentially impact underlying categories used to divide the legal actors into the wronged and the wrongdoer, and label actions as illegal. To use the example at hand, imagine that in the case of religious feelings, the offender, who, say, posted a caricature of Jesus on social media, presents as evidence his brain scan. His attorney points to the frontal lobe, indicating the loss of brain matter and citing as reason childhood malnutrition, alcohol overuse and several head traumas during the defendant's life. This, the lawyer argues, explains the defendant having diminished control over his impulses and difficulty in recognizing what is socially acceptable, and thus should be taken as a mitigating factor. This line of defence was already used with some success in the American courts[18]. Imagine further, that in Society 2.0 not only the brain injury defence will become more common, but some day in court the

16 G. Jędrejek, T. Szymański, 'Prawna ochrona uczuć religijnych w Polsce. Próba oceny dotychczasowych rozwiązań, czyli o rozdźwięku pomiędzy literą prawa a jego aplikacją' [2002] Studia z Prawa Wyznaniowego vol. V, p. 183.

17 S.J. Morse, 'Brain Overclaim Syndrome and Criminal Responsibility: A Diagnostic Note' [2006] 117 Faculty Scholarship at Penn Law 397.

18 G. Miller, 'Did Brain Scans Just Save a Convicted Murderer from the Death Penalty?' [2013] WIRED, accessed at: http://www.wired.com/wiredscience/2013/12/murder-law-brain.

defence conducts a replication of the Libet experiment[19] (famous for supposed empirical confirmation of the lack of free will) in order to demonstrate that the defendant does not have free will; that their experience of conscious control only follows, and does not precede, the choice already made by their nervous system[20]. How could legal categories and theories of law change as a result of that, and what effects would it have on the society?

The most potential for redefinition lies with the legal doctrine of *mens rea* – the guilty mind. Intent appears to be one of the most crucial concepts in criminal cases, and so it is in the present case, as offence of religious feelings is an intentional crime[21]. It may be more productive to consider this problem within broader notions of free will and responsibility, as *mens rea* is a problematic issue as it is not readily translatable to neuroanatomical data. Pardo and Patterson underline that "intentions are not brain processes or inner feelings, nor are they the neural activity that precedes an internal process or feeling"[22]. Knowledge is not a brain state, as far as we know it. We can only speculate on the consequences if it was possible, in real times, to map out neurological states to particular intentions. It would certainly place the capacity to act at the forefront, as Pardo and Patterson noted[23]. This poses a practical question: would a brain state reflecting an intention, together with the capacity for that intention constitute a basis for criminal responsibility? If that would be the case, one would have to punish for murderous thoughts of drivers stuck in traffic; after all, there is little stopping them from storming out of their car; and, similarly, one would have to punish just for thinking of offending religion. If brain imaging were to happen in real time (again a fantasy of distant future) this raises question about the privacy of our thoughts and the bizarre possibility of law to become our quasi-conscience.

As neuroscience enters law, the need to re-evaluate the vision of *free will* becomes imminent – are we in control of our actions, or are they either predestined or random? The question pondered for centuries appears to demand an instant answer. Greene and Cohen stirred the debate in the legal community by taking *the lack* of free will as a given. They searched for the origins of this change in the moral and social roots of law and not law itself: "new neuroscience will change the law, not by undermining its current assumptions, but by transforming people's moral intuitions about free will and responsibility. This change in moral outlook will result (...) from a new appreciation of old arguments, bolstered by vivid new illustrations provided by cognitive neuroscience"[24]. However, our everyday experience makes us sceptical towards lack of free will. The change Greene and Cohen talk about would only be possible when society's intuitions change. In that case, law about religious feelings would prove problematic, as in its current form it clearly frames offending religious sentiments as wrong. In the neurodeterministic world of Law 2.0, notion of wrongness would lose its gravity. Imagine that a person would have been found to possess appropriate intent and capacity to act at the time the crime was committed, which would indubitably make her guilty. However, the new doctrine of legal determinism does not allow to ascribe *responsibility*. How to account for the penal part of the regulation? The transformative potential of no free will doctrine translates to a change in punishments.

19 P.G.H. Clarke, 'The Libet Experiment and its Implications for Conscious Will' [2013] Faraday Paper no. 17, accessed at: https://www.bethinking.org/human-life/the-libet-experiment-and-its-implications-for-conscious-will

20 'Free Will and Neuroscience' accessed at: https://wmpeople.wm.edu/asset/index/cvance/libet.

21 J. Wojciechowska,'Komentarz do artykułów 117–221' (in:) A. Wąsek (ed.), 'Kodeks karny. Cześć szczególna' (Warszawa: CH Beck 2006) 782–783.

22 M.S. Pardo, D. Patterson, 'Minds, Brains, and Law' (New York: Oxford University Press 2013) 132.

23 Pardo, Patterson, ibidem, 134.

24 J. Greene, J. Cohen, 'For the Law, Neuroscience Changes Nothing and Everything' [2004], 359 Phil. Transactions Royal Soc'y London B 1775, p. 1775.

Because of their views, Greene and Cohen would see the penal system changed, by abolishing *retributivism*, which is one of the strong drives of punishing for the most of human history[25]. They vouch for a "progressive, consequentialist"[26] approach to punishment instead. Consequentialism could assume the form of underlining the "deterrent effect of the law and the containment of dangerous individuals."[27] If Law 2.0 was to do away with the concept of free will as ordinarily conceived of by law, one would have to deeply rethink the catalogue of punishments prescribed by Polish regulation. All three forms: fine, restriction of freedom and jail time are, in some way, retributive in nature and exert unpleasant consequences over the offender. Seemingly innocent nature of this crime further complicates the matter: it does not seem that a person who insulted religious objects is so dangerous to the society that they must be contained, as in case of murder. The choice of 'Religious Feelings Law 2.0' is as follows: either prescribe containment in lenient conditions, or become a *lex imperfecta*, that is a legal regulation which prohibits something without a penalty. Of course, it is possible than another kind of regulator would take over – powerful deterring social norms.

There are concerns that legal talk focused on brains could render the legal definition of a *person* obsolete. If we infer legal consequences from the state of the brain and detection of specific facts, what do we need this notion for? As Desmoulin-Canselier said, law sees a person as "the individual entitled to rights and bound by obligations, whose deeds are woven into legal life as if it were the lining of social life"[28] ,but if it is to start perceiving people as bundles of neurons, *personhood* becomes irreversibly lost. This was the concern of Feigenson, who described that attitude as "the fundamental psycho-legal error"[29]. This tendency would deepen even more in case of 'Religious Feelings Law 2.0', for which it would be more rational to infer directly from neurological and physiological data to legal norms. In the Law 2.0 paradigm, to say that a person offended other's religious feelings would be to say that in a given time, a brain worked in such a way that it produced consequences assessed as negative for some other brains. When *free will* and *responsibility* goes away, and all that is left of emotional distress are biological markers, we need not more than the brain. It is perhaps the scariest consequence of all. If brain one acted in such way that it negatively impacted brain two, what are we actually protecting by sanctioning this event?

As is evident, neuroscientific and technological advances integrated into Law 2.0 alter the inner workings and logic of law. There is a need, however, for a broader reflection: it is law that prescribes what is socially acceptable in a given culture; law on one hand *expresses* and on the other hand *shapes* the moral intuitions of its subjects. In line with legal realism, the transformations here described would have a profound impact on the society. So what would become of Law 2.0 in its broader societal setting?

