MASARYK UNIVERSITY JOURNAL OF LAW AND TECHNOLOGY

VOLUME 12 | NUMBER 2 | FALL 2018 | ISSN 1802-5943

PEER REVIEWED

CONTENTS:

www.mujlt.law.muni.cz

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

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

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

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

MASARYK UNIVERSITY JOURNAL OF
LAW AND TECHNOLOGY

VOLUME **12** | NUMBER **2** | FALL **2018**

LIST OF ARTICLES

DOI 10.5817/MUJLT2018-2-1

THE AFRICAN UNION CONVENTION ON CYBERSECURITY: A REGIONAL RESPONSE TOWARDS CYBER STABILITY?

by

UCHENNA JEROME ORJI*

Following the liberalization of telecommunication markets in African States, and the increasing availability of wireless technologies and broadband capacity, the levels of Internet penetration and ICT access in Africa has continued to grow in a phenomenal manner since the beginning of the new millennium. Internet use statistics indicate that Africa's Internet user population grew from about four and a half million people in 2000 to about 400 million people in December, 2017. However, widespread ICT access and Internet penetration in Africa has also raised concerns over the need to promote cybersecurity governance and cyber stability across the continent. This prompted the African Union to establish a regional cybersecurity treaty, known as the African Union Convention on Cyber Security and Personal Data Protection, in June, 2014. The Convention imposes obligations on Member States to establish legal, policy and regulatory measures to promote cybersecurity governance and control cybercrime. This article analyzes the nature and scope of the cybersecurity governance obligations under the Convention and examines how the adoption of the Convention can promote cyber stability in the African region. In so doing, the paper also examines the challenges impeding the application of the Convention as a framework for promoting regional cyber stability in Africa. The paper identifies the slow pace of Member State ratification and the absence of effective regional coordination as some of the major reasons why the Convention has not been effectively applied as a framework for promoting regional cyber stability. Therefore, the paper makes a case for the establishment of a regional monitoring mechanism within the AU framework to improve

* jeromuch@yahoo.com, LL.B (Hons.) (University of Nigeria); LL.M (University of Ibadan); PhD (Nnamdi Azikiwe University Nigeria) Barrister and Solicitor of the Supreme Court of Nigeria.

the regional harmonization of cybersecurity governance frameworks, and harness the application of the Convention as a framework for promoting regional cyber stability.

KEY WORDS

African Union, Cyber Stability, Regional Cybersecurity Obligations

1. INTRODUCTION

Since the beginning of the 21st century, the African continent has continued to witness a tremendous growth in ICT and Internet penetration. Recent Internet use statistics indicate that Africa's Internet user population grew from about 4.515 million people in 2000 to 453.3 million people in December, 2017, representing approximately 35.2 percent of Africa's entire population estimate.[1] This phenomenal growth, which still continues into the future,[2] has been linked to factors such as the liberalization of telecommunications markets in African States, the widespread proliferation of mobile telecommunication technologies, and the increasing availability of broadband capacity.[3] However, the spread of ICTs and Internet penetration in Africa has also raised concerns over the need to promote cybersecurity governance and cyber stability in the continent. This need prompted the African Union to establish a regional cybersecurity treaty known as the African Union (AU) Convention on Cyber Security and Personal Data Protection, in June, 2014.[4] The Convention imposes obligations on Member States to establish legal, policy and regulatory measures to promote cybersecurity governance and control cybercrime. This paper analyzes the nature and scope of the cybersecurity governance obligations under the Convention, and also examines how the adoption of the Convention can promote cyber stability in the African region, as well as the challenges impeding the application of the Convention as a framework for promoting regional cyber stability in Africa.

---

1 Miniwatts Marketing Group. (2017) *Internet Usage Statistics for Africa* [online]. Available from: http://www.internetworldstats.com/stats1.htm [Accessed 6 June 2018].

2 The GSMA (Global System for Mobile Communications Association) reports that *"over the next five years, an additional 168 million people will be connected by mobile services across Africa, reaching 725 million unique subscribers by 2020"*. See GSMA. (2016) *The Mobile Economy Africa 2016.* London: GSMA, p. 2.

3 See GSMA (2013) *The Mobile Economy Report 2013.* London: A. T. Kearney, p. 16.

4 See *The African Union Convention on Cyber Security and Personal Data Protection,* 27 June, 2014 (EX.CL/846 (XXV)).

The paper identifies the slow pace of ratification by Member States and the absence of effective regional coordination as some of the major reasons why the Convention has not been effectively applied as a framework for promoting regional cyber stability. Accordingly, the paper makes a case for the establishment of a regional monitoring mechanism within the AU framework to improve the regional harmonization of cybersecurity governance frameworks, and harness the application of the Convention as a framework for promoting regional cyber stability.

The paper comprises seven sections. The first section, which includes this introduction, will provide a brief overview of the concepts of cybersecurity and cyber stability. The second section discusses the development of the AU Convention on Cybersecurity. The third section discusses the nature and scope of the cybersecurity governance obligations under the Convention. The fourth section examines the legal status of the Convention in the domestic legal order of AU Member States. The fifth section examines the prospects of applying the Convention as a framework for promoting regional cyber stability in the African region, while the sixth section examines the challenges impeding the application of the Convention as a framework for promoting regional cyber stability. This is then followed by recommendations and the conclusion.

1.1 DEFINING CYBERSECURITY AND CYBER STABILITY

Cybersecurity is defined as

> *"the collection of tools, policies, guidelines, risk management approaches, actions, training, best practices, assurances and technologies that can be used to protect the cyber-environment and organization, as well as users' assets"*.[5]

Cybersecurity governance measures include technical, organizational, policy, and legal aspects.[6] The technical aspects of cybersecurity governance deal with the development and implementation of technical protection measures for computer systems and network infrastructure, while the organizational aspects deal with the development of institutional capacities to promote cybersecurity, such as the establishment of law

[5] See ITU High Level Experts Group (2008) *ITU Global Cyber-Security Agenda (GCA) High Level Experts Group [HLEG] Global Strategic Report*. Geneva: ITU, p. 27. See Orji, U. J. (2012) *Cybersecurity Law and Regulation*, Nijmegen: Wolf Legal Publishers, pp. 10–16.

[6] *Id*. at pp. 17–42.

enforcement organizations as well as the development of institutional capacities including the establishment of Computer Emergency Response Teams (CERTs) to provide critical services such as prevention and early warning, detection and management of cybersecurity incidents. The policy and legal aspects of cybersecurity governance deal with policy and legal measures that aim to promote cybersecurity. Legal measures are usually considered as probably the most relevant aspect of cybercrime control.[7] Such measures include the establishment of laws which prohibit acts that violate the security or integrity or availability of computer data and systems or networks and attacks against critical information infrastructure. It also includes legal measures to facilitate cross-border cooperation on cybersecurity, including the prevention, investigation and prosecution of prohibited acts.

On the other hand, the concept of "cyber stability" has been defined as

> *"a geostrategic condition whereby users of the cyber domain enjoy the greatest possible benefits to political, civic, social, and economic life, while preventing and managing conduct that may undermine those benefits at the national, regional, and international levels"*.[8]

It has been observed that this definition creates a basis from which to identify when stability is the goal and also to discern what is potentially relevant, useful, and strategic information about activity in the cyber domain from what is not.[9] However, cyber stability is also regarded an emerging concept that has not yet been developed as an analytic category.[10] Basically, the concept of cyber stability aims to promote the exercise of State responsibilities to address the security challenges of the information society. This particularly requires States to establish appropriate legal, policy and regulatory measures to protect cyber users and cyber infrastructure within their jurisdiction, and also ensure that cyber activities which are conducted within their jurisdiction do not cause harm to other individuals or infrastructure in another jurisdiction. Thus, the concept of cyber stability requires that States will establish cybersecurity

---

[7] See Marco, G. (2009) *Understanding Cybercrime: A Guide for Developing Countries.* Geneva: ITU, p. 84.

[8] See Rudnick, L. et al. (2015) *Towards Cyber Stability: A User-Centered Tool for Policy Makers*. Geneva: United Nations Institute for Disarmament Research, p. 7.

[9] *Id.*

[10] *Id.*

governance measures including criminal laws such as cybercrime laws and regulations for the purpose of deterring persons within their jurisdiction from engaging in malicious cyber activities that will cause harm to other individuals or infrastructure in another jurisdiction. Apparently, the need to promote cyber stability arises from the increasing the interconnectedness of national information communication networks in different countries which has ushered in an age of network interdependence where the security of each country's network is also dependent on the actions of State and non-State actors around the world. Therefore, the concept of cyber stability requires States to maintain governance responsibility over cyber activities on their territory, and thus it enshrines elements of the international principles of trans-boundary harm and State responsibility. These principles have been recognized in different contexts in the Corfu Channel Case, where the International Court of Justice (ICJ) held that a State may not

> *"allow knowingly its territory to be used for acts contrary to the rights of other States"*,[11]

and in the Trail Smelter Case, where it was held that

> *"no State has a right to use or permit the use of its territory in such a manner as to cause injury […] in or to the territory of another or the properties or persons therein"*.[12]

2. THE AFRICAN UNION AND THE DEVELOPMENT OF THE CONVENTION CYBERSECURITY

The African Union (AU) is an intergovernmental regional body that unites sovereign States within the entire African continent.[13] The AU was established in 2001 to replace the Organization of African Unity[14] and its headquarters is located in Addis Ababa, Ethiopia. Currently, the AU comprises 55 sovereign African States.[15] The aims of the AU include *inter alia* to *"accelerate the political and socio-economic integration"* of the African

[11] See *The Corfu Channel Case (United Kingdom v. Albania)* (1949) ICJ Reports 4, at paragraph 22.

[12] See *The Trail Smelter Arbitration Case (United States of America v. Canada)* (1938) 3 R.I.A.A. 1905. *See* Editorial, (1941) The Trail Smelter Arbitral Decision. *American Journal of International Law*, 35, p. 684.

[13] See The African Union (AU) [online] Available from: http://www.au.int/en/ [Accessed 6 June 2018].

continent;[16] to promote economic development and *"the integration of African economies"*,[17] and to

> *"coordinate and harmonize the policies between the existing and future regional economic communities for the gradual attainment of the objectives of the Union"*.[18]

These mandates which are enshrined in the Constitutive Act of the AU create broad legal basis for the AU and its institutions to establish regional policy and regulatory regimes on issues that affect Africa's economic integration and development, such as telecommunications/ICTs and cybersecurity governance.[19] However, the AU did not commence the development of concrete regulatory initiatives cybersecurity until after 2008.[20] A major factor that might have impeded the development of regional cybersecurity initiatives can be traced to the low penetration of ICTs in Africa prior to the widespread availability of wireless technologies within the first decade of the 21st century. One of the AU's first statements on the need to promote cybersecurity is found in the AU Draft Report on a Study of the Harmonization of Telecommunication, and Information Communication Technology Policies and Regulation (2008).[21] The Report emphasized the need for the establishment of a harmonized regional policy

---

[14] The AU was originally established as the Organization of African Unity (OAU) by the OAU Charter on 25 May, 1963 in Addis Abba, Ethiopia. However, on the September 1999, the Heads of States of the OAU issued a Declaration (The Sirte Declaration) which called for the establishment of an African Union to accelerate the process of integration within the African continent with a view to enhancing Africa's role in the global economy and also addressing Africa's social, economic and political problems. Subsequently, the AU was established on 26 May, 2001 in Addis Abba and launched on 9 July, 2002 in South Africa to replace the OAU. See African Union (2017) *African Union in a Nutshell.* [online] Available from: http://www.au.int/en/abut/nutshell [Accessed 6 June 2018].

[15] See African Union (2017) *Member States*. [online] African Union. Available from: http://www.au.int/en/member_states/country profiles [Accessed 6 June 2018].

[16] See Article 3(c) Constitutive Act of the AU. Togo: The Thirty-sixth Ordinary Session of the Assembly of Heads of State and Government. In English.

[17] See Article 3(j) *id.*

[18] See Article 3(i) *id.*

[19] See Orji, U. J. (2018) International Telecommunications Law and Policy. United Kingdom: Cambridge Scholars Publishing, p. 240.

[20] For example, in Europe issues relating to cybersecurity have been on the Council of Europe's agenda since 1976. See Council of Europe (1976) *Twentieth Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime*. Strasbourg. See Schjolberg, S. (2008) *The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva*, p. 2. [online] Available from: http://www.cybercrime law.net/documents/cybercrime_history.pdf [Accessed 6 June 2018].

[21] See African Union (2008) *Study on the Harmonization of Telecommunication and Information and Communication Technologies Policies and Regulation in Africa: Draft Report*. Addis Ababa, Ethiopia: African Union.

and regulatory framework on cybersecurity.[22] Subsequently, on 5 November, 2009, the AU Ministers in Charge of Communication and Information Technologies convened an Extraordinary Session in Johannesburg, South Africa, where they adopted a set of declarations known as the Oliver Tambo Declaration.[23] The Declaration directed the AU to

> *"jointly develop with the United Nations Economic Commission for Africa (UNECA), under the framework of the African Information Society Initiative, a Convention on cyber legislation based on the continent's needs and which adheres to the legal and regulatory requirements on electronic transactions, cybersecurity, and personal data protection"*.[24]

The Declaration further recommended that AU Member States should adopt the proposed Convention by 2012.[25]

In 2011, the efforts of the AU and UNECA led to the development of the Draft Convention for the Establishment of a Credible Legal Framework for Cybersecurity in Africa.[26] The Draft Convention was meant to harmonize the laws of African States on electronic commerce, data protection, cybersecurity governance and cybercrime control. Later, in June, 2012, the AU Expert Group on Cybersecurity (comprising experts from Member States and Regional Economic Communities in Eastern, Southern and Northern Africa) met in Addis Ababa, Ethiopia, to consider the Draft Convention.[27] The Draft Convention was subsequently adopted in September, 2012, by the AU Expert Group on Cybersecurity.[28] This was also followed by its approval during the 22nd Ordinary Session of the AU Executive Council in January, 2013. After that, the Draft Convention was to be presented for legal validation by the AU Justice Ministers Conference

---

[22] See African Union (2008) n. 21, p. 75.

[23] See Extra-Ordinary Conference of African Union Ministers in Charge of Communication and Information Technologies (2009) *Oliver Tambo Declaration*. Johannesburg, South Africa: African Union.

[24] *Id.* p. 4.

[25] *Id.*

[26] See Draft African Union (AU) Convention on the Establishment of a Credible Legal Framework for Cybersecurity in Africa, AU Draft0 010111, Version 01/01.2011.

[27] See Economic Commission for Africa (June 2012) *Declaration of Addis Ababa on the Harmonization of Cyber Legislation in Africa*. Addis Ababa: Economic Commission for Africa, paragraph 10, p. 2.

[28] *See* United Nations Economic Commission for Africa (UNECA) Press Release, *Draft African Union Convention on Cybersecurity Comes to its Final Stage*. [online] Available from: http://www1.uneca.org/TabId/3018/Default. aspx?ArticleId=1931 [Accessed 6 June 2018].

in October, 2013,[29] after which it was also to be presented for adoption by the AU Summit in January, 2014 and then open for signatures and ratification by AU Member States. However, the Draft Convention could not be presented to the AU for adoption in January, 2014, as a result of technical delays,[30] and also due to opposition from civil society groups and the academia.[31] There were also concerns that the Convention was drafted without a wide consultation of relevant stakeholders in Member States,[32] and lacked critical cybersecurity governance mechanisms to facilitate effective legal harmonization and international cooperation.[33] A revised version of the Draft Convention was later adopted on 27 June, 2014, by the AU Heads of State and Government during the 23rd Ordinary Session of the AU Assembly in Malabo.[34]

The Convention is known as the AU Convention on Cyber Security and Personal Data Protection[35] and basically aims to harmonize the laws of African States on electronic commerce, data protection, cybersecurity governance and cybercrime control. The Convention also defines the objectives for the information society in Africa and seeks to strengthen existing ICT laws in Member States and the Regional Economic

---

[29] See ECA Press Release (2012) ICT Ministers call for harmonized policies and cyber legislations on Cybersecurity. [online] Available from: http://www1.uneca.org/ArticleDetail/tabid/3018/ArticleId/1934/ICT-Ministers-call-for-harmonized-policies-and-cyberlegislations-on-Cybersecurity.aspx [Accessed 6 June 2018].

[30] See Rosewarne, C. and Odunfa, A. (2014) *The 2014 Nigerian Cyber Threat Barometer Report.* South Africa and Nigeria: Wolfpack Information Risk and Digital Jewels, p. 40.

[31] See Van Zyl, G. (2014) Adoption of 'flawed' AU Cybersecurity Convention Postponed. *IT Web Africa*. [online] Available from: http://www.itwebafrica.com/ict-and-governance/523-africa/232273-adoption-of-flawed-au-cybersecurity-convention-postponed [Accessed 6 June 2018].

[32] See *Open Forum to discuss the proposed legal framework for cybersecurity in Africa*, (26 July 2013) [online] Available from: http://daucc.wordpress.com/2013/07/26/event-panel-discussion-on-the-draft-african-union-cyber-security-convention/#comment-4 [Accessed 6 June 2018].

[33] See Orji, U. J. (2012) A Discourse on the Perceived Defects of the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cybersecurity. *Communications Law*: *The Journal of Computer, Media and Telecommunications Law*, vol. 17, no. 4, pp. 128–130.

[34] For a history of the development of AU Convention on Cybersecurity and Personal Data Protection, see Orji, U. J. (2014) Examining Missing Governance Mechanisms in the African Union Convention on Cybersecurity and Personal Data Protection. *Computer Law Review International*, Issue 5, pp. 129–135; Orji, U. J. (2015) Multilateral Legal Responses to Cybersecurity in Africa: Any Hope for Effective International Cooperation? In Maybaum, M. *et al* (eds.) *Architectures in Cyberspace – 7th International Conference on Cyber Conflict*. Tallinn, Estonia: NATO Cooperative Cyber Defence Center of Excellence, pp. 105–118; Orji, U. J. (2012) A Discourse on the Perceived Defects of the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cybersecurity. *Communications Law*: *The Journal ofComputer, Media and Telecommunications Law*, 17 (4), pp. 128–130.

[35] See *African Union Convention on Cyber Security and Personal Data Protection*, 27 June 2014 (EX.CL/846(XXV)) (hereafter, *AU Convention on Cybersecurity and Personal Data Protection*).

Communities (RECs).[36] With respect to cybersecurity governance and cybercrime control, the Convention recognizes that:

> *"the current state of cybercrime constitutes a real threat to the security of computer networks and the development of the information society in Africa"*[37]

and that this state of affairs underscores the need

> *"to define broad guidelines of the strategy for the repression of cybercrime in Member States of the AU, taking into account their existing commitments at the sub-regional, regional and international levels".*[38]

Accordingly, the Convention adopts a *"technology neutral"*[39] language to establish substantive and procedural criminal law provisions which address cybersecurity governance and cybercrime control in AU Member States. Thus, aside from establishing substantive and procedural criminal law provisions on cybercrime, the Convention also imposes broad obligations on Member States to establish national cybersecurity policies as well as legal, regulatory and institutional frameworks for cybersecurity governance and cybercrime control. This approach apparently goes beyond that of the Council of Europe Convention on Cybercrime[40] which mainly requires Member States to criminalize cybercrimes by establishing substantive criminal law measures as well as procedural and international cooperation mechanisms for law enforcement.[41] The Convention will enter into force after it has been ratified by 15 AU Member States.[42]

---

[36] See Preamble, *AU Convention on Cybersecurity and Personal Data Protection*, 2014.

[37] *Id.*

[38] *Id.*

[39] The technology neutrality principle proposes that *"legislation should define the regulation to be achieved and should neither impose, nor discriminate in favour of the use of a particular type of technology to achieve those objectives"*. See European Commission (1999) *Towards a New Framework for Electronic Communications Infrastructure and Associated Services.* Brussels: European Commission, p. 539. See generally, Sharpe A. (2009) Communications Technologies, Services and Markets. In: Ian Walden (ed.) *Telecommunications Law and Regulation*. 3rd ed. New York: Oxford University Press, p. 53.

[40] See *The Council of Europe Convention on Cybercrime*, 23 November 2001 (41 I.L.M. 282).

[41] See Orji, U. J. (2014) Examining Missing Governance Mechanisms in the African Union Convention on Cybersecurity and Personal Data Protection. *Computer Law Review International*, vol. 5, p. 132.

[42] See Article 36 *AU Convention on Cybersecurity and Personal Data Protection*.

3. MEMBER STATE OBLIGATIONS TO IMPLEMENT MEASURES THAT PROMOTE CYBER STABILITY

The Convention establishes obligations on Member States to implement measures that will promote cyber stability. In this regard, the Convention requires Member States to implement obligations that include: establishing a national cybersecurity framework; promoting a culture of cybersecurity; establishing national cybersecurity governance structures; protecting critical information infrastructure; establishing cybercrime offences and procedural measures; and, promoting international cooperation and legal harmonization. These obligations are discussed below.

3.1 OBLIGATIONS TO ESTABLISH A NATIONAL CYBERSECURITY FRAMEWORK

The Convention requires Member States to promote cyber stability by establishing appropriate cybersecurity governance frameworks. In this regard, Member States are required to establish a national cybersecurity framework that comprises a national cybersecurity policy and a national cybersecurity strategy.[43] A Member State's national cybersecurity policy is required to recognize the importance of national Critical Information Infrastructure (CII), and identify related risks using the all-hazards approach, while also outlining how the objectives of such policy are to be achieved.[44] The "all-hazards" approach to CII protection entails the protection of such infrastructure from all forms of threats, whether they originate from deliberate attacks, accidents or natural disasters.[45] In addition, the obligation to establish a national cybersecurity policy requires Member States to outline how their national cybersecurity policy will achieve the objectives of protecting national CII from identified risks.

With respect to the establishment of a national cybersecurity strategy, Article 24:2 of the Convention requires Member States to adopt strategies they deem "appropriate and adequate" when implementing their national cybersecurity policy, especially when undertaking initiatives such as legal reform and development, capacity building, public-private partnership,

---

[43] See Article 24 *AU Convention on Cybersecurity and Personal Data Protection*, 2014.

[44] See Article 24:1 *id*.

[45] See Gordon, K. and Dion, M. (2008) *Protection of 'Critical Infrastructure' and the Role of Investment Policies Relating to National Security*. Paris: OECD, p. 5. See also Brommelhorster, J. et al. (2004) Critical Infrastructure Protection: Survey of World-wide Activities. *BSI KRITIS*, (4), p. 1.

international cooperation and cybersecurity awareness raising. In this regard, the Convention recognizes the sovereign right of each Member State to adopt any strategy that it deems fit or appropriate in order to effectively implement its national cybersecurity policy. The obligation under Article 24:2 of the Convention also requires that a Member State's national cybersecurity strategy should define the organizational structures for cybersecurity governance, set objectives and timeframes for the successful implementation of the national cybersecurity policy, and also establish the critical basis for the effective management of cybersecurity incidents and international cooperation in such matters.

To a large extent, the Convention's requirement that Member States should establish cybersecurity policies and strategies appears similar to Article 7 of the European Union (EU) Directive on Network and Information Security (2016)[46] which also requires Member States to adopt

> *"a national strategy on the security of network and information systems defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems […]".*[47]

3.2 OBLIGATIONS TO PROMOTE A CULTURE OF CYBERSECURITY

Article 26 of the Convention establishes obligations on Member States to promote a culture of cybersecurity amongst all stakeholders (such as governmental institutions, businesses and the civil society) that develop, operate, or use information systems and networks.[48] In this respect, Article 26:1 (a) of the Convention declares that

> *"the culture of cybersecurity should lay emphasis on security in the development of information systems and networks, and on the adoption of new ways of thinking and behaving when using*

[46] See Directive of the European Parliament and of the Council of 6 July 2016 concerning Measures for a High Common Level of Security of Network and Information Systems across the Union, *Official Journal of the European Union* (2016/1148) 19 July 2016) (hereafter *EU Directive on Network and Information Security*, 2016).

[47] See Article 7:1 EU Directive on Network and Information Security (2016).

[48] See Article 26:1(a) AU Convention on Cybersecurity and Personal Data Protection.