In the era of neurolaw, there are angry voices that brain evidence helps murderers escape punishment[30]; however, when Law 2.0 is upon us, society may have different intuitions about the 'eye for an eye' rule. The new punishment does not warrant the name of

25 A. Oldenquist, 'An Explanation of Retribution' [1988] 9(85) Journal of Philosophy 464.
26 Greene, Cohen, ibidem, 1776.
27 Ibidem.
28 S. Desmoulin-Canselier, 'Another Perspective On "Neurolaw": The Use Of Brain Imaging In Civil Litigation Regarding Mental Competence' [2017] 3 BioLaw Journal (Rivista di BioDritto) 233, p. 244.
29 M. Moore, 'Stephen Morse on the Fundamental Psycho-Legal Error' [2016] 10(1) Criminal Law and Philosophy 45.
30 Miller, ibidem.

punishment; all that would remain is the protective function, so the penal process would become more of a containment procedure, determined by the danger that one poses to society rather than by the gravity of their offence. As of now, neurolegal cases meet with backlash based on society's 'thirst for blood' - the deeply ingrained desire for retributivism. Instead, there may appear a tendency for protection and more paternalism. In case of religious feelings, where passions run high quite literally, one could expect a serious amount of backlash over 'catharsis' lost due to lack of punishment. Some argue that retributive punishment has a restorative aspect: in the present case, the person whose religious feelings suffered could experience positive feelings and heal as a result of seeing the offender punished. Law 2.0 can choose to ignore that aspect or try to heal feelings in other ways, finding new methods of compensation and valuing the role of an apology.

Will adapting Law 2.0 lead to alienating the 'wrong' and placing it in a medical discourse as a disorder and malfunctioning human brain? Even today there are signs of ease with which people sign over the causes of unexplainable atrocities to a defunct organ. In the case of Grady Nelson, a murderer and rapist, two juries admitted that seeing his brain scans turned their decision from death penalty to life in prison[31]. They said that it convinced them that there was something wrong with this man's brain[32] - even though they didn't necessarily understand what their saw on the colourful brain scans, and a neurologist assessed the scans as riddled with mistakes[33]. But maybe such a reaction is one of the ways to deal with evil in others; neurolaw may bring about a new way of absolving the sins, not by punishment but by recognizing defects, isolation and rehabilitation. Perhaps criminals would be met with clinical pity rather than the rage they awaken today. It is surely less bloodthirsty, but no less unsettling version – there is much wiggle room between electric chairs and solitary cells on one hand, and sterile hospital-like containment on the other. However, in case of the offence of religious feelings, which appears benign and is often related to free speech and artistic expression rather than simple malice, there is little evil to speak of in this case. What is more concerning in this case is that the transformation could potentially mute the public discourse and value feelings over creativity.

Law 2.0 could also cause a cascade of other social changes, among which are the redefinition of the right to privacy, the notion of justice, and free will in connection to personal responsibility. Each of these topics is an extensive issue warranting a study on its own. Some tendencies, however, should be pointed out. First, searching for the offence of religious feelings in the brains poses a danger to privacy. As Kraft and Giordan noted, there is a clash between two concepts: that public institutions have no business investigating someone's inner life ("citizens should be 'generally free from governmental intrusions into one's privacy and control of one's thoughts'"[34]), and that neuroscience should be used to scrutinize, for example, memories, intent or emotions pertinent to law. This may be the true double-edged sword of the debate: surveillance of thoughts and mental processes could on one hand lead to apprehension of the guilty and let the innocent prove that they are, beyond doubt; but it could lead to abuse and misuse, perhaps even putting an end to individual liberty. This is inconceivable in most current societies. But maybe Society 2.0 would prefer

31 P. Shetty 'Law and Order: Blame It On the Brain' [2012] BBC Future, accessed at: http://www.bbc.com/future/story/20120710-blame-it-on-the-brain.
32 Ibidem.
33 G. Miller, 'Brain Exam May Have Swayed Jury in Sentencing Convicted Murderer' [2010] Science, accessed at: https://www.sciencemag.org/news/2010/12/brain-exam-may-have-swayed-jury-sentencing-convicted-murderer
34 C.J. Kraft, J. Giordano, 'Integrating Brain Science and Law: Neuroscientific Evidence and Legal Perspectives on Protecting Individual Liberties' [2017] 11 Frontiers in neuroscience 621, p. 622.

its safety over its right to privacy? Secondly, Law 2.0 could alter what one perceives as lawful, and the broader notion of justice itself. Is there such a thing as a scientific iteration of justice, that is being as close to the empirical truth as possible? If we were to adapt this connotation of justice in day to day life, our society would look very different. Would scientific justice, which is neither about fairness nor about equality but rather about the most perfect following of empirical description of the world, migrate to the collective consciousness? How would this new, scientific justice tie in with reflection about free will, and would we even care about justice, being convinced about the deterministic nature of the world? There is a chance that experiencing our lack of free will would make us hopeless and apathetic, rather than enlightened and compassionate – both as individuals and as a society. Would it not leave millions of people without meaning? Is that not too big a price to pay for having a perfectly science-based legal system?

Conclusion: Will Law 2.0 Be (Good) Law?

Only after analysing which methods could the new law employ and what would be its broader consequences, the new formulation of 'Religious Feelings Law 2.0' could be devised. This iteration of the regulation would replace the text cited at the beginning with specific, technical categories: article 196 of the Polish Penal Code would no longer speak about "punishing for the offence of religious feelings", but rather "predict the containment of someone whose actions provoked someone else's negative affective response in connection with religion". This shows how different conceptual foundations of neuroscience and law are and how hard it is to integrate them. Sooner or later, Law 2.0 would be faced with an uneasy task of balancing between the scientific and social world. Traditionally a product of the latter, it would now strive to express the former in an accurate way. Can it do that? Can it be true to science and still retain the name and character of law? What language it is to use? These questions would define the regulatory demands set before lawmakers: to reconcile the scientific and legal standards during the drafting of the regulation.

The core values of lawful democratic state demand all its laws to be formulated in such a way that every member of the public can understand them – this is in order to provide the citizens with a clear information on what is permitted, what is forbidden and which punishment will follow if one disregards the prohibition. However, if the new law was to be based on detection of specific neural states and visual patterns, redefine the notion of intent in a complicated way and replace traditional ways of punishment, then communicating it to the general public with a clear and concise manner seems quite a task for the lawmakers. In this case, Law 2.0's interpretation of religious emotions will decide between its old categories, expressed in language rooted in folk psychology, or highly specialized, technical language of physiological parameters, visual identification algorithms and containment. A question underlying this transformation is whether our feeling of what is "lawful" as a moral foundation would disappear altogether, pushed out by the scientific jargon.

This article aimed at stretching the limits of what is possible by initiating a series of thought experiments in law. In a world where there are flying cars, would law look like it used to for the most of modern history? Would our morality? Attempting to answer these questions allowed to reflect on the tangle between science, law and morality – one inspires and feeds the other, altering the reality we live in. Looking at a possible Law 2.0 and imagining the response of humans confronted with it may help us exercise our intuitions in preparation for the changes to come. In the end, it all comes down to Society 2.0 deciding

what kind of society it aims to be and which values it decides to protect. We can only hope that by the time the changes arrive, we will come to understand and remedy malfunctions not only of our brains, but also of our criminal system as well.

Bibliography

1. A. D'Amato, 'Can/Should Computers Replace Judges?' [1977] 11 Georgia Law Review 1277.
2. Artificial intelligence is coming for both judges and defendants' [2018] New York Post, https://nypost.com/2018/01/31/artificial-intelligence-is-coming-for-both-judges-and-defendants.
3. D. Bright, J.Goodman-Delahunty, 'Gruesome Evidence and Emotion: Anger, Blame, and Jury Decision-Making' [2006] 30 Law and human behavior 183.
4. P.G.H. Clarke, 'The Libet Experiment and its Implications for Conscious Will' [2013] Faraday Paper no. 17, https://www.bethinking.org/human-life/the-libet-experiment-and-its-implications-for-conscious-will
5. Z. Corbyn, 'Hungry Judges Dispense Rough Justice' [2011] Scientific American,: https://www.scientificamerican.com/article/hungry-judges-dispense-rough-justice.
6. S. Desmoulin-Canselier, 'Another Perspective On "Neurolaw": The Use Of Brain Imaging In Civil Litigation Regarding Mental Competence' [2017] 3 BioLaw Journal (Rivista di BioDritto) 233.
7. D. W. Denno, 'The Myth of the Double-Edged Sword: An Empirical Study of Neuroscience Evidence in Criminal Cases' [2015] 56 B.C.L. Rev. 493.
8. A. Dike, 'Would You Trust an Artificially Intelligent Expert?' [2017] National Law Review, https://www.natlawreview.com/article/would-you-trust-artificially-intelligent-expert.
9. 'Free Will and Neuroscience' https://wmpeople.wm.edu/asset/index/cvance/libet.
10. J. Greene, J. Cohen, 'For the Law, Neuroscience Changes Nothing and Everything' [2004], 359 Phil. Transactions Royal Soc'y London B 1775.
11. G. Jędrejek, T. Szymański, 'Prawna ochrona uczuć religijnych w Polsce. Próba oceny dotychczasowych rozwiązań, czyli o rozdźwięku pomiędzy literą prawa a jego aplikacją' [2002] Studia z Prawa Wyznaniowego vol. V, p. 183.
12. C.J. Kraft, J. Giordano, 'Integrating Brain Science and Law: Neuroscientific Evidence and Legal Perspectives on Protecting Individual Liberties' [2017] 11 Frontiers in neuroscience 621.
13. T. A. Maroney, 'Law and Emotions: The proposed taxonomy of an emerging field' [2006] 30 Law Hum Behav 119
14. G. Miller, 'Brain Exam May Have Swayed Jury in Sentencing Convicted Murderer' [2010] Science https://www.sciencemag.org/news/2010/12/brain-exam-may-have-swayed-jury-sentencing-convicted-murderer
15. G. Miller, 'Did Brain Scans Just Save a Convicted Murderer from the Death Penalty?' [2013] WIRED, http://www.wired.com/wiredscience/2013/12/murder-law-brain. G. Miller, 'The Brain Gets Its Day in Court' [2016] The Atlantic, accessed at: https://www.theatlantic.com/science/archive/2016/03/neurolaw-brain-scans-court/471615.

16. M. Moore, ’Stephen Morse on the Fundamental Psycho-Legal Error’ [2016] 10(1) Criminal Law and Philosophy 45
17. S.J. Morse, ‘Brain Overclaim Syndrome and Criminal Responsibility: A Diagnostic Note’ [2006] 117 Faculty Scholarship at Penn Law 397.
18. P. McNamara, ‘The Neuroscience of Religious Experience’ (New York: Cambridge University Press 2009)
19. A. Oldenquist, ‘An Explanation of Retribution’ [1988] 9(85) Journal of Philosophy 464.
20. M.S. Pardo, D. Patterson, ‘Minds, Brains, and Law’ (New York: Oxford University Press 2013)
21. S. Pinker, ‘The Cognitive Revolution’ [2011] Harvard Gazette https://news.harvard.edu/gazette/story/2011/10/the-cognitive-revolution.
22. I. Poggi, F. D'Errico, ‘Feeling Offended: A Blow to Our Image and Our Social Relationships’ [2018] 8 Frontiers in psychology 2221
23. P. Shetty ‘Law and Order: Blame It On the Brain’ [2012] BBC Future http://www.bbc.com/future/story/20120710-blame-it-on-the-brain.
24. E.H. Siegel et.al, ‘Emotion Fingerprints or Emotion Populations? A Meta-Analytic Investigation of Autonomic Features of Emotion Categories’ [2018] 4(144) Psychological Bulletin 343.
25. A. Taves, ‘Ascription, attribution, and cognition in the study of experiences deemed religious’ [2008] 38 Religion 125
26. The Republic of Poland, The Act of June 6, 1997 – Penal Code [1997] Journal of Laws of the Republic of Poland 1997 no. 88 item 53.
27. J. Wojciechowska,’Komentarz do artykułów 117–221’ (in:) A. Wąsek (ed.), ‘Kodeks karny. Cześć szczególna’ (Warszawa: CH Beck 2006).

CORPORATIONS OF THE FUTURE? PRESENTATION OF THE CONCEPT OF DECENTRALIZED AUTONOMOUS ORGANIZATIONS ON THE EXAMPLE OF THE DAO

Katarzyna Ziółkowska[1]

Abstract

Together with the emergence of Bitcoin and the underlying blockchain technology, many enthusiasts of the phenomenon started to put the idea of a company established on blockchain - digitalized, anonymous and genuinely democratic - in practice.

The DAO – the first and most well-known example of the decentralized autonomous organization – was a smart contract created on the Ethereum blockchain. It was concluded in a digital reality between Ethereum users, who have been purchasing tokens ("shares" in The DAO) in exchange for Ether units (cryptocurrency of the Ethereum). The tokens represented the rights of the participants of The DAO, especially the voting rights, because the funds collected by The DAO were to be invested, according to the participants' votes, in chosen hi-tech start-ups. During the initial offering of the DAO Tokens, which started in April 2016, the participants transferred to the platform Ethers worth approximately 150 million dollars.

Therefore, even tough The DAO did not have articles of association, management board, directors nor registered office, it was intended to enable its participants to collect funds, manage investments directly and cooperate in order to make profits. The rules of the undertaking were based entirely on the programming code, in line with the philosophy of "code as law" and the belief that technology may replace legal regulation and DAOs may replace traditional corporations.

Soon after the kick-off of The DAO, in June 2016, an anonymous hacker used a code gap and stole funds worth about 60 million dollars. It was immediately followed by the investigation of the United States Securities and Exchange Commission, which ruled that the offer of the DAO Tokens was subject to the federal rules on securities and in this case the law had been broken. Surprisingly, the fall of The DAO did not discredit entirely the idea of companies based on the blockchain and it opened up a broad discussion on the future of decentralized anonymous organizations and the clarification of the "code as law" approach.

This paper indicates the most important effects and controversy of the emergence and fall of The DAO project as well as problems with the qualification of this vehicle within the framework of known legal institutions. The paper tries to answer to the question whether decentralized anonymous organizations will replace traditional corporations in the future, and computer code – AoA and by-laws?

Keywords: DAO, blockchain, companies, tokens, code as law

[1] PhD student at the University of Warsaw, Faculty of Law and Administration. Member of the Research Centre on the Legal Aspects of Blockchain Technology. Professionally associated with the Polish National Centre for Research and Development. Email: k.ziolkowska@wpia.uw.edu.pl

Introduction

The idea of creating a decentralised autonomous organization based on the blockchain exists at least as long as the blockchain itself[2]. The creation of a technological solution which enables parties to carry out peer-to-peer transactions automatically and directly without an intermediary, very quickly triggered a discussion about the potential revolution in the way of running a business. It was noticed then that the blockchain allows not only making simple financial transactions, but also managing long-term and more complicated relations[3].

Having in mind the main feature of the blockchain that enables parties to conclude contracts and enforce its terms without the need of a central trusted entity, enthusiasts of the concept realised that it might also help improving corporate governance by automating underlying processes of managing a business venture. The main idea was to return power and decision making to the main interested participants of any corporation – owners, shareholders. Using the blockchain consensus mechanism, they would decide how the undertaking they invest in should look like, while relevant, digitalized documents concerning the investment would be available to them quickly, directly and safely. In such a case, administrative bodies of the company, such as a board of directors, may in fact turn out to be an unnecessary and expensive burden. DAO does not need a complicated, hierarchical system including levels of management, because its peer-to-peer structure enables getting rid of many ineffective elements from the process of managing a business venture.