> *information systems as well as during communication or transactions across networks".*[49]

The need for the promotion of a culture of cybersecurity arises from the increasing interconnection of networks and the growing integration of networked ICTs to many of the essential aspects of daily life, including the provision of goods and services, research and development, innovation and entrepreneurship, and the free flow of information amongst individuals and organizations, governments, businesses and civil society.[50] This state of affairs implies that cybersecurity governance issues are not meant to be addressed only through the application of law enforcement or technological measures, but rather through holistic governance approaches that are widely supported by society.[51]

The obligation to promote a culture of cybersecurity under Article 26 of the Convention requires Member States to take the lead in developing a cybersecurity culture within their national territories by promoting public awareness and providing education and training on cybersecurity.[52] In this regard, Member States have obligations to

> *"adopt measures to develop capacity building with a view to offering training which covers all areas of cybersecurity to different stakeholders, and setting standards for the private sector".*[53]

This also includes the promotion of technical education for ICT professionals in both the public and private sectors through certifications and standardization trainings.[54] In addition, Member States are required to develop a public-private partnership model that will engage the participation of stakeholders such as industry groups, the civil society and the academia in promoting a culture of cybersecurity.[55]

---

[49] See Article 26:1(a) *AU Convention on Cybersecurity and Personal Data Protection.*

[50] See *United Nations Resolution on the Creation of a Global Culture of Cybersecurity,* 21 December 2009 (A/RES/64/211). See also *United Nations Resolution on the Creation of a Global Culture of Cybersecurity,* 23 December 2003 (A/RES/58/199).

[51] See ITU (2009) *National Cybersecurity/CIIP Self-Assessment Tool*. Geneva: ITU, p. 26. See also United Nations Resolution on the Creation of a Global Culture of Cybersecurity, 20 December 2003 (A/RES/57/239).

[52] See Article 26:2 AU Convention on Cybersecurity and Personal Data Protection.

[53] See Article 26:4 *id.*

[54] *Id.*

[55] See Article 26:3 *id.*

3.4 OBLIGATIONS TO ESTABLISH NATIONAL CYBERSECURITY GOVERNANCE STRUCTURES

Article 25:2 of the Convention imposes obligations on Member States to establish appropriate structures or institutions as well as regulatory powers that are necessary for cybersecurity governance. Article 27:1(a) of the Convention also requires Member States

> *"to adopt the necessary measures to establish an appropriate institutional mechanism responsible for cybersecurity governance".*[56]

to a large extent, the provisions of Articles 25:2 and 27:1(a) of the Convention have similar implications with Article 8(1) of the EU Directive on Network and Information Security (2016), which requires Member States to

> *"designate one or more national competent authorities on the security of network and information systems".*[57]

Under the Convention, the obligations to establish national cybersecurity governance structures requires the establishment of appropriate national institutions with responsibilities to tackle cybercrimes and respond to cybersecurity incidents, and also facilitate international cooperation in the management of such incidents.[58] Thus, within the context of those obligations, it is implied that every Member State should establish institutions such as a national cybersecurity agency and a national Computer Emergency Response Team (CERT).[59] The Convention also requires that national cybersecurity governance structures should be established within a national framework that can respond to challenges and issues affecting all aspects of cybersecurity at the national level.[60] In order to ensure the effective functioning of national cybersecurity structures, the Convention requires Members States to take necessary measures to establish clear accountability on cybersecurity issues at all levels of government by defining the roles and responsibilities of institutions

---

[56] See Article 27:1(a) *AU Convention on Cybersecurity and Personal Data Protection.*
[57] See Article 8:1 EU Directive on Network and Information Security (2016).
[58] See Article 27:2 AU Convention on Cybersecurity and Personal Data Protection.
[59] See Article 28:3 *id.*
[60] See Article 27:1(c) *id.*

in clear and precise terms[61] and also expressing a clear public and transparent commitment to the promotion of cybersecurity, including encouraging the participation of the private sector in governmental initiatives to promote cybersecurity.[62]

3.5 OBLIGATIONS TO PROTECT CRITICAL INFORMATION INFRASTRUCTURE

The Convention establishes obligations on Member States to protect CII. In this respect, Article 25:4 of the Convention requires Member States to adopt necessary legislative and regulatory measures to identify those sectors that are "sensitive" to their national security and economic wellbeing, and also to classify the ICT systems that are designed to function in those sectors as elements of CII. Although, the Convention does not define the meaning of CII, it however classifies CII in relation to the concept of *"Critical Cyber/ICT Infrastructure"*.[63] Under Article 1 of the Convention the concept of Critical Cyber/ICT Infrastructure is defined as

> *"the cyber infrastructure that is essential to vital services for public safety, economic stability, national security, international stability and for the sustainability and restoration of critical cyberspace".*[64]

The CII protection obligations under Article 25:4 of the Convention requires Member States to establish severe sanctions for cybercrimes and other criminal activities that affect ICT systems in critical sectors and also establish measures to improve the security and management of such systems.[65] Article 30:1(d) of the Convention also creates a CII protection obligation which requires Member States to

> *"establish necessary criminal law measures to restrict access to protected systems which have been classified as critical national defence infrastructure due to the critical national security data they contain".*[66]

The Convention does not provide a definition of *"critical national defence infrastructure"*, however, within the context the term would apparently refer

---

[61] See Article 27:1(b) (i) *AU Convention on Cybersecurity and Personal Data Protection.*
[62] See Article 27:1(b) (ii) *id.*
[63] See Article 1 *id.*
[64] *Id.*
[65] See Article 25:4 *id.*
[66] See Article 30:1(d) *id.*

to CII (critical cyber/ICT infrastructure) which are used to provide national defence services, such as computer systems that are used for national security or military operations.

The Convention does not explicitly classify the sectors that should be regarded as "sensitive" to the national security and economic wellbeing of Member States. Apparently, the absence of such explicit classification could be due to the fact that sectors which are designated as "sensitive" vary in different countries.[67] However, the common trend in establishing such classification is that where the prolonged disruption of a sector or infrastructure would affect the wellbeing of a State by causing severe economic dislocation or national security challenges, then such sector or infrastructure is generally regarded as being "sensitive" to the national security and economic wellbeing of the State and therefore classified as a "critical sector" or "critical infrastructure".[68] Such sectors include (but are not limited to) banking and financial services, governmental services, telecommunications services and ICT infrastructure providers, emergency and rescue services, energy and electricity services, health services, transportation services including traffic management services, and water supply and distribution services.[69] Generally, most of the sectors that are classified as "critical sectors" rely heavily on elements of ICT systems such as computer technologies and digital networks to function effectively. Consequently, those elements of ICT systems in critical sectors are classified as CII. Therefore, the CII concept is generally used to designate core ICT elements including interconnected and interdependent information network systems that are vital to the functioning of critical sectors and essential services in modern societies.

The essence of establishing CII protection obligations in the African context arise from the increasing penetration of ICTs in Africa[70] which has given rise to their growing integration in sectors that can be classified

[67] See generally, Gordon, K. and Dion, M. (2008) *Protection of 'Critical Infrastructure' and the Role of Investment Policies Relating to National Security*. Paris: OECD.

[68] See the United States President's Commission on Critical Infrastructure Protection (PCCIP). (1997) *Critical Foundations: Protecting America's Infrastructure*. Washington DC: PCCIP, Appendix B, Glossary B-2.

[69] See Dunn, M. (2005) A Comparative Analysis of Cybersecurity Initiatives Worldwide. *World Summit on Information Society (WSIS) Thematic Meeting on Cybersecurity*. Geneva: ITU, p. 14. See Annex II EU Directive on Network and Information Security (2016).

[70] See GSMA (2016) *The Mobile Economy Africa 2016*. London: GSMA, pp. 2, 8 & 19. See also, Miniwatts Marketing Group (2017) *Internet Usage Statistics for Africa*. [online] Miniwatts Marketing Group. Available from: http://www.internetworldstats.com/stats1.htm [Accessed 6 June 2018].

as critical sectors. This increasing integration of ICTs in critical sectors is also seen a means of facilitating Africa's economic development and regional integration.[71] However, while African States have not achieved a high level of digitalization that is comparable to developed countries, the rise of digitalization in Africa has increased the reliance of critical sectors on ICT elements as well as interconnected and interdependent information network systems, to the extent that the disruption of such infrastructure by accidents or malicious acts could also cause the disruption of economic and social activities as well as public services, and thereby trigger national security concerns.[72] Therefore, African States are also vulnerable to cybersecurity threats which affect the elements of critical sectors that rely on information infrastructure usually classified as CII. This appears to underscore the reason why Article 25:4 of the Convention aims to enhance the protection of CII in Africa by imposing obligations on AU Member States to establish legal and policy measures for their identification and protection.

3.6 OBLIGATIONS TO ESTABLISH CYBERCRIME OFFENCES AND PROCEDURAL MEASURES

Article 25:1 of the Convention imposes obligations on Member States to criminalize substantive criminal acts that affect the confidentiality, integrity, availability and survival of ICT systems, and the data processed by such systems. This implies that Member States are required to establish offences that criminalize acts such as unauthorized access to a computer system, unauthorized interference with a computer system or data, and unauthorized interception of data processed by a computer system. In addition, Article 25:1 of the Convention requires Member States to criminalize substantive criminal acts that affect ICT network infrastructure. This entails the establishment of offences that criminalize attacks against CII. The Convention also requires Member States to explicitly criminalize cybercrime offences including: attacks on computer systems;[73] unauthorized access to computer systems;[74] acts that hinder

[71] See GSMA (2016), n. 70, p. 2. *See also* GSMA (2013) *Sub-Saharan Africa Mobile Economy Report 2013.* London: A.T. Kearney, p. 4.

[72] See Solutions Consulting (2018) *West Africa Cybersecurity Indexing and Readiness Assessment.* Florida, United States: Solutions Consulting, p. 8.

[73] See Article 29:1 AU Convention on Cybersecurity and Personal Data Protection.

[74] See Article 29:1(a) *id.*

the functioning of a computer;[75] unauthorized modification of computer data;[76] unauthorized interception of computer data;[77] computer data forgery;[78] computer fraud;[79] child pornography offences;[80] and preparatory offences relating to the misuse of computing devices, such as the unlawful production, sale, importation, possession, or making available of computer equipment, program, or any device or data that is *"designed or specifically adapted"* for the purpose of committing any cybercrime offence.[81] To some extent, the Convention's requirement that Member States should explicitly criminalize the above cybercrime offences appears similar to some of the obligations under the European Union Directive on Attacks against Information Systems (2013).[82] For example, the Directive requires Member States to criminalize illegal access to information systems,[83] illegal interference with information systems,[84] illegal data interference,[85] and illegal data interception.[86]

Article 25:1 of the Convention also imposes obligations on Member States to establish effective procedural mechanisms for the prosecution of cybercrime offences. Such procedural mechanisms are basically meant to enhance the legal capabilities of law enforcement authorities to investigate and prosecute cybercrime offences, and they usually include measures to facilitate the search, seizure, or preservation of digital evidence, or the interception of electronic communications. While establishing substantive and procedural legal measures to tackle cybercrimes, Member States are also required to take into consideration the choice of language that is used in international best practices.[87] This implies that Member States are to consider the choice of language that is used in international

[75] See Article 29:1(d) *AU Convention on Cybersecurity and Personal Data Protection.*

[76] See Article 29:1(e) & (f) *id.*

[77] See Article 29:2(a) *id.*

[78] See Article 29:2(b) *id.*

[79] See Article 29:2(d) *id.*

[80] See Article 29:3(1) *id.*

[81] See Article 29:2(b) *id.*

[82] See Directive of the European Parliament and of the Council of 12 August 2013 on Attacks against Information Systems (2013/40/EU) replacing Council Framework Decision 2005/222/JHA. *Official Journal of the European Union,* 14. August 2013 (hereafter, EU Directive on Attacks against Information Systems, 2013).

[83] See Article 3 EU Directive on Attacks against Information Systems (2013).

[84] See Article 4 *id.*

[85] See Article 5 *id.*

[86] See Article 6 *id.*

[87] See Article 25:1 AU Convention on Cybersecurity and Personal Data Protection.

instruments and model laws on cybercrime such as the Council of Europe Convention on Cybercrime and the ITU Toolkit for Cybercrime Legislation.[88] Apparently, this obligation aims to encourage Member States to draft substantive and procedural legal measures on cybercrime in a technology neutral language in order to promote the international harmonization of national cybercrime laws and procedural measures.