As it was defined in the literature, decentralised autonomous organisation (DAO) means an organisation whose participants communicate with each other via the rule set of a computer network protocol, enabling them to achieve consensus or an agreement on rules and execute or implement the rules. This rule set means the decentralised organisation can be programmed to run autonomously without much of human involvement[4].

Decentralized autonomous organisation is not a type of a traditional company nor investment fund, other Bitcoin, another cryptocurrency or a website – it is a re-imagination of a company's structure and valid point in a discussion on possibilities to create a completely new and digital method of running a business.

---

[2] S. Nakamoto, 'Bitcoin: A peer-to-peer electronic cash system' [2008], https://bitcoin.org/en/bitcoin-paper, accessed: 15 April 2019. However, first to actually present the detailed description of a decentralized autonomous corporation was Vitalik Buterin, co-founder of Ethereum Foundation in 2013 (see V. Buterin, 'A next generation smart contract & decentralized application platform' Ethereum White Paper, http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf, accessed: 15 April 2019).

[3] Y. Hsieh, 'The Rise of Decentralized Autonomous Organizations: Coordination and Growth within Cryptocurrencies' [June 2018], https://ir.lib.uwo.ca/cgi/viewcontent.cgi?article=7386&context=etd, accessed: 15 April 2019, p. 101.

[4] G. Patrick, A. Bana, 'Rule of Law Versus Rule of Code: A Blockchain-Driven Legal World', [2017] IBA Legal Policy & Research Unit Legal Paper, p. 5.

1. The concept of "Code is law" and its implications for digitalized autonomous organisations

Term "code as law" or "code is law" refers to the concept of using means of computer code to influence (and in some way regulate) behaviour of software users. The term was coined by Lawrence Lessig, who introduced an idea of code (software and hardware) being a regulator for cyberspace[5].

Supporters of this theory argue that although the scope of 'regulation' created by means of a computer code is limited, it could be more effective within that scope. By limiting the functions and methods of use available to software users, it is possible to eliminate non-compliance problem in an extremely effective way. Software rules are, in a sense, self-executing, so there is no need for any additional bodies or instruments to guard their observance. On the other hand, it is impossible not to notice a series of limitations of this idea. Self-validity and automatism mean the lack of flexibility, choice and omission of a broader context when assessing compliance with the rules[6]. What is more, the short history of technological development shows that there is no ideal solution that does not have flaws or gaps.

Along with the creation and development of the blockchain technology, the 'code is law" theory found practical application in smart contracts. By definition, smart contract means an automatically enforceable code allowing parties to perform a credible transaction without a middleman. It does not require a separate legal document (like written agreement) and can be even used between anonymous parties. As contractual terms are written in the code and the code is the only carrier of legal intents of the parties, there can be no more legal obligations, rights or liabilities beyond what is written in the code.

As smart contracts are the underlying mechanism of decentralized autonomous organizations, above described rules are valid also for them. DAO, as it was defined by the United States Securities and Exchange Commission, is a "virtual" organization embodied in computer code and executed on a distributed ledger or the blockchai[n7]. Similarly, as in the case of smart contracts, software can replace the legal frameworks and provisions governing relations between participants of a DAO. Coordination is carried out by means of a permit system, consensus protocol and most of the functioning of an organisation is thus automated.

The participants of a DAO seek to reach a common economical goal by investing funds in a given venture. For determined amounts of cryptocurrency, they purchase tokens, which then serve to exercise certain rights in a DAO, like voting or sharing profits. Participants who have acquired tokens become "shareholders in the venture". Since the access to DAO's documents and voting process is easy, quick and does not require an intermediary, these "shareholders" themselves can make decisions regarding the organization's business activity or funds allocation. Therefore, administrative bodies are unnecessary in the structure of a DAO. Due to automation, full transparency as well as clear

[5] L. Lessig, ' Code and Other Laws of Cyberspace' (New York: Basic Books 1999).
[6] P. De Filippi, S. Hassan, 'Blockchain technology as a regulatory technology: From code is law to law is code' [2016] First Monday.
[7] Securities and Exchange Commission, 'Report on Investigation Pursuant to Section 21(a) of the Securities and Exchange Act of 1934: The DAO, [2017], https://www.sec.gov/litigation/investreport/34-81207.pdf, accessed: 15 April 2019, p. 1.

and self-enforcing rules of governance, shareholders themselves can manage and supervise the business. To do so, thanks to the application of the "code is law" approach in the concept of a DAO, they do not even need Articles of Association nor by-laws.

2. About The DAO

All the above mentioned advantages of a DAO over a regular incorporation has been noticed by founders of the first ever functioning decentralized autonomous organization called The DAO. In November 2015, Christoph Jenztsch, CTO of Slock.it (start-up developing a technology of blockchain-based sharing of assets), presented his first scheme of The DAO during Ethereum Developer Conference DEVCON1 in London. He described it as a for-profit DAO Entity, where participants would send units of Ether (virtual cryptocurrency of the Ethereum network) to The DAO in order to purchase DAO Tokens, which would permit the participants to vote and entitle them to "rewards"[8]. Since the organization was supposed to bring profits, funds from the sale of the DAO Tokens were to be invested in high-tech start-ups chosen by the participants who should vote on submitted proposals. In fact, Slock.it was to be the first start-up to submit proposal for funding from The DAO.

Main document containing conceptual and technical details about the initiative called the White Paper was published on 23rd March 2017[9]. In the opening, its author compared a traditional corporate form with The DAO code, stating however that the latter, by allowing automate organizational governance and decision-making, can more effectively mitigate the risk of non-compliance. Application of the "code is law" approach in The DAO was clearly articulated in the White Paper: "The terms of The DAO Creation are set forth in the smart contract code existing on the Ethereum blockchain (…). Nothing in this explanation of terms or in any other document or communication may modify or add any additional obligations or guarantees beyond those set forth in The DAO's code (…). The DAO's code controls and sets forth all terms of The DAO Creation."[10]

The proper kick-off of The DAO took place on 30th April 2016 when the sale of the DAO Tokens began. Gradually, by 28 May 2016 investors from all over the world transferred over 12 million units of Ether with a trading value in excess of 150 million dollars purchasing approximately 1.15 billion DAO Tokens in total. This made the offer of the DAO Tokens the largest crowdfunding project at that time[11].

3. Fall and investigation

[8] Rewards for participants of The DAO were comparable to dividends for shareholders of a traditional company. Christopher Jentzsch's speech about Slock.it and The DAO during DEVCON1 in London in November 2015 is available at: https://www.youtube.com/watch?v=49wHQoJxYPo, accessed: 15 April 2019.

[9] C. Jentzsch, 'Decentralized autonomous organization to automate governance' [2016], https://download.slock.it/public/DAO/WhitePaper.pdf, accessed: 15 April 2019.

[10] Christoph Jentzsch during his first presentation of the concept of The DAO compared The DAO's smart contract to its constitution.

[11] 'Blockchain, smart contracts and DAO', ed. Justyna Zandberg-Malec, Wardyński i Wspólnicy [2016], https://www.wardynski.com.pl/w_publication/blockchain-inteligentne-kontrakty-i-dao/, accessed: 15 April 2019 (in Polish).

On 17 June 2017, just after the initial offering of the DAO Tokens was over, but before The DAO started investing collected funds, the Ethereum Foundation announced that The DAO had been attacked. Anonymous hacker used a flaw in The DAO's code to derive nearly 3.6 milion Ethers – 1/3 of the total sum - collected in The DAO to so-called childDAOs. Since they were simply new smart contracts on the same Ethereum blockchain, general rules of that blockchain were applicable also for all the childDAOs. Therefore, the hacker could not withdraw stolen funds from the new organizations immediately and had to wait until the end of the creation periods for the childDAOs. For this reason, the Ethereum community had some time to analyse the situation.

Surprisingly the most important issue raised in that discussion was not 'can something be done?' but rather 'should something be done?'. Bearing in mind the basic characteristics of the blockchain and smart contracts, that they are autonomous, immutable and are not subject to institutional control, the question arose as to whether the hacker's doing can be considered as unlawful. Part of the community argued that any attempt to restore the situation to the state from before the incident could create a dangerous precedence and seriously undermine the credibility of the Ethereum network and even the blockchain itself. Even those participants however, just like the vast majority of the Ethereum community, deemed it fair that the investors should get their money back. Others, and among them the hacker himself[12], stated that the creation of the childDAOs was possible because of certain features of the code, the code enabled withdrawing of the funds from The DAO and so that the incident can not be regarded as theft.

The discussion on The DAO and Ethereum forums, however, indicated that most of the Ethereum blockchain users expected to counteract the effects of the attack by conducting so called hard fork on the Ethereum blockchain. On 20 July 2016 the majority of the community decided to modify the transaction history and retrieve stolen funds. They were transferred to another smart contract that had just one function – for every 100 DAO Tokens it should reimburse 1 Ether. Since the hacker could not deduce funds from the childDAOs right away, all the funds were easy traceable and retrievable and the hard fork proved itself effective[13].

But the history of The DAO did not end there. Soon after its fall, the United States Securities and Exchange Commission has opened up an investigation[14]. Besides establishing relevant facts and circumstances of the case, the SEC aimed at determining

[12] Interestingly, on 18 June 2016 the hacker (who called himself "The Attacker") issued an open letter to the Ethereum Community in which he expressed his concern about plans to conduct hard fork on the Ethereum blockchain. He claimed that the feature of the code that allowed him to withdraw funds to childDAOs was there on purpose, "to promote decentralization and encourage the creation of "child DAOs". In that letter he wrote also that „a soft or hard fork would amount to seizure of my legitimate and rightful ether, claimed legally through the terms of a smart contract (…). I reserve all rights to take any and all legal action against any accomplices of illegitimate theft, freezing, or seizure of my legitimate ether, and am actively working with my law firm." Letter is available online at: https://pastebin.com/CcGUBgDG, accessed: 15 April 2019.

[13] Some Ethereum users did not agree to the hard fork, because in their opinion this had been undermining the whole idea of cryptocurrencies and immutable of the blockchain. These users decided to support the old blockchain reflecting the transaction history with the theft that occurred. In this way a new cryptocurrency - Ethereum Classic - was created.

[14] Even though the founders were Germans and The DAO as a virtual and unincorporated organisation did not have a registered seat, the American SEC considered itself to be competent to investigate on The DAO because the DAO Token had been offered and sold in the United States. Securities and Exchange Commission, 'Report…', p. 2.

whether federal securities laws should have been applicable to The DAO. In the Report of July 25, 2017 it stated that the DAO Tokens were securities so they should had been registered with the Commission or qualified for an exemption, and so should other instruments offered by "virtual organizations or capital raising entities that use distributed ledger or blockchain technology to facilitate capital raising and/or investment and the related offer and sale of securities".[15]

The report showed that the Commission had brought The DAO to the form of a contact or interface mechanism between participants involved in this venture. By not deciding whether The DAO was an investment company or not, the SEC did not respond also whether The DAO had been a company at all. There was no constructive comment from the SEC on the lack of corporate documents, board of directors and other managing bodies. By stating that "the automation of certain functions through this technology, "smart contracts" or computer code, does not remove conduct from the purview of the U.S. federal securities laws", the SEC ruled that it does not recognise decentralized autonomous organizations as a new form of companies, but merely technological facilitation for business undertakings.

4. Lessons learned[16]

In spite of the unsuccessful end of The DAO, there are always more and more new decentralized autonomous organisations starting or further developing their business operation[17]. Now, after almost three years from the fall of The DAO, we cannot say, however, that those existing DAOs are revolutionising or even changing dramatically the way of running a business. Lack of official recognition of The DAO as a completely new and disrupting form of a company by the SEC, any other institution or legal and social system in general is not however the only reason why decentralized autonomous organisation will not replace soon traditional corporations. In my opinion, complete replacement of the present corporate governance by self-enforcing computer code will not be successful on a larger scale until codes are not fully reliable. As long as we do not have full confidence that the technology is robust, transparent and understandable to make sure that the code reflects the intent of its user with certainty, human arbitrators, documents and laws will be necessary. And as it turns out, we can never be 100% sure.

The end of The DAO story showed practical consequences of implementing the "code is law" rule in a real world. Interestingly, all the participants and observers could possibly agree on the statement that the code of The DAO just did not work. But the actual question that raises here is: what do we mean by that? Did the code not work because there was a flaw in the smart contract? Or maybe it did not work because the Ethereum community prevent its programmed functioning? What happened after the attack on The DAO was the decision to reverse the consequences of the hacker's actions (which were taken in accordance with the code) so to recover the funds. The Ethereum community did that simply because it was a right thing to do - fair (morally) and lawful (legally). The basics of that

[15] Securities and Exchange Commission, 'Report…', p. 2; at the same time, the SEC did not deal with the question whether The DAO was an investment company arguing that it never started its proper business operation - investing in projects.

[16] The title of this last chapter containing conclusions was inspired by the blog entry of Christoph Jentztsch titled 'The History of the DAO and Lessons Learned' published on 24 August 2016 on blog.slock.it soon after the fall of The DAO, https://blog.slock.it/the-history-of-the-dao-and-lessons-learned-d06740f8cfa5, accessed: 15 April 2019.

[17] Like, for example, MakerDAO, DigixDAO, DAOStack.

decision lied not in the code, assumptions of the blockchain technology or IT sciences, but in the basic moral and legal principles of democratic societies.

This short, but eventful history of The DAO teaches us that the code is not and will not replace law. Paraphrasing words of Patrick Murck, researcher on legal aspects of the blockchain, we can say that maybe code is law for machines, but law should remain code for people[18].

Bibliography

1. 'Blockchain, smart contracts and DAO', ed. Justyna Zandberg-Malec, Wardyński i Wspólnicy [2016], https://www.wardynski.com.pl/w_publication/blockchain-inteligentne-kontrakty-i-dao/, accessed: 15 April 2019 (in Polish).
2. C. Jentzsch, 'Decentralized autonomous organization to automate governance' [2016], https://download.slock.it/public/DAO/WhitePaper.pdf, accessed: 15 April 2019.
3. C. Jentztsh, 'The History of the DAO and Lessons Learned', https://blog.slock.it/the-history-of-the-dao-and-lessons-learned-d06740f8cfa5, accessed: 15 April 2019.
4. G. Patrick, A. Bana, 'Rule of Law Versus Rule of Code: A Blockchain-Driven Legal World', [2017] IBA Legal Policy & Research Unit Legal Paper.
5. L. Lessig, ' Code and Other Laws of Cyberspace' (New York: Basic Books, 1999)
6. P. De Filippi, S. Hassan, 'Blockchain technology as a regulatory technology: From code is law to law is code' [2016] First Monday.
7. P. Murck, 'Who Controls the Blockchain?' [2017] Harvard Business Review, https://hbr.org/2017/04/who-controls-the-blockchain, accessed: 15 April 2019.
8. S. Nakamoto, 'Bitcoin: A peer-to-peer electronic cash system' [2008], https://bitcoin.org/en/bitcoin-paper, accessed: 15 April 2019.
9. Securities and Exchange Commission, 'Report on Investigation Pursuant to Section 21(a) of the Securities and Exchange Act of 1934: The DAO, [2017], https://www.sec.gov/litigation/investreport/34-81207.pdf, accessed: 15 April 2019.
10. The Attacker, 'Open letter', https://pastebin.com/CcGUBgDG, accessed: 15 April 2019.
11. V. Buterin, 'A next generation smart contract & decentralized application platform' Ethereum White Paper, http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf, accessed: 15 April 2019.
12. Y. Hsieh, 'The Rise of Decentralized Autonomous Organizations: Coordination and Growth within Cryptocurrencies' [June 2018], https://ir.lib.uwo.ca/cgi/viewcontent.cgi?article=7386&context=etd, accessed: 15 April 2019

[18] P. Murck, 'Who Controls the Blockchain?' [2017] Harvard Business Review, https://hbr.org/2017/04/who-controls-the-blockchain, accessed: 15 April 2019.