In addition, Article 25:3 of the Convention requires Member States to ensure that the establishment and implementation of legal measures for cybersecurity governance does not infringe the constitutional rights of citizens, such as the right to freedom of expression, the right to privacy, the right to fair hearing, and other fundamental rights that are protected under national or international law, including those established under the African Charter on Human and People's Rights.[89] This requirement appears similar to some degree with the approach that is adopted by the Council of Europe Convention on Cybercrime. Thus, the Council of Europe Convention on Cybercrime requires Member States to ensure that their procedural instruments for the investigation and prosecution of cybercrime do not violate fundamental human rights.[90]

3.7 OBLIGATIONS TO PROMOTE INTERNATIONAL COOPERATION AND LEGAL HARMONIZATION

The Convention establishes a framework to facilitate international cooperation on cybersecurity and cybercrime control within the AU. In this regard, Member States are required to

> *"encourage the establishment of institutions that exchange information on cyber threats and vulnerability assessment such as Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs)".*[91]

Article 28:4 of the Convention also requires Member States to

---

[88] See ITU and American Bar Association - Privacy and Computer Crime Committee (2010) *ITU Toolkit for Cybercrime Legislation*. Geneva: ITU.

[89] See *African (Banjul) Charter on Human and Peoples' Rights*, 27 June 1981 (OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58) which entered into force on 21 October 1986.

[90] See Article 15:2 Council of Europe Convention on Cybercrime.

[91] See Article 28:3 Convention on Cybersecurity and Personal Data Protection.

> *"make use of existing channels for international cooperation with a view to responding to cyber threats and improving cybersecurity and stimulating dialogue between stakeholders".*[92]

Such channels for international cooperation may be based on international or intergovernmental or regional arrangements, or private and public partnerships.[93]

In order to facilitate the effective harmonization of legal rules and international cooperation amongst Member States, Article 28:1 of the Convention establishes obligations on Member States to

> *"ensure that the legislative measures and/or regulations adopted to fight against cybercrime will strengthen the possibility of regional harmonization […] and respect the principle of double criminal liability".*[94]

Article 28:2 of the Convention also provides that Member States that do not have mutual assistance agreements on cybercrime

> *"shall undertake to encourage the signing of agreements on mutual legal assistance in conformity with the principle of double criminal liability, while promoting the exchange of information as well as the efficient sharing of data between the organizations of [Member States] on a bilateral and mutual basis".*[95]

This implies that Member States that lack mutual legal assistance agreements on cybercrime have obligations to engage in such agreements in accordance with the principles of double criminality (dual criminality).[96]

---

[92] See Article 28:4 *AU Convention on Cybersecurity and Personal Data Protection.*

[93] *Id.*

[94] See Article 28:1 *id.*

[95] See Article 28:2 *id.*

[96] "Double criminality" or "dual criminality" exists where a conduct in issue has been criminalized in the laws of both the State requesting for assistance or extradition and the State to whom such request for assistance or extradition is being made to. Under this principle, an extradition request can only be granted in accordance with an extradition treaty between two countries where both countries have criminalized the criminal conduct for which an extradition request is sought and the crimes are punishable by one year imprisonment or more. See ITU High Level Experts Group [HLEG]. (2008) *ITU Global Cyber-Security Agenda (GCA) High Level Experts Group [HLEG] Global Strategic Report*. Geneva: ITU, p. 14. *See also* Garner, B. A. (ed.) (2004). *The Black's Law Dictionary*. 8th ed., St Paul MN, United States: West Publishing Co, p. 537.

4. THE STATUS OF THE AU CYBERSECURITY CONVENTION IN THE DOMESTIC LEGAL ORDERS

Having discussed the Convention's Member State obligations that aim to promote cyber stability, this section will discuss the legal status of the Convention in the domestic legal systems of Member States. Article 35 of the AU Cybersecurity Convention provides that the Convention

> *"shall be open to all Member States of the Union, for signature, ratification or accession, in conformity with their respective constitutional procedures".*[97]

The Convention will enter into force after it has been ratified by 15 AU Member States.[98] According to a report by the AU, as of May 2018, only 10 AU Member States (Benin, Chad, Comoros, Congo, Ghana, Guinea-Bissau, Mauritania, Sierra Leone, Sao Tome & Principe and Zambia) had signed the Convention, while two Member States (Mauritius and Senegal) had ratified the Convention.[99] The AU report also showed that the signatures and ratifications were done in 2015, 2016, 2017 and 2018 with none in 2014 when the Convention was adopted.[100] This slow pace of Member States towards signing and ratifying the Convention would hinder the timely achievement of its objectives such as the harmonization of cybersecurity laws in Member States. More importantly, the slow pace of ratifications also indicates that it will probably take some more years before the Convention can be ratified by the required 15 Member States in order for it to have legal force within the AU. This state of affairs practically impedes the sense of urgency that should normally characterize cybersecurity governance responses and also has the effect of slowing down the urgency of implementing the Convention's obligations.

However, it is also recognized that one of the major challenges to the effective implementation of international and regional legal instruments has been how to balance national sovereignty concerns

---

[97] See Article 35 AU Convention on Cybersecurity and Personal Data Protection.

[98] See Article 36 *id.*

[99] See African Union. (2018) *List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection.* [online] African Union. Available from: https//au.int/sites/default/files/treaties/29560-slafrican_union_convention_on_cyber_security_and_personal_data_protection.pdf [Accessed 6 June 2018].

[100] *Id.*

by Member States and the obligations under such legal instruments in order to ensure that they are recognized and domestically implemented by Member States. The AU comprises English speaking (Anglophone), French speaking (Francophone) and Portuguese speaking (Lusophone) Member States that operate different legal systems with respect to the domestic reception of international or regional legal instruments. The Anglophone States that are Members of the AU operate a dualist legal tradition. Under the dualist legal tradition, national law and international law are considered as two distinct categories of legal systems. Hence, regional legal instruments, such as the AU Cybersecurity Convention, cannot be directly applied within the national legal system of a dualist State, unless they have been domesticated by an Act of the parliament. For example, in Nigeria which is an AU Member State that operates a dualist legal tradition, Section 12(1) of the 1999 Constitution provides that

> *"No treaty between the Federation and any other country shall have the force of law except to the extent to which any such treaty has been enacted into law by the National Assembly".*[101]

A similar legal requirement exists in the Constitutions of other Anglophone Member States within the AU.[102]

On the other hand, Francophone States that are Members of the AU operate a monist legal tradition. Under this tradition, international law and national law are regarded as the manifestations of a single conception of law since both laws are meant to apply to the conduct of the same subjects.[103] The monist legal tradition is regarded as having its root in national law theories which see all law as the product of reason.[104] Thus, it

[101] See Section 12:1 *Constitution of the Federal Republic of Nigeria* (1999).

[102] See for *e.g.*, Section 79:1 *Constitution of the Gambia* (1997); Section 75:1 *Constitution of Ghana* (1992); Article 40:4(1) *Constitution of Sierra Leone* (1991), and; Section 57 *Constitution of Liberia* (1986).

[103] See Oji, E. A. (2011) Application of Customary International Law in Nigerian Courts. *Nigeria Institute of Advanced Legal Studies Law and Development Journal*, 1(1), p. 156.

[104] See Oppong, R. F. (2008) Making Regional Economic Laws Enforceable in National Legal Systems: Constitutional and Judicial Challenges. In Bosi, A. and Breytenbech, W. et al (eds.) *Monitoring Regional Integration in Southern Africa Year Book*. Stellenbosch: Trade Law Center for Southern Africa, pp. 10–11.

> *"envisions international law to automatically be part of national legal systems and suggests that no conflict can arise between international and national law because they derive from the same source"*.[105]

Accordingly, the monist legal tradition allows international law or community law to become part of a State's national law without the need for an enactment to domesticate such international law within a State's legal system, provided that such law is reciprocally enforced by other State parties. Therefore, an AU Member State that operates a monist legal tradition would allow a regional legal instrument such as the AU Cybersecurity Convention to become part of its national law without the need for the domestication of the Convention within that State's legal system, provided however, that the Convention is reciprocally enforced by other Member States. For example, in the Republic of Benin which is an AU Member State that operates a monist legal tradition, Article 147 of the Constitution provides that treaties or agreements lawfully ratified shall have upon their publication an authority superior to that of laws, without prejudice for each agreement or treaty in its application by the other party.[106] A similar legal requirement exists in other Francophone States within the AU.[107] The Lusophone States within the AU also practice a monist legal tradition and establish similar requirements for the enforcement of regional legal instruments such as the AU Cybersecurity Convention.[108]

5. PROSPECTS OF APPLYING THE CONVENTION AS A FRAMEWORK FOR REGIONAL CYBER STABILITY

The AU Cybersecurity Convention holds several prospects towards promoting regional cyber stability in Africa. Such prospects arise from

---

[105] See Oppong, R. F. (2008) n. 104, p. 11.

[106] See Section 147 *Constitution of the Republic of Benin* (1990).

[107] See for e.g., Article 98 of the *Constitution of Senegal* (2001) which provides that treaties or agreements duly ratified shall, upon their publication, have an authority superior to that of the laws, subject to its application by the other party.

[108] See for e.g., Article 11:2 of the *Constitution of Cape Verde* (1992) which provides that *"international treaties and agreements, validly approved or ratified, shall be in force in the Cape Verdian legal order after their official publication and their entry into force in the international legal order, and for the time that they are internationally binding on the State of Cape Verde"*. See also Article 11:4 of the *Constitution of Cape Verde* which provides that rules and principles of general or common international law and of conventional international law, validly approved or ratified, shall prevail, after their entry into force in the international and domestic legal orders over all legislative and domestic normative acts of an infra--constitutional value.

the fact that the establishment of the Convention increases policy and regulatory awareness on cybersecurity governance, while also improving the harmonization of national cybersecurity regimes in AU Member States. Other prospects of the Convention in this regard include that it imposes a range of positive obligations on AU Member States to establish national cybersecurity regimes, and also increases the possibility of imposing AU sanctions on non-compliant Member States. These prospects are discussed below.

5.1 INCREASED CYBERSECURITY AWARENESS

One of the major advantages of establishing regional legal instruments for cybersecurity governance is that they enhance the cybersecurity awareness of regional organizations and their Member States.[109] As such, there are prospects that the establishment of the AU Cybersecurity Convention would help to promote cyber stability by increasing regional and national awareness on cybercrime and cybersecurity governance in Africa. Such awareness can also help to facilitate the establishment of cybersecurity laws and policies and other governance frameworks, such as CERTs in AU Member States that are yet to establish such frameworks. For example, as of June, 2018, about 40 States out of the 55 States of the African continent had established laws on cybersecurity, while about 20 States had established national cybersecurity policies, and, on the other hand, 18 States had national CERT frameworks.[110]

5.2 HARMONIZATION OF NATIONAL CYBERSECURITY REGIMES

Another advantage of establishing regional legal instruments for cybersecurity governance is that such instruments provide a model framework of minimum standards that will guide Member States in the development of their national cybersecurity regimes. In this regard,

---

[109] See Orji, U. J. (2016) Regionalizing Cybersecurity Governance in Africa: An Assessment of Responses. In Samuel, C. and Sharma, M. (eds.) *Securing Cyberspace: International and Asian Perspectives.* New Delhi: Institute for Defence Studies and Analyses & Pentagon Press, p. 211.

[110] See UNCTAD. (2018) *Cybercrime Laws.* [online] Available from: http://www.unctad.org/en/Docs/Cyberlaw/CC.xlsx [Accessed on 6 June 2018]. See ITU. (2018) *Cybersecurity Country Profiles.* [online] Available from: https//www.itu/en/ITU-D/Cybersecurity/Documents/Country_Profiles/ [Accessed 6 June 2018]. See also African Union and Symantec Corporation. (2016) *Cyber Crime & Cyber Security Trends in Africa*. United States: Symantec Corporation, pp. 53–56.

harmonization refers to the process of creating common standards within Member States that belong to a common regional or international intergovernmental body with a view to promoting uniformity in national laws and policies. Harmonization helps to coordinate different national legal and regulatory systems by eliminating or minimizing major differences in national laws and policies, and thereby creating minimum standards in a manner that makes them similar with each other.[111] Within the context of cybersecurity governance, the harmonization of national cybersecurity regimes through regional instruments contributes to a large extent in minimizing national differences in such regimes and also helps in promoting regional cybersecurity cooperation. Thus, to a large extent, the AU Cybersecurity Convention's establishment of minimum standards that are meant to guide Member States in the development of their national cybersecurity regimes also has prospects to promote regional cyber stability through legal harmonization and cybersecurity cooperation within the AU.

5.3 IMPOSITION OF POSITIVE OBLIGATIONS ON MEMBER STATES

Apparently, the most significant implication that arises from the adoption of the AU Cybersecurity Convention by Member States is that the Convention imposes positive obligations on them to promote cyber stability by establishing legal, policy and regulatory frameworks on cybersecurity governance and cybercrime control. As such, every AU Member State that is a party to the Convention has positive obligations to establish national cybersecurity laws, as well as policy and regulatory frameworks that enshrine the standards under the Convention. Thus, under international law, the general principle of *pacta sunt servanda* which is expressed in Article 26 of the Vienna Convention on the Law of Treaties declares that

> *"every treaty in force is binding upon the parties to it and must be performed by them in good faith."*[112]

The Vienna Convention further declares that

---

[111] See Shuma, T. (2015) Revisiting Legal Harmonization under the Southern African Development Community Treaty: The Need to Amend the Treaty. *Law, Democracy and Development*, 19, pp. 135–136. See also Walter, J. K. (1974) Comparative Law: A Theoretical Framework. *International and Comparative Law Quarterly*, 23 (3), p. 501.

[112] See Article 26, *Vienna Convention on the Law of Treaties*, 23 May 1969.

> *"a party may not invoke the provisions of its internal law as justification for its failure to perform a treaty"*.[113]

Consequently, it appears that, once the AU Cybersecurity Convention has entered into force, the positive obligations under the Convention can provide a basis for holding a Member State accountable, where the latter's failure to fulfill the obligations to establish relevant cybersecurity governance frameworks has encouraged the perpetration of cybercrime which results in the violation of human rights, such as those rights guaranteed under African international human rights instruments, including the African Charter on Human and Peoples' Rights,[114] the African Charter on Rights and Welfare of the Child,[115] and the Protocol on the Rights of Women in Africa.[116] In this regard, another Member State, or an individual, or a non-governmental organization that has an Observer status before the African Commission on Human and Peoples' Rights, can directly institute an action before the African Court on Human and Peoples' Rights for a determination of a Member State's liability for the non-fulfillment of its positive obligations under the AU Cybersecurity Convention.[117]

A Member State's failure to fulfill the obligations under the AU Cybersecurity Convention can also provide a valid basis for bringing a Communication before the African Commission on Human and Peoples' Rights, where the non-fulfillment of those obligations has resulted in the violation of any of the rights guaranteed under the African Charter on Human and Peoples' Rights.[118] In this respect, an individual may bring a Communication before the Commission to determine a Member State's liability, where the failure of such Member State to fulfill the obligations under the Convention (such as the establishment of legal and regulatory frameworks for cybersecurity governance) has passively encouraged the perpetration of cybercrimes that resulted in the violation of any

---

[113] See Article 27 *id.*

[114] See *African (Banjul) Charter on Human and Peoples' Rights*, 27 June 1981 (OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58).

[115] See *African Charter on the Rights and Welfare of the Child*, 1990 (OAU Doc. CAB/LEG/24.9/49).

[116] See *Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa*, 11 July 2003.

[117] See Articles 5:1 & 5:3 *Protocol to the African Charter on Human and Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights*, 10 June 1998.

[118] See Articles 45, 47 and 56 *African Charter on Human and Peoples' Rights* (1982).

of the human rights under the African Charter.[119] The possibility of holding an AU Member State accountable for its failure to fulfill the obligations under the African Charter has already been illustrated in several decisions of the African Commission on Human and Peoples' Rights (ACHPR).[120] For example, in *Social and Economic Rights Action Center (SERAC) and the Center for Social and Economic Rights (CESR) v. Nigeria*[121], a Communication which was brought before the ACHPR alleged that the Nigerian government had been directly involved in oil production through the Nigerian National Petroleum Company (NNPC) alongside other multinational oil companies, and that oil production caused environmental degradation and severe health problems amongst the Ogoni people of the Niger Delta. The ACHPR found the Nigerian government liable for not fulfilling its positive obligations under the African Charter as a result of its failure to take measures to prevent environmental pollution and promote sustainable development use of natural resources in Ogoni land.[122] Thus, the ACHPR, while finding Nigeria liable for the violation of the right to health and the right to a generally satisfactory environment under Articles 16 and 24 of the African Charter, held that

> *"the State is obliged to protect right holders against other subjects by legislation and provision of effective remedies […] [and that] protection generally entails the creation and maintenance of an atmosphere or framework by an effective interplay of laws and regulations so that individuals will be able to freely realize their rights and freedoms"*.[123]

The ACHPR also held that a State is required to fulfill the rights and freedoms it freely undertook under the various human right regimes.[124]

The possibility of holding a State accountable for the non-fulfillment of its treaty obligations has also been illustrated outside Africa

[119] See Articles 55 and 56 *id.* See also, Hansungule, M. African Courts and the African Commission on Human and Peoples' Rights. In Bosi, A. and Diescho, J. (2009) *Human Rights in Africa: Legal Perspective on their Protection and Promotion*. Namibia: Macmillan Education, p. 259.

[120] See *Free Legal Assistances Group and Others v. Zaire*, ACHPR/COMM, No.25/89, 47/90, 56/91, 100/93 (1995), and; *International Penn & Others (on behalf of Saro-Wiwa) v. Nigeria*, ACHPR/COMM, 137/94, 139/94, 154/96, 161/97 (1998).

[121] See *Social and Economic Rights Action Center (SERAC) and the Center for Social and Economic Rights (CESR) v. Nigeria*, Communication No. 155/96, ACHPR/COMM/A044/1 (2002).

[122] See Coomans, F. (2003) The Ogoni Case before the African Commission on Human and Peoples' Rights', *International and Comparative Law Quarterly*, 52, pp. 749-760.

[123] See *SERA and CESR v. Nigeria*, at paragraphs 46-47.

[124] *Id.* at paragraph 47.

by the decisions of the European Court of Human Rights in the cases of *K.U. v. Finland*[125] and *I. v. Finland*.[126] In both cases, the Court found the State of Finland liable for not taking adequate measures to fulfill the positive obligations that are attached to the right to a private life under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (1950) due to Finland's failure to timely establish adequate cybercrime and data protection frameworks.

Also, even where an AU Member State has not adopted or ratified the AU Cybersecurity Convention, there are still prospects that such Member State can be held accountable for failing to establish adequate cybersecurity governance frameworks that will ensure the protection of the human rights guaranteed under its national laws, or under Africa's human right treaties. This is because the guarantee of human rights in national laws or international treaties imposes obligations on States to ensure their protection,[127] and also gives rise to citizens' expectation that such rights will be protected by the State. Therefore, the mere fact that an AU Member State has guaranteed human rights in its national laws or as a State party to any of the AU's human right treaties would trigger obligations to protect its citizens from malicious cyber acts that can infringe on those human rights. For example, malicious cyber acts such as hacking and denial of service of attacks can infringe the exercise of several human rights including the right to privacy,[128] the right to receive information and express ideas,[129] the right to freedom of association,[130] and the right to education.[131] As such, there exists a legitimate expectation by citizens that their fundamental human rights will be protected by the State against malicious cyber acts, which can impede the exercise of those rights. Consequently, if an AU Member State that has not signed or ratified the AU Cybersecurity Convention has also failed to establish adequate measures to tackle cybercrimes that can infringe on the exercise of the human rights

[125] Judgment of 2 December 2008, ECHR No. 2872/02.

[126] Judgment of 17 July 2008, ECHR No. 20511/03.

[127] See *Social and Economic Rights Action Center (SERAC) and the Center for Social and Economic Rights v. Nigeria*, at paragraphs 46–47.

[128] See Article 10 *African Charter on the Rights and Welfare of the Child* (1990).

[129] See Article 9 *African Charter on Human and Peoples' Rights* (1982). See Article 17 *African Charter on the Rights and Welfare of the Child* (1990).

[130] See Article 10 *African Charter on Human and Peoples' Rights* (1982). See Article 8 *African Charter on the Rights and Welfare of the Child* (1990).

[131] See Article 17 *African Charter on Human and Peoples' Rights* (1982). See Article 11 *African Charter on the Rights and Welfare of the Child* (1990).

guaranteed under its national laws or under African human right instruments, then such Member State would be failing in its obligation to protect those rights.

5.4 THE POSSIBILITY OF AU SANCTIONS ON NON-COMPLIANT MEMBER STATES

Another significant implication of the AU Cybersecurity Convention with respect to the promotion of cyber stability is that it would enhance the possibility of applying AU sanction mechanisms against Member States that fail to fulfill their obligations under the Convention when it enters into force. Thus, AU Member States are generally bound to comply with the "decisions and policies" of the AU including those made by the AU Executive Council and the AU Assembly of Heads of State and Government. In this respect, Article 23:2 of the Constitutive Act of the AU provides that

> *"Any Member State that fails to comply with the decisions and policies of the Union may be subjected to other sanctions, such as the denial of transport and communications links with other Member States and other measures of a political and economic nature to be determined by the Assembly".*[132]

The AU Cybersecurity Convention clearly constitutes a decision and policy of the AU.[133] As such, once the Convention has entered into force, Article 23:2 of the AU Constitutive Act would provide a legal basis for the AU to administer sanctions against Member States that fail to implement their obligations under the Convention. However, despite the existence of sanction mechanisms within the AU's governance framework, the AU has rarely applied sanctions for the purpose of promoting the national implementation of its legal instruments, or for the purpose of facilitating the transposition of such instruments in order to promote legal harmonization amongst Member States.[134] Although, the AU has imposed sanctions on Member States in cases

[132] See Article 23:2 *Constitutive Act of the African Union*, 11 July 2000 (hereafter, Constitutive Act of the AU).

[133] See African Union. *The African Union Convention on Cyber Security and Personal Data Protection,* 27 June, 2014 (EX.CL/846 (XXV).

[134] See Magliveras, K. D. (2011) The Sanctioning System of the African Union: Part Success, Part Failure?, *The African Union: The First Ten Years*. 11–13 October 2011. Addis Ababa: Institute of Security Studies, pp. 1–33.

of the unconstitutional overthrow of governments[135] and non-payment of membership contributions,[136] however, it appears that sanctions have not been imposed on the authority of Article 23:2 of the AU Constitutive Act.[137]

6. CHALLENGES IMPEDING THE CONVENTION AS A FRAMEWORK FOR REGIONAL CYBER STABILITY

There are several challenges that impede the application of the obligations under the AU Cybersecurity Convention for the purpose of promoting regional cyber stability. These challenges include the absence of capacity in terms of expert personnel that will facilitate the development and implementation of national policy and regulatory frameworks for cybersecurity governance, and the administration of national cybersecurity agencies and CERTs.[138] There are also peculiar challenges arising from the absence of requisite institutional capacities in terms of cybersecurity governance and cybercrime law enforcement. For example, law enforcement authorities in many African States still lack capacities to detect, investigate and prosecute cybercrime.[139] Although there have been various initiatives to build capacities in law enforcement authorities in some States, it however, appears that such initiatives to a large extent have not yet achieved the intended results. Weak institutional capacity is reflected in terms of lack of up to date technological tools to enhance law enforcement and lack of awareness amongst law enforcement officials.[140] Another indicator of weak institutional capacities is the absence of functional national CERTs and national cybersecurity agencies and to coordinate responses to cybersecurity threats in most African States. [141]

The challenge of weak institutional capacities can also be traced to the poor funding of cybersecurity governance initiatives.[142] Poor funding

---

[135] See Mkhize, S. (2014) *Assessing the Efficacy of the AU Sanctions Policies with Regard to Unconstitutional Changes in Government: The Examples of Guinea and Madagascar*. M.A. University of South Africa, pp. 67–118.

[136] See Magliveras K. D. (2011), *id.* pp. 1–33.

[137] *Id.* pp. 8–9.

[138] See African Union and Symantec Corporation (2006) *Cyber Crime & Cyber Security Trends in Africa.* United States: Symantec Corporation, pp. 60, 61, 63, 66, 70, and 83.

[139] *Id.* pp. 70, 83, 134.

[140] See n. 138, p. 10.

[141] See Solutions Consulting (2018) *West Africa Cybersecurity Indexing and Readiness Assessment*. United States: Solutions Consulting, p. 37.