THE IMPORTANCE OF PERSON'S WILL TO PARTICIPATE IN BIOMEDICAL RESEARCH

Milda Žaliauskaitė[1258]

Abstract

The increased welfare of humans over the time can be significantly attributed to medical advances and innovations resulting from medical research. Improved treatments, innovative techniques and more effective drugs prove the importance of efficient and qualitative medical research. One of the research elements involves studies of people who may be subjects in clinical trials. This article explores legal aspects of person's intentions and will to participate in biomedical research, i. e. to enter into a legally binding agreement. What states an intention to be legally enough to obligate and how to determine person's true will? What should be the required level of person's competency to hold the intention valid? This paper seeks to answer such questions in order to contribute to protection of people from improper or illegal participation in biomedical research.

Key words: True will, Intentions to obligate, Participation in biomedical research, Human rights protection.

Introduction

It is generally believed that every person possesses freedom of will and as a free being is able to exercise his moral authority in deciding, acting and taking responsibility for his life[1259]. The scope and legality of person's will to undertake any obligations is crucial in various legal scenarios, including participation in biomedical research.

People's will to participate in different research settings is extremely important in a sense that their implication may improve overall relevance and quality of the research itself. Actually, study shows that people's engagement into research even in advisory groups (consisted of patients, family, carers, etc.) settings, may influence the research to be more deep, responsive and reflective to the needs and experiences of the patients with particular diseases[1260]. Moreover, patient's involvement, including range of patient's views incorporation into research, is considered as a central tenet of biomedical research, not only

[1258] Master's degree in law and master's degree in business and management, Vytautas Magnus university. Currently, PhD candidate in Law, Vytautas Magnus university, Faculty of Law, writing dissertation on "The concept of advance will in private law: balancing between public and private interests". Research interests include private law, particularly contract law. E-mail: milda.zaliauskaite@vdu.lt.

[1259] L. Johnsson, S. Eriksson, 'Autonomy Is a Right, Not a Feat: How Theoretical Misconceptions Have Muddled the Debate on Dynamic Consent to Biobank Research' [2016] Bioethics 30/7.

[1260] S. J. Hill et al., 'Consumer Engagement Critical to Success in an Australian Research Project: Reflections from Those Involved' [2018] Australian Journal of Primary Health 24/3.

shaping the research agendas, but also required for funding programmes[1261]. Given the significance of both human subjects' participation and protection of human rights in biomedical research, proper procedures must ensure ethically and legally justifiable involvement of the research participants.

Despite the importance aligned to person's consent to participate in biomedical research, less attention has been paid to the role of person's will to participate. Questions of whether patient expresses his true, authentic will, without undue influence or coercion and whether that volition is not influenced by the disease, depression or desperate position are not widely debated throughout scientific literature. The focus is given to the legal requirements of obtaining consent while the assessment of whether that consent represents conscious intention and definite willingness to participate is disregarded.

In the view of the above, this paper analyses fundamental international documents related to the research topic so as to determine what states an intention and acceptance of the person to participate in biomedical research, also explores scientific publications in furtherance of identifying the importance various researchers impose to person's will to participate and challenges that follows herewith.

1. International Legal Frameworks for Consent

Nowadays there are variety of international documents that are relevant to diverse questions of biomedical research on people. Yet, the subject of person's consent to participate in the research initiated since Second World War, when experimental research was conducted on war prisoners without obtaining their consent[1262]. This led to manifold initiatives to establish basic ethical and legal principles and guidelines with regards to patient's autonomy, self-determination and protection of other rights. Consequently, in length of time a number of international documents concerning research with human subjects were adopted and that affirms the fact that issues such as person's consent to participate in biomedical research are global in nature and cannot be confined to and solved within individual states boundaries. For this reason, it is particularly valuable to pursue specific review of most pivotal international documents in the interest of consent and volition of human participation in medical research.

To begin with, the Universal Declaration of Human Rights is the most significant international document on human rights and fundamental freedoms. This Universal Declaration has a profound influence on human rights protection, ergo it lays the common grounds and standards to follow for all the actions involving humans, including biomedical research on humans. Accordingly, Article 5 prohibits cruel, inhuman or degrading treatment, whereas Article 19 entitle everyone to freedom of opinion and expression[1263]. In the light of biomedical research, these terms protect person's right to autonomously decide and express his will lest to participate in the research unwillingly that could cause unwished negative or even harsh experiences and emotions. Universal Declaration of Human Rights serves as an umbrella measure for recognition and observance of person's position in society granting valid and solid consideration of person's will.

[1261] G. Russell et al., 'Selective Patient and Public Involvement: The Promise and Perils of Pharmaceutical Intervention for Autism' [2018] Health Expectations 21/2.
[1262] G. Sridharan, 'Informed Consent in Clinical Dentistry and Biomedical Research' [2013] Journal of Education and Ethics in Dentistry 2/2.
[1263] The United Nations General Assembly resolution 217 (III) A 'Universal Declaration of Human Rights' [1984].

On the basis of Universal Declaration of Human Rights, General Conference of UNESCO adopted Universal Declaration on Bioethics and Human Rights. With the intention to promote respect for human dignity and to protect human rights in biomedical research, this document prioritize person's interests and welfare over the interests of science and society. Foremost, it promotes respect for person's right to make decisions herewith taking responsibility for those decisions[1264]. In addition to this, professionalism, honesty, integrity, transparency and adequate sharing of knowledge should follow all the decision-making process and autonomous person's will must be validated by prior, free and informed consent[1265]. This standard view recurs throughout other international documents making person's consent as a foundation to hold that person respectively expressed his will to be involved in biomedical research.

Declaration of Helsinki adopted by World Medical Association is held as one of the cornerstone documents guiding ethical questions of research on human. This document is not legally binding, yet its fundamental principles are recognized as standards of human protection. The pivotal attention is given to respect for individual as declaration states that generating new knowledge should "never take precedence over the rights and interests of individual research subjects"[1266]. This document is particularly important for the protection of patient's interests, including his readiness to participate in the research. It declares that not only the consent of the patient must be given freely, but also it is necessary that the patient's intention to participate in the research should be voluntary and properly informed[1267]. Duty to inform the patient adequately demonstrates the prime need to form a subjective state of mind on the procedure in order to express considered will. It is also worth to mention that Declaration of Helsinki supports patient's change of heart, i. e. patient's wish to abstain from participation at any time without any reprisal[1268]. This proves that one should have sufficient notion of will to participate all along the research and this will should be attentively determined and continually verified throughout the research. With regards to what states an expressed will to participate, declaration suggests that consent (i) by the patient or his legally authorized representative may preferably be received (ii) in writing, and if not, consent must be formally documented and witnessed, also, (iii) physician must ensure to have no dependent relationship with the patient and (iv) to refuse consent made under duress[1269]. Although these four aspects indicate fair attempts to receive formal and valid approval of the individual, yet, little attention is paid to making sure that the approval is based on a true and deliberate will.

Another document adopted by World Medical Association relevant to human subjects' inclusion into biomedical research is International Code of Medical Ethics. Although this document does not explicitly discuss biomedical research, it does provide general principles applicable to such cases. Most importantly, it recognizes physician's duty to respect and follow patient's position, i. e.: (i) to respect patient's right to accept or refuse treatment; (ii) to respect the rights and preferences of patients; and (iii) to act in the patient's best interest when providing medical care[1270]. As a matter of fact, these three duties seemingly indicate the substantial weight of patient's will assigned to his involvement in biomedical research.