[142] See African Union and Symantec Corporation (2016) *Cyber Crime & Cyber Security Trends in Africa.* United States: Symantec Corporation, pp. 70, 76, 88, 89, and 92. See Serianu Limited (2016) *Africa Cybersecurity Report 2016*. Kenya: Serianu Limited, p. 46.

of cybersecurity initiatives has been responsible for the absence of expert personnel that would facilitate the development and implementation of national policy and regulatory frameworks for cybersecurity governance and also assist law enforcement authorities in the prevention, investigation or prosecution of cybercrime. In addition, poor funding has limited research and development initiatives that would promote regional cybersecurity governance within the AU. To some extent, the poor funding of cybersecurity initiatives by African governments has been caused by the fact that cybersecurity is not really considered as a national security priority in many African States. This is also not unconnected with the fact many African States face physical national security challenges such as terrorism which policy makers usually consider more pervasive than cybercrime and other cybersecurity challenges.[143]

Another major challenge that has hindered the application of the Convention's obligations as a framework for promoting regional cyber stability is the slow pace that has characterized both the signing and ratification of the Convention by Member States, and the development of national policy and regulatory frameworks for cybersecurity governance in many Member States. To some extent, the challenge of slow responses appears to characterize the development of ICT regulatory initiatives in Africa.[144] The slow pace of responses can be traced to factors including lack of awareness amongst policy makers and legislators in Member States,[145] which may have resulted from factors such as the lack of a broad consultation of key stakeholders that drive policy and legislative processes in Member States during the development of the Convention.[146] This is also compounded by lack of capacity in terms of expert personnel to drive

[143] See Shuaibu, M. and Bernsah, L.D. (2016) An Analysis of the Macroeconomic Impact of Insecurity on Nigeria: A Dynamic Modeling Approach. *Journal of Social and Management Sciences*, 2 (1), pp. 3, 4, 6. See Ploch, L. (2010) Countering Terrorism in East Africa: The U.S. Response. *Congressional Research Service*, R41473, p. 19. See Vanguard (2017) *Federal Government Committing Significant Share of 2017 Budget to North-East – Onyeama*. [online] Vanguard. Available from: https://www.vanguardngr.com/2017/02/fgcommittingsignificant-share-2017-budget-northeast-onyeama/ [Accessed 6 June 2018].

[144] See UNTCAD (2012) *Harmonizing Cyberlaw and Regulations: The Experience of the East African Community*. New York/Geneva: UNCTAD, pp. 8–9.

[145] See Seck, M. (2014) Tackling the Challenges of Cybersecurity in Africa. *United Nations Economic Commission for Africa Policy Brief*, NTIS/002/2014, p. 4. [online] Available from: https:///www.uneca.org/sites/default/files/PublicationFiles/ntis_policy_brief_1.pdf [Accessed 6 June 2018]. See Serianu Limited (2016) *Africa Cybersecurity Report 2016*. Kenya: Serianu Limited, pp. 21–22. See Links F. (2018) Tackling Cyber Security/Crime in Namibia – Calling for a Human Rights Respecting Framework. *Democracy Report – Special Briefing Report*, 20, p. 4.

the development of national cybersecurity governance frameworks[147] which then results in much reliance on technical assistance from international organizations[148] and their consultants.[149] In practice, however, a country's request for such technical assistance from an international organization may not be timely, which further contributes in slowing down the pace of developing national policy and regulatory frameworks for cybersecurity governance in Member States that request assistance. National budget constraints also impede the timely development of national cybersecurity policy and regulatory frameworks in many Member States who are challenged by other development concerns which are considered priority areas that require increased government funding such as curbing the spread of HIV/AIDS, tackling widespread poverty, and promoting the sustainable exploitation of natural resources.[150]

The slow pace of responses can further be traced to the absence of a dedicated and effective regional institutional governance mechanism that would promote the ratification of the Convention by Member States and also monitor and facilitate the development of national cybersecurity governance frameworks. This state of affairs appears to be resulting in a poor regional coordination and harmonization of cybersecurity frameworks, while also limiting prospects for regional cybersecurity cooperation and the dissemination of best practices. In addition, the large size of the AU with its 55 Member States and their diverse national legal traditions, and how they receive and implement international treaties is also a major challenge to the effective application of the Convention

---

[146] See Open Forum to Discuss the Proposed Legal Framework for Cybersecurity in Africa. (26 July 2013) [online] Available from: http://daucc.wordpress.com/2013/07/26/event-panel-discussion-on-the-draft-african-union-cyber-security-convention/#comment-4 [Accessed 6 June 2018].

[147] See Bertelsmann-Scott, T. (2013) Regional Cooperation in the Telecommunications Sector via CRASA. *PERISA Series*, p. 3.

[148] A study by the United Nations Office on Drugs and Crime (UNODC) indicates that all African States that responded to its questionnaire, requested technical assistance to build the capacities of law enforcement, prosecution and court authorities to prevent and combat cybercrime. See UNODC (2013) Comprehensive Study on Cybercrime. New York: United Nations, p. 178.

[149] See Calandro, E. S. *Regionalism and the Development of the Information Society: Policy Considerations from SADC*, p. 10. [online]. Available from http://www.cprsouth.org/wp-content/uploads/2015/08/CPRsouth2015_PP115FINAL_vReviewed.pdf [Accessed 6 June 2018].

[150] See Orji, U. J. (2018) *International Telecommunications Law and Policy*. United Kingdom: Cambridge Scholars Publishing, p. 369. See also, African Union and Symantec Corporation (2016) *Cyber Crime & Cyber Security Trends in Africa*. United States: Symantec Corporation, p. 60.

as a framework for promoting regional cyber stability and harmonizing cybersecurity governance measures in Member States.

7. RECOMMENDATIONS

Article 32 of the AU Cybersecurity Convention provides for the establishment of a monitoring and operational mechanism for the purpose of implementing the Convention. The responsibilities of the Convention's operational mechanism include:

> (a) promoting the adoption and implementation of measures to strengthen cybersecurity in electronic services and combating cybercrime and human right violations in cyberspace; and
> (b) advising African governments on measures to promote cybersecurity and combat cybercrime and human right violations in cyberspace at the national level.[151]

The Convention's regional monitoring mechanism has not yet being formally established. However, the above mandates under Article 32 of the Convention may be broadly interpreted to create a regional network agency that is similar to the European Information Security Agency (ENISA).[152] The ENISA was established in 2004 by the European Commission[153] to promote cyber security and critical information infrastructure protection. The Agency serves as a center of excellence for Member States of the European Union and European institutions on cybersecurity issues. Its responsibilities include providing advice and recommendations on cybersecurity and disseminating information on best practices.[154] Given that the slow pace which has characterized both the signing and ratification of the Convention by Member States and the development of national cybersecurity governance frameworks in many AU Member States can also be traced to the absence of a dedicated and effective regional institutional governance mechanism that would promote the ratification of the Convention by Member States and also monitor

[151] See Article 32 *AU Convention on Cybersecurity and Personal Data Protection*.

[152] See Orji, U. J. (2015) Multilateral Legal Responses to Cybersecurity in Africa: Any Hope for Effective International Cooperation? In: Maybaum, M. et al. (eds.) *Architectures in Cyberspace - 7th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE, p. 116.

[153] See Regulation establishing the European Network and Information Security Agency (EC No 460/2004).

[154] See ENISA (2018) Available from: http://www.enisa.europa.eu/ [Accessed 6 June 2018].

the development of national cybersecurity governance frameworks, it appears imperative for the AU to formally set up the regional monitoring mechanism established under Article 32 of the Convention. This is also necessary in order to improve the regional coordination and harmonization of cybersecurity governance frameworks, while also increasing prospects for regional cybersecurity cooperation and the dissemination of best practices. Such a measure would go a long way towards harnessing the application of the Convention as a framework for promoting regional cyber stability. In addition, it is imperative for African States to take other measures such as: promoting cybersecurity governance as a core regional security priority; improving the funding of cybersecurity capacity building initiatives to enhance the development of a pool of skilled personnel; promoting awareness amongst policy makers and legislators; and, improving funding for national cybersecurity initiatives including the operation of National CERTs/CSIRTS and law enforcement institutions.

8. CONCLUSION

Africa still lacks efficient capacities and resources for cybersecurity governance. This absence of capacities and resources remains a major factor that has contributed to creating an enabling environment for rising cybercrime trends in African States.[155] The adoption of the AU Cybersecurity Convention indicates Africa's awareness of cybersecurity concerns and also signals its interest in promoting cyber stability at least from a regional perspective. However, while there is no doubt that the AU Cybersecurity Convention seeks to promote regional cyber stability, the achievement of this objective is dependent on the timely implementation obligations that arise from the Convention, as well as on the ability of the AU to coordinate and monitor its implementation by Member States. In order to achieve such desired outcomes, the AU and its Member States may have to consider taking timely steps towards addressing the highlighted challenges that impede the application of the Convention as a framework for promoting regional cyber stability.

[155] See Flores, R. et al. (2017) *Cybercrime in West Africa: Poised for an Underground Market*. United States: Trend Micro and INTERPOL, p. 3. See also, Kharouni. L. (2013) *Africa: A New Safe Harbour for Cyber Criminals?* Trend Micro Research Paper. United States: Trend Micro Inc. pp. 1–26.

LIST OF REFERENCES

[1] *African (Banjul) Charter on Human and Peoples' Rights*, 27 June 1981 (OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58).

[2] *African Charter on the Rights and Welfare of the Child*, 29 November 1999 (OAU Doc. CAB/LEG/24.9/49)(1990).

[3] African Union (2008) *Study on the Harmonization of Telecommunication and Information and Communication Technologies Policies and Regulation in Africa: Draft Report*. Addis Ababa: African Union.

[4] African Union. (2017) *African Union in a Nutshell*. [online] Available from: http://www.au.int/en/abut/nutshell [Accessed 6 June 2018].

[5] African Union. (2017) *Member States*. [online] Available from: http://www.au.onlinet/en/member_states/country profiles [Accessed 6 June 2018].

[6] African Union. (2018) *List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection.* [online] Available from: https//au.int/sites/default/files/treaties/29560slafrican_union_convention_on_cybe_security_and_personal_data_protection.pdf [Accessed 6 June 2018].

[7] African Union (AU). Available from: http://www.au.int/en/ [Accessed 6 June 2018].

[8] African Union and Symantec Corporation (2016) *Cyber Crime & Cyber Security Trends in Africa*. United States: Symantec Corporation.

[9] *African Union Convention on Cyber Security and Personal Data Protection*, 27 June 2014 (EX.CL/846 (XXV).

[10] Bertelsmann-Scott, T. (2013) Regional Cooperation in the Telecommunications Sector via CRASA. *PERISA Series*.

[11] Brommelhorster, J. et al. (2004) Critical Infrastructure Protection: Survey of World-wide Activities. *BSI KRITIS*, (4).

[12] Calandro, E.S. Regionalism and the Development of the Information Society: Policy Considerations from SADC. [online] Available from http://www.cprsouth.org/wp-content/uploads/2015/08/CPRsouth2015_PP11FINAL_vReviewed.pdf [Accessed 6 June 2018].

[13] *Constitution of Cape Verde* (1992).

[14] *Constitution of Ghana* (1992).

[15] *Constitution of Liberia* (1986).

[16] *Constitution of Senegal* (2001).

[17] *Constitution of Sierra Leone* (1991).

[18] *Constitution of the Federal Republic of Nigeria* (1999).

[19] *Constitution of the Gambia* (1997).

[20] *Constitution of the Republic of Benin* (1990).

[21] *Constitutive Act of the African Union*, 11 July 2000.

[22] Coomans, F. (2003) The Ogoni Case before the African Commission on Human and Peoples' Rights, *International and Comparative Law Quarterly*, vol. 52.

[23] Council of Europe (1976) *Twentieth Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime*. Strasbourg.

[24] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks against Information Systems and replacing Council Framework Decision 2005/222/JHA, *Official Journal of the European Union.*

[25] Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning Measures for a High Common Level of Security of Network and Information Systems across the Union, *Official Journal of the European Union.*

[26] Dunn, M. (2005) A Comparative Analysis of Cybersecurity Initiatives Worldwide. *World Summit on Information Society (WSIS) Thematic Meeting on Cybersecurity*. Geneva: ITU.

[27] Economic Commission for Africa (2012) *Declaration of Addis Ababa on the Harmonization of Cyber Legislation in Africa*. Addis Ababa: Economic Commission for Africa.

[28] Editorial (1941) The Trail Smelter Arbitral Decision. *American Journal of International Law*.

[29] European Commission (1999) *Towards a New Framework for Electronic Communications Infrastructure and Associated Services.* Brussels: European Commission.

[30] Flores, R. et al. (2017) *Cybercrime in West Africa: Poised for an Underground Market*. United States: Trend Micro and INTERPOL.