[1264] UNESCO SHS/EST/BIO/06/1, SHS.2006/WS/14 'Universal Declaration on Bioethics and Human Rights' [2006].
[1265] UNESCO, Ibid.
[1266] World Medical Association 'Declaration of Helsinki. Ethical principles for medical research involving human subject' [2001] Bulletin of the World Health Organization 79(4).
[1267] World Medical Association, Ibid.
[1268] World Medical Association, Ibid.
[1269] World Medical Association, Ibid.
[1270] World Medical Association, 'International Code of Medical Ethics' [2006].

On the other hand, similarly to Declaration of Helsinki, International Code of Medical Ethics does not expressly set a duty to assess certainty and reliability of will, this document just merely stipulates to respect it.

International Ethical Guidelines for Biomedical Research Involving Human Subjects prepared by the Council for International Organizations of Medical Sciences (CIOMS) in collaboration with the World Health Organization (WHO)[1271] is quite a comprehensive document providing general ethical principles with detailed explanations and comments on how to interpret it. This document is based on three main principles – beneficence, justice and, most importantly, respect for autonomy that serves as a protection of person's right for self-determination and personal choices[1272]. With this in mind, CIOMS Guidelines portray sound and reasonable approach to determine and evaluate person's will to participate in biomedical research. Guideline 4, which is aimed at informed consent, basically sets forth fundamental duties that contribute to person's will ascertainment. Firstly, the process of getting voluntary informed consent must begin at initial contact "[b]y informing the prospective subjects, by repetition and explanation, by answering their questions as they arise, and by ensuring that each individual understands each procedure"[1273]. Secondly, investigator must provide the information in a language suitable for individual's maturity, intelligence, education and belief system; and lastly, he must ensure that individual has adequately understood that information[1274]. In a like manner to previously mentioned documents, questions of renewing consent, documentation of consent, essential information requirements, withdrawing the consent are stressed out, too. Nonetheless, CIOMS Guidelines emphasize the demand to protect patient's personal decision from intimidation and undue influence. The duty to refrain from unjustified deception, undue influence, or intimidation is explained as avoiding those situations, where physician has certain credibility in patient's eyes or considerable influence that may cause fear for further low-quality or even suspended treatment in case of patient's refusal to participate[1275]. Furthermore, before seeking the consent sponsors and investigators must be sure that person "has adequate understanding of the relevant facts and of the consequences of participation and has had sufficient opportunity to consider whether to participate"[1276]. In 2016, new version of CIOMS Guidelines were published that addresses additional topics, such as involving vulnerable groups in research, low-resource settings, etc. With regards to person's will to participate in biomedical research, requirements correspond with a previous version, highlighting the importance of securing patient from unjustified deception, withholding of relevant information, undue influence or even coercion[1277].

To summarize, various international documents identify the significance of person's right to decide whether to participate in biomedical research. What connects those all documents is an attempt to ensure prior, informed and free consent of the patient. However, international documents distinguish vulnerable patient groups for which additional attention should be given to, especially in cases where patient is not able to give consent himself thus legal guardian has to take over this right. These situations seem to get rather little attention

[1271] Hereafter referred to as CIOMS Guidelines.
[1272] The Council for International Organizations of Medical Sciences, 'International Ethical Guidelines for Biomedical Research Involving Human Subjects' [2002].
[1273] The Council for International Organizations of Medical Sciences, Ibid.
[1274] The Council for International Organizations of Medical Sciences, Ibid.
[1275] The Council for International Organizations of Medical Sciences, Ibid.
[1276] The Council for International Organizations of Medical Sciences, Ibid.
[1277] The Council for International Organizations of Medical Sciences, 'International Ethical Guidelines for Biomedical Research Involving Human Subjects' [2016] Revised version.

with regards to questions of what shall prevail – patient's best interests or patient's will, and whether it is ethically justifiable enough to carry out research with a lack of patient's will.

2. The Challenges of Consent and Will

Even with internationally recognized ethical and legal principles in place, certain challenges still are faced in practice. In terms of person's consent to participate in biomedical research, there are still on-going debates on whether the procedures of obtaining consent are effective and just. In order to illustrate this, some of the most striking and relevant challenges related to the person's consent to participate in biomedical research are presented in this chapter.

Initially, one of the main apprehensions of human consent procedure is whether consent *per se* ensures expression of patient's true will. Scientists suggest that true volition embodies a complex interplay of beliefs[1278] and conscious experiences in voluntary action[1279], active decision-making, resolvement of uncertainty and commitment on a certain course of action[1280]. Nonetheless, in revised literature there are no traces of actual consideration of these aspects. Despite the acknowledgment of the importance of patient's consent, the lack of clear and common assessment methods and standards of actual volition poses a risk of undue influence, coercion and manipulation to person's decision.

As is evident from the previous chapter, person's consent to participate is recognized as an obligatory requirement for implementation of biomedical research. To ensure that patients were not deceived nor coerced to participate in the research is considered as the main purpose of obtaining consent[1281]. Nevertheless, it may be argued that this duty embodies only formal fulfillment of legal obligations. In fact, some scientists make an observation that investigators view these requirements purely as something "they are required to do in order to fulfill funding guidelines", as "tick-box" exercise[1282], "an instrument of fulfilling the legal obligations of respecting patients' right"[1283], "merely presenting a contract to be signed"[1284], etc. For this reason, it seems that the procedures protect physicians rather than the patients' rights[1285]. That being the case, researchers do not consider person's will and intentions as significant factors in practice. Conversely, researchers neither are given duty to ascertain person's true will nor they are interested to do this. A twofold quandary hence arises from this perspective: on the one hand, researcher is invested in his own research, ergo he may avoid delving deeply into potential participant's will so as not to frighten and lose him; on the other hand, researcher is not well equipped by tools and methods to evaluate whether the person expresses his true, uncompromising will. Indeed, international documents provide an obligation to get voluntary consent, yet ways to ensure or verify that consent are not specified[1286]. Although modern society promotes

[1278] K. Nair et al., 'Patients' Consent Preferences Regarding the Use of Their Health Information for Research Purposes: A Qualitative Study' [2004] Journal of Health Services Research and Policy 9/1.
[1279] P. Haggard, 'Human Volition: Towards a Neuroscience of Will' [2008] Nature Reviews Neuroscience 9/12 (2008).
[1280] J. Zhu, 'Intention and Volition' [2004] Canadian Journal of Philosophy 34/2.
[1281] L. Johnsson, S. Eriksson, Ibid.
[1282] G. Russell et al., Ibid.
[1283] A. Frunza, A. Sandu, 'Ethical Acceptability of Using Generic Consent for Secondary Use of Data and Biological Samples in Medical Research' [2017] Acta Bioethica 23/2.
[1284] L. Johnsson, S. Eriksson, Ibid.
[1285] J. A. Sacristán, 'Clinical Research and Medical Care: Towards Effective and Complete Integration' [2015] BMC Medical Research Methodology 15/1.
[1286] K. Gillies et al., 'Patient Reported Measures of Informed Consent for Clinical Trials: A Systematic Review' [2018] PLoS ONE 13/6.

informed dialogue and patients right to autonomy and self-governance, having no actual guidelines and standards to determine validity of person' will shows a considerable limitation on existing international legal framework.

The other difficulty arises with the effectiveness of consent forms. First of all, criticism is expressed for the generic consent forms that are also used for therapeutic interventions for fear that this type of form fails to ensure the real quality of consent for the research[1287]. It is argued that consent might be too uncertain in generic forms, also therapist might have broad potentiality to manipulate patient's decision, research might be implicitly authorized without specific consent for it[1288], forms are overly long and complex[1289], etc. In addition to this, the attention is given to the difficult readability of consent due to heavy language and specific terms, hence scientists note that decision to proceed cannot be held autonomous and informed without understanding the risks and benefits[1290]. This criticism proves that general consent forms are outdated, ineffective and poorly ensures patients' autonomy to decide. Therefore, there are new consent formats offered, such as wide (broad) or narrow consent, meta-consent, opt-out or opt-in consent, etc. By way of example, some scientists suggest personalized consent flow, based on a similar principle of privacy settings on Facebook, where patients may opt for "narrow" or "broad" consent, which is personalized, transparent and very simple[1291]. And in the era of new technologies, where artificial intelligence and machine learning are developing rapidly, there should be more effective tools, firstly, for presenting information for the patient in an individualized, simple and understandable manner and, secondly, for obtaining specific consent by convenient means. For instance, such tools as videos, information graphics and appealing examples may be used in order to ensure effective patient understanding[1292]. Scientists note that even if the process of gaining an informed consent may be legally correct, whether the decision was truly informed may be measured only by asking patients for their perspectives[1293]. Accordingly, social media technologies have a strong potential to establish immediate and reciprocal relation between researcher and participant, thus ensuring participants to have more control and information about the research project.

Obtaining consent from vulnerable patients' groups, such as mentally ill patients, minors, patients who need intensive care, is another question of debate. In some circumstances it is allowed to proceed the research without a consent or with a proxy consent when patients do not have the capacity to provide consent by themselves. Therefore, these situations basically contradict patient's right to autonomy: patient not being able to express his will is followed by other people deciding for the patient what his best interests may be. Moreover, it raises a question of how to justify that patient's best interests are participating in the research, when in fact research is oriented not towards the good of the patient but for common goods of knowledge development. Not to mention that such cases deny the standard belief that "you should not treat someone who does not want to be

[1287] A. Frunza, A. Sandu, Ibid.
[1288] A. Frunza, A. Sandu, Ibid.
[1289] O'M. Spence et al., 'Patient Consent to Publication and Data Sharing in Industry and NIH-Funded Clinical Trials' [2018] Trials 19/1 (2018).
[1290] H. E. Taylor, D. E. P. Bramley, 'An Analysis of the Readability of Patient Information and Consent Forms Used in Research Studies in Anaesthesia in Australia and New Zealand' [2012] Anaesthesia and Intensive Care 40/6.
[1291] E. A. Rake et al., 'Personalized Consent Flow in Contemporary Data Sharing for Medical Research: A Viewpoint' [2017] BioMed Research International 2017.
[1292] E. A. Rake et al., Ibid.
[1293] K. Gillies et al., Ibid.

treated", they also lead to concerns about enforced treatment[1294]. Nevertheless, the justifiable solution to carry out the research without patient's instantaneous consent may be respecting his previously expressed wishes (e.g. following his preferences stated in advance directive or living will). It is worth to mention that different approach is suggested for child-participants as minor willingness to participate plays the paramount role in the decision making, where the consent process should be designed to determine and promote his will and to prevent it from duress or distress[1295]. Again, no standards nor methods are introduced to assure this approach are followed.

In conclusion, it is obvious that to assess person's true will may be a difficult task, mostly because it includes subjective psychological aspects. That leaves room for person's consent to be compromised by unfavorable influence or even coercion. The process of obtaining consent also causes debate on its effectiveness what shows that certain issues still remain unanswered. Therefore, taking into account significance of the person's will, solutions at the international level should be proposed.

Conclusions

Person's voluntary and informed consent to participate in biomedical research is acknowledged at the international level. Various international documents underline the importance of the protection of human rights, recognizing rights of personal autonomy and self-determination. Nevertheless, there are still some issues remaining, such as usage of non-effective generic consent forms, researchers' attitude towards consent obtaining process, research implementation without patient's consent, etc. Still, in the era of new technologies and rapid development of innovations, new tools should be explored and launched to ensure more effective approach towards legal human subjects' involvement into biomedical research procedures. Particularly, more attention should be given to developing standards and methods to assess and ascertain actual person's will in order to minimize potential risks of coercion, undue influence or even illegal participation.

Bibliography

1. Frunza, A., Sandu, A. 'Ethical Acceptability of Using Generic Consent for Secondary Use of Data and Biological Samples in Medical Research' [2017] Acta Bioethica 23/2.
2. Gill, D., et al., 'Guidelines for Informed Consent in Biomedical Research Involving Paediatric Populations as Research Participants' [2003] European Journal of Pediatrics 162/7–8.
3. Gillies, K., et al., 'Patient Reported Measures of Informed Consent for Clinical Trials: A Systematic Review' [2018] PLoS ONE 13/6.
4. Haggard, P., 'Human Volition: Towards a Neuroscience of Will' [2008] Nature Reviews Neuroscience 9/12 (2008).

[1294] G. Russell et al., Ibid.
[1295] D. Gill et al., 'Guidelines for Informed Consent in Biomedical Research Involving Paediatric Populations as Research Participants' [2003] European Journal of Pediatrics 162/7–8.

5. Hill, S. J., et al., 'Consumer Engagement Critical to Success in an Australian Research Project: Reflections from Those Involved' [2018] Australian Journal of Primary Health 24/3.
6. Johnsson, L., Eriksson, S. 'Autonomy Is a Right, Not a Feat: How Theoretical Misconceptions Have Muddled the Debate on Dynamic Consent to Biobank Research' [2016] Bioethics 30/7.
7. Nair, K., et al., 'Patients' Consent Preferences Regarding the Use of Their Health Information for Research Purposes: A Qualitative Study' [2004] Journal of Health Services Research and Policy 9/1.
8. Rake, E. A., et al., 'Personalized Consent Flow in Contemporary Data Sharing for Medical Research: A Viewpoint' [2017] BioMed Research International 2017.
9. Russell, G., et al., 'Selective Patient and Public Involvement: The Promise and Perils of Pharmaceutical Intervention for Autism' [2018] Health Expectations 21/2.
10. Sacristán, J. A., 'Clinical Research and Medical Care: Towards Effective and Complete Integration' [2015] BMC Medical Research Methodology 15/1.
11. Spence, O'M., et al., 'Patient Consent to Publication and Data Sharing in Industry and NIH-Funded Clinical Trials' [2018] Trials 19/1 (2018).
12. Sridharan, G. 'Informed Consent in Clinical Dentistry and Biomedical Research' [2013] Journal of Education and Ethics in Dentistry 2/2.
13. Taylor, H. E., Bramley, D. E. P., 'An Analysis of the Readability of Patient Information and Consent Forms Used in Research Studies in Anaesthesia in Australia and New Zealand' [2012] Anaesthesia and Intensive Care 40/6.
14. The Council for International Organizations of Medical Sciences, 'International Ethical Guidelines for Biomedical Research Involving Human Subjects' [2002].
15. The Council for International Organizations of Medical Sciences, 'International Ethical Guidelines for Biomedical Research Involving Human Subjects' [2016] Revised version.
16. The United Nations General Assembly resolution 217 (III) A 'Universal Declaration of Human Rights' [1984].
17. UNESCO SHS/EST/BIO/06/1, SHS.2006/WS/14 'Universal Declaration on Bioethics and Human Rights' [2006].
18. World Medical Association 'Declaration of Helsinki. Ethical principles for medical research involving human subject' [2001] Bulletin of the World Health Organization 79(4).
19. World Medical Association, 'International Code of Medical Ethics' [2006].
20. Zhu, J., 'Intention and Volition' [2004] Canadian Journal of Philosophy 34/2.

Vilnius University Press
Saulėtekio al. 9, LT-10222 Vilnius
info@leidykla.vu.lt
www.leidykla.vu.lt