[31] *Free Legal Assistances Group and Others v. Zaire*, ACHPR/COMM, No. 25/89, 47/90, 56/91, 100/93 (1995).

[32] Garner, B. A. (ed.) (2004). *The Black's Law Dictionary*. 8th ed., St Paul MN, United States: West Publishing Co.

[33] Gordon, K. and Dion, M. (2008) *Protection of 'Critical Infrastructure' and the Role of Investment Policies Relating to National Security*. Paris: OECD.

[34] Gordon, K. and Dion, M. (2008) *Protection of 'Critical Infrastructure' and the Role of Investment Policies Relating to National Security*. Paris: OECD.

[35] GSMA (2013) *Sub-Saharan Africa Mobile Economy Report 2013.* London: A.T. Kearney.

[36] GSMA (2013) *The Mobile Economy Report 2013*. London: A.T. Kearney.

[37] GSMA (2016) *The Mobile Economy Africa 2016*. London: GSMA.

[38] Hansungule, M. African Courts and the African Commission on Human and Peoples' Rights. In: Bosi, A. and Diescho, J. (2009) *Human Rights in Africa: Legal Perspective on their Protection and Promotion*. Namibia: Macmillan Education.

[39] *I. v. Finland* (2008), Judgment of 17 July 2008 (No. 20511/03, ECHR).

[40] *International Penn & Others (on behalf of Saro-Wiwa) v. Nigeria (*1998), ACHPR/COMM, 137/94, 139/94, 154/96, 161/97 .

[41] ITU (2009) *National Cybersecurity/CIIP Self-Assessment Tool*. Geneva: ITU.

[42] ITU (2018) *Cybersecurity Country Profiles* [online] Available from: https//www.itu/en/ITU -D/Cybersecurity/Documents/Country_Profiles/ [Accessed 6 June 2018].

[43] ITU High Level Experts Group (2008) *ITU Global Cyber-Security Agenda (GCA) High Level Experts Group [HLEG] Global Strategic Report*. Geneva: ITU.

[44] ITU High Level Experts Group [HLEG] (2008) *ITU Global Cyber-Security Agenda (GCA) High Level Experts Group [HLEG] Global Strategic Report*. Geneva: ITU.

[45] *ITU Toolkit for Cybercrime Legislation*. Geneva: ITU.

[46] *K.U. v. Finland* (2008), Judgment of 2 December 2008 (No. 2872/02ECHR).

[47] Kharouni. L. (2013) Africa: A New Safe Harbour for Cyber Criminals? *Trend Micro Research Paper*. United States: Trend Micro Inc.

[48] Links F, (2018) Tackling Cyber Security/Crime in Namibia – Calling for a Human Rights Respecting Framework. *Democracy Report – Special Briefing Report*.

[49] Magliveras, K. D. (2011) The Sanctioning System of the African Union: Part Success, Part Failure?, *The African Union: The First Ten Years*. Addis Ababa: Institute of Security Studies, 11–13 October 2011.

[50] Marco, G. (2009) *Understanding Cybercrime: A Guide for Developing Countries.* Geneva: ITU.

[51] Miniwatts Marketing Group (2017), *Internet Usage Statistics for Africa*. [online] Miniwatts Marketing Group. Available from: http://www.internetworldstats.com/stats1.htm [Accessed 6 June 2018].

[52] Mkhize, S. (2014) *Assessing the Efficacy of the AU Sanctions Policies with Regard to Unconstitutional Changes in Government: The Examples of Guinea and Madagascar.* M.A. University of South Africa.

[53] Oji, E. A. (2011) Application of Customary International Law in Nigerian Courts. *Nigeria Institute of Advanced Legal Studies Law and Development Journal*, vol. 1, no. 1.

[54] *Oliver Tambo Declaration* (2009).

[55] *Open Forum to discuss the proposed legal framework for cybersecurity in Africa*, (26 July 2013) [online] Available from: http://daucc.wordpress.com/2013/07/26/event-panel-discussion-

on-the-draft-african-union-cyber-security-convention/#comment-4
[Accessed 6 June 2018].

[56] Oppong, R. F. (2008) Making Regional Economic Laws Enforceable in National Legal Systems: Constitutional and Judicial Challenges. In: Bosi, A. and Breytenbech, W. et al. (eds.) *Monitoring Regional Integration in Southern Africa Year Book*. Stellenbosch, South Africa: Trade Law Center for Southern Africa.

[57] Orji, U. J. (2012) A Discourse on the Perceived Defects of the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cybersecurity. *Communications Law*: *The Journal of Computer, Media and Telecommunications Law*, vol. 17, no. 4.

[58] Orji, U. J. (2012) *Cybersecurity Law and Regulation*. Nijmegen, Nijmegen: Wolf Legal Publishers.

[59] Orji, U. J. (2014) Examining Missing Governance Mechanisms in the African Union Convention on Cybersecurity and Personal Data Protection. *Computer Law Review International*, vol. 5.

[60] Orji, U. J. (2015) Multilateral Legal Responses to Cybersecurity in Africa: Any Hope for Effective International Cooperation? In: Maybaum, M. et al. (eds.) *Architectures in Cyberspace – 7th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE.

[61] Orji, U. J. (2016) Regionalizing Cybersecurity Governance in Africa: An Assessment of Responses. In: Samuel, C. and Sharma, M. (eds.) *Securing Cyberspace: International and Asian Perspectives.* New Delhi, India: Institute for Defence Studies and Analyses & Pentagon Press.

[62] Orji, U. J. (2018) *International Telecommunications Law and Policy*. United Kingdom: Cambridge Scholars Publishing.

[63] Ploch, L. (2010) Countering Terrorism in East Africa: The U.S. Response. *Congressional Research Service*, R41473.

[64] *Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa*, 11 July 2003.

[65] *Protocol to the African Charter on Human and Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights*, 10 June 1998.

[66] Regulation (EC) establishing the European Network and Information Security Agency (No 460/2004).

[67] Rosewarne, C. and Odunfa, A., (2014) *The 2014 Nigerian Cyber Threat Barometer Report.* South Africa and Nigeria: Wolfpack Information Risk and Digital Jewels.

[68] Rudnick, L. et al. (2015) *Towards Cyber Stability: A User-Centered Tool for Policy Makers*. Geneva: United Nations Institute for Disarmament Research.

[69] Schjolberg, S. (2008) *The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva* (2008). [online] Available from: http://www.cybercrimelaw.net/documents/cybercrime_history.pdf [Accessed 6 June 2018].

[70] Seck, M. (2014) Tackling the Challenges of Cybersecurity in Africa. *United Nations Economic Commission for Africa Policy Brief*, NTIS/002/2014.

[71] Sharpe A. (2009) Communications Technologies, Services and Markets. In: Ian Walden (ed.) *Telecommunications Law and Regulation*. 3rd ed. New York: Oxford University Press.

[72] Shuaibu, M. and Bernsah, L.D. (2016) An Analysis of the Macroeconomic Impact of Insecurity on Nigeria: A Dynamic Modeling Approach. *Journal of Social and Management Sciences*, vol. 2, no. 1.

[73] Shuma, T. (2015) Revisiting Legal Harmonization under the Southern African Development Community Treaty: The Need to Amend the Treaty. *Law, Democracy and Development*, vol. 19.

[74] *Social and Economic Rights Action Center (SERAC) and the Center for Social and Economic Rights (CESR) v. Nigeria* (2002), Communication No. 155/96, ACHPR/COMM/A044/1.

[75] Solutions Consulting (2018) *West Africa Cybersecurity Indexing and Readiness Assessment.* Florida, United States: Solutions Consulting.

[76] *The Corfu Channel Case (United Kingdom v. Albania),* (1949), Merits, ICJ Reports.

[77] *The Council of Europe Convention on Cybercrime* (2001), 41 I.L.M. 282.

[78] *The Trail Smelter Arbitration Case (United States of America v. Canada)*, (1938) 3 R.I.A.A.

[79] UNCTAD 2018) *Cybercrime Laws.* [online] Available from: http://www.unctad.org/en/Docs/Cyberlaw/CC.xlsx [Accessed 6 June 2018].

[80] UNECA Press Release, *ICT Ministers call for harmonized policies and cyber legislations on Cybersecurity*. [online] Available from: http://www1.uneca.org/ArticleDetail/tabid/3018/ArticleId/1934/ICT-Ministers-call-for-harmonized-policies-and-cyberlegislationson Cybersecurity.aspx [Accessed 6 June 2018].

[81] United Nations Economic Commission for Africa (UNECA) Press Release, *Draft African Union Convention on Cybersecurity Comes to its Final Stage*. [online] Available from: http://www1.uneca.org/TabId/3018/Default.aspx?ArticleId=1931 [Accessed 6 June 2018].

[82] United Nations Resolution on the Creation of a Global Culture of Cybersecurity, 20 December 2003, (A/RES/57/239).

[83] United Nations Resolution on the Creation of a Global Culture of Cybersecurity, 21 December 2009 (A/RES/64/211).

[84] United Nations Resolution on the Creation of a Global Culture of Cybersecurity, 23 December 2003 (A/RES/58/199).

[85] United States President's Commission on Critical Infrastructure Protection (PCCIP). (1997) *Critical Foundations: Protecting America's Infrastructure*. Washington DC: PCCIP, Appendix B, Glossary B-2.

[86] UNODC (2013) *Comprehensive Study on Cybercrime*. New York: United Nations.

[87] UNTCAD (2012) *Harmonizing Cyberlaw and Regulations: The Experience of the East African Community*. New York/Geneva: UNCTAD.

[88] Van Zyl, G. (2014) Adoption of 'flawed' AU Cybersecurity Convention Postponed. *IT Web Africa*, 21 January. [online] Available from: http://www.itwebafrica.com/ict-and-governance/523-africa/232273-adoption-of-flawed-au-cybersecurity-convention-postponed [Accessed 6 June 2018].

[89] Vanguard (25 February 2017) *Federal Government Committing Significant Share of 2017 Budget to North-East – Onyeama.* [online] Vanguard. Available from: https://www.vanguardngr.com/2017/02/fg-committing-significant-share-2017-budget-northeast-onyeama/ [Accessed 6 June 2018].

[90] *Vienna Convention on the Law of Treaties*, 23 May 1969.

[91] Walter, J. K. (1974) Comparative Law: A Theoretical Framework. *International and Comparative Law Quarterly*, vol. 23, no. 3.

DOI 10.5817/MUJLT2018-2-2

SEARCHING FOR A REFERENCE: USING AUTOMATED TEXT ANALYSIS TO STUDY JUDICIAL COMPLIANCE[*]

by

KATARÍNA ŠIPULOVÁ[**], HUBERT SMEKAL[***], JOZEF JANOVSKÝ[****]

The concept of judicial compliance has attracted plenty of attention in the last two decades. Yet, despite the growing scholarly interest, important research questions remain largely unresolved. This is partly due to the persistent use of unsystematic research, built on the cherry picking of cases. The content of only a few well-known judgments has been thoroughly examined, and the rest remains largely ignored by the legal scholarship. The aim of this article is to introduce a sketch of a new three-level approach for improving research on judicial compliance in a multi-level arena. We show how the use of automated text analysis in combination with more traditional legal methods might shed more light on the concept of judicial compliance and judicial dialogues. We explain the procedure of the automated collection of data and their coding and also point out the risks of using automated text analysis when studying judicial compliance. The approach is demonstrated on a single case study of the use of European Court of Human Rights rulings by Czech apex courts. This study assesses how often and in what way the domestic courts engage with the European Court of Human Rights case law.

---

[*] The authors would like to express their gratitude to the reviewers and MUJLT editor Marek Pivoda, who immensely helped to improve the quality of the manuscript.

The research leading to this article has received funding from the Czech Science Foundation under Grant Agreement no. 16-09415S, Panel P408 ('Beyond Compliance – Domestic Implementation of International Human Rights Case Law').

[**] katarina.sipulova@law.muni.cz, Senior Researcher, Judicial Studies Institute, Law Faculty, Masaryk University, Czech Republic.

[***] hsmekal@fss.muni.cz, Senior Researcher, Faculty of Social Studies, and Judicial Studies Institute, Law Faculty, Masaryk University, Czech Republic.

[****] janovsky@mail.muni.cz, Law Faculty, Masaryk University, Czech Republic.

KEY WORDS

Automated Text Analysis, Compliance, European Court Of Human Rights, National Courts, References

1. INTRODUCTION

The last two decades have seen a proliferation in various international judicial bodies.[1] The phenomenon does not solely include a numerical increase of judicial bodies, but also an increase in their influence and engagement in both domestic and international politics.[2] This applies especially to the bodies that hold the benefits of compulsory jurisdiction, high levels of independence from national governments, and a big caseload thanks to individual petitions.[3] Yet, these courts usually lack the power to oversee and foster the execution of their own decisions. With law as the dominant regulatory tool in modern states, the judiciary lays the foundations of its power on the possession of legal expertise[4] and on the reputation of learned interpreters of law.

The European Court of Human Rights ("ECtHR") is no exception. The literature generally acknowledges the importance of the ECtHR, calling it the most successful international adjudication and enforcement regime for the protection of human rights.[5] The ECtHR's judgments influence the functioning of all branches of power, with possible significant intrusion into national balance of powers.[6] The Committee of Ministers supervises the implementation of adverse judgments at the national level.[7] Yet,

---

1 On international courts and judicial bodies see Romano, C., Alter, K. and Shany, Y. (2014) Mapping International Adjudicative Bodies, the Issues, and Players. In: Cesare Romano, Karen Alter, and Yuval Shany (eds.) *The Oxford Handbook of International Adjudication*. Oxford: OUP, pp. 4–9.

2 Romano, C. (1999) The Proliferation of International Judicial Bodies: The Pieces of the Puzzle. *New York University Journal of International Law and Politics*, 31 (4), pp. 710.

3 For more on characteristics see Alter K. (2014) *The New Terrain of International Law: Courts, Politics, Rights*. Princeton: Princeton UP; Stone Sweet, A. and Brunell, T. (2013) Trustee Courts and the Judicialization of International Regimes: The Politics of Majoritarian Activism in the European Convention on Human Rights, the European Union, and the World Trade Organization. *Journal of Law and Courts*, (1) 1, pp. 61–88.

4 Compare with the conception of the legal field – Bourdieu, P. (1987) The Force of Law: Toward a Sociology of the Juridical Field. *Hastings Law Journal*, 38 (5), pp. 805–853.

5 Moravcsik, A. (2000) The Origins of Human Rights Regimes: Democratic Delegation in Postwar Europe. *International Organization*, 54 (2), pp. 243; Janis, M. W., Kay, R. S. and Bradley, A. W. (2008) *European Human Rights Law: Text and Materials*. Oxford: Oxford UP, USA, p. lix.

6 Kosař, D. and Lixinski, L. (2015) Domestic Judicial Design by International Human Rights Courts. *American Journal of International Law*, 109 (4), pp. 713–760.

the ECtHR still depends largely on the cooperation of domestic courts, which are vital for the execution of its judgments.

Several noteworthy questions were raised by existing research, e.g. Do domestic courts function as transmission belts for the EctHR?[8] What is the form of judicial compliance? Do domestic courts engage in judicial dialogue with Strasbourg? If so, in what form? Why, or in what instances, do courts refer to the ECtHR? How did the reference (compliance) patterns evolve over time? However straightforward these questions may appear, we still lack clear answers.

The research on interactions between national and international courts has become voluminous, yet considerable gaps remain. While it is widely acknowledged that international courts' case law is reflected by domestic courts, we do not know exactly how or to what extent. Legal papers have typically built on a rather low number of the most important cases and overlooked the big picture of the ordinary, but the most frequent cases. We therefore do not know much about how often the domestic courts use international case law and what its typical use is in daily practice. Recent enormous developments in technology have significantly improved accessibility to the data, the process of data collection, coding and analysis. In our project, we utilize these developments to enrich traditional legal research methods and examine the core research question of whether and how domestic courts comply with ECtHR's case law. Accordingly, this paper aims to introduce a framework for the systemic research on the use of international case law by domestic courts.

Our three-level framework utilizes both manual and automated methods of data collection and coding, as well as quantitative and qualitative methods of analysis. Thus, it does not rely only on a classical, detailed legal analysis of the most important cases nor does it employ only traditional hand coding, but it builds on more cases and also uses automated text analysis. We find this rich mix of methods of data collection, coding and analysis as the most promising way of acquiring knowledge about

---

[7] Although the Committee of Ministers lacks 'hard' execution powers, it can refer a question to the ECtHR on whether a Party has failed to fulfil its obligation to abide by the final judgment of the Court (see Art. 46 para. 4 of the European Convention on Human Rights, as amended by Protocol No. 14).

[8] i.e. courts helping the ECtHR to transmit certain ideas. See Kosař, D. (2016) *Perils of Judicial Self-Government in Transitional Societies.* Cambridge: Cambridge University Press, p. 391; Kosař, D. and Šipulová, K. (2018). The Strasbourg Court Meets Abusive Constitutionalism: Baka v. Hungary and the Rule of Law. *Hague Journal on Rule of Law*, 10, pp. 83–110.

the phenomenon under study.[9] However, based on our experience with carrying out the research project on judicial references between the national and international levels, we warn that the automated methods need careful validation because many false positives and negatives can occur.

This paper describes the advantages of the three-level framework and shows its potential to improve current scholarship in the field of judicial compliance with international human rights case law. The paper focuses on the methodological aspects of the research on the use of international case law by domestic courts, mainly on the problem of how to approach judicial compliance both quantitatively and qualitatively. The paper covers issues of sampling, data collection and text recognition, and coding, while the data analysis is only briefly introduced. Snapshots of the preliminary results of the use of ECtHR case law by Czech apex courts are presented in order to illustrate the potential of our approach; a comprehensive presentation of the results would require a book-long enterprise.[10]

The paper first addresses the use of reference-based research in the study of domestic judicial compliance with international case law (Section 2). Then, we present the fundamentals of our three-level framework, which advances the research on how often, and how, national courts participate in the compliance exercise (Section 3). Section 4 points to the challenges and potential problems that may occur when conducting research based on our three-level framework, while Section 5 presents in detail the methodology of the project, specifically data collection and coding that incorporates automated methods. Application of the framework is demonstrated on the case of the Czech Supreme Administrative Court's references to the ECtHR case law (Section 6). Section 7 concludes.

2. JUDICIAL COMPLIANCE AND REFERENCE-BASED LEGAL RESEARCH IN THE INTERNATIONAL SETTING

This section briefly introduces the field. First, we address the concept of judicial compliance with international human rights law and explain why the research of references is essential for its understanding. Then we

[9] Mixed methods are believed to offset the weaknesses of both quantitative and qualitative research, see Creswell, J. W., and Plano Clark, V. L. (2018) *Designing and Conducting Mixed Methods Research*. 3rd ed. Thousand Oaks, CA: Sage, p. 12.

[10] Such a book will be the final outcome of our whole research project.

demonstrate how this field of research might benefit from the use of mix methods, especially from the inclusion of automated text analysis.

We have already noted above that the increasing importance of the courts, including international courts, is widely acknowledged. Both national and international courts can benefit from their co-existence. Domestic courts may use citations of the international case law to support their own reasoning, while reminding the executive and legislative branches that they themselves agreed to and ratified the international treaty establishing the international court. Vice versa, international courts largely depend on the cooperation of domestic courts, especially those standing at the top of the judicial hierarchy. Apex courts unify domestic jurisprudence and may help with the domestication of international case law by frequently referencing it. Most of the existing research focuses on the relationship between domestic courts and the Court of Justice of the European Union ("CJEU") or the EctHR.[11]

Our research focuses on the use of ECtHR case law by the Czech apex courts – the Constitutional Court, the Supreme Court and the Supreme Administrative Court. We assume that when courts use the existing case law, they then cite it. References to international case law indicate that domestic judges feel the urge to engage with international judgments. A reference does not automatically mean judicial compliance (in the sense of conformity, see *infra*), e.g. in cases when domestic judges expressly oppose an international judgment. However, even such a reference provides an important hint that domestic judges take international case law seriously, because they consider it important to expressly acknowledge their opposition to the direction international case law is taking.

When domestic courts approvingly refer to the international case law, then they significantly contribute to compliance with the case law. Usually, compliance is understood as a state of conformity of practice or policy with legal norms.[12] It has been widely argued that national courts belong among the most important compliance partners of international courts.[13] Frequent references to international case law indicate its domestication by national

[11] See e.g. Anagnostou, D. (2014) *The European Court of Human Rights. Implementing Strasbourg's Judgments on Domestic Policy*. Edinburgh: Edinburgh UP; Alter. K. J. (2010) *Establishing the Supremacy of European Law: The Making of an International Rule of Law in Europe*. Oxford: Oxford UP; Scheeck, L. (2007) Competition, Conflict and Cooperation between European Courts and the Diplomacy of Supranational Judicial Networks, *GARNET Working Paper 2307*. Available from: http://www.ucd.ie/t4cms/06_wish_paper_laurent_scheeck.pdf [Accessed 1 March 2018].

judges and subsequently higher compliance. Thus, references by national courts help in building the legitimacy of international courts and their case law.[14]

Yet the systematic tracing of references has only slowly started making its way to the study of interactions between national and international levels. The automated reference recognition has developed remarkably in legal informatics, but it typically remains confined within the boundaries of one legal system, national or international,[15] and unlike our project does not try to connect the two levels. Moreover, the use of the automated reference recognition has not significantly infiltrated the general legal research.[16] Legal research still relies on traditional methods of analysis and views new trends with suspicion.[17]

We position our paper in the discussion on the use of references to international case law by national courts, rather than in the discussion on automated reference recognition. However, for the latter debate, or for the field of legal informatics, our three-level framework might serve as a manifestation of the use of automated methods in the larger research project. Moreover, it points to the practical difficulties that arise when carrying out such research (see Sections 3, 4 and 5).

---

[12] Kingsbury B. (1998) The Concept of Compliance as a Function of Competing Conceptions of International Law. *Michigan Journal of International Law*, 19 (2), p. 345. However, understanding of the term compliance remains quite divided, see Hillebrecht C. (2017) Compliance: Actors, Context and Causal Processes. In: Wayne Sandholtz and Christopher Whytock (eds.) *Research Handbook on the Politics of International Law*. Cheltenham: Edward Elgar, pp. 27–54.

[13] Nollkaemper, A. (2012) The Role of National Courts in Inducing Compliance with International and European Law – A Comparison. In: Marise Cremona (ed.) *Compliance and the enforcement of EU law*. Oxford: Oxford UP; Gerards J. and Fleuren J. (eds., 2014) *Implementation of the European Convention on Human Rights and of the Judgments of the ECtHR in National Case-Law: A Comparative Analysis*. Antwerp: Intersentia; Roberts A. (2011) Comparative International Law? The Role of National Courts in Creating and Enforcing International Law. *The International and Comparative Law Quarterly*, 60 (1), pp. 57–92.

[14] Wind, M. (2016) Do Scandinavians Care about International Law? A Study of Scandinavian Judges' Citation Practice to International Law and Courts. *Nordic Journal of International Law*, 85 (4), p. 283.

[15] See e.g. Harašta, J. and Šavelka, J. (2017) Toward Linking Heterogenous References in Czech Court Decisions to Content. In: Adam Wyner and Giovanni Casini (eds.) *Legal Knowledge and Information Systems*, pp. 177–182.

[16] Epstein, L., Friedman, B. and Stone, G. R. (2015) Testing the Constitution. *New York University Law Review*, 90 (4), pp. 1001–1002.

[17] Dyevre speculates that this might be a result of legal technical jargon which is not as conducive for automated content analysis, and also raise greater concerns for the process of validation. Dyevre, A. (2015) The Promise and Pitfalls of Automated Text-Scaling Techniques for the Analysis of Judicial Opinions. *SSRN*. Available from: http://dx.doi.org/10.2139/ssrn.2626370 [Accessed 10 February 2018]. For more on the suitability of legal language for applying methods using algorithms, see Hildebrandt, M. (2018) Law as Computation in the Era of Artificial Legal Intelligence: Speaking Law to the Power of Statistics. *University of Toronto Law Journal*, 68 (supplement 1), pp. 12–35.

Systematic research using references in a large number of cases would not have been possible without the use of modern technologies. Courts worldwide produce immense amounts of decisions. It became impossible a long time ago for scholars to fully process such a sheer volume of data (read judgments, analyse them and comment, systematize, etc.). The use of computers can, however, significantly help, at least in some stages of research. Huge advancements in information technology over the last few decades have made a previously unimaginable quantity of data available and ready to be analysed, and processed for practical use.[18]

Researching judicial compliance and references to ECtHR case law requires access to domestic courts' databases, as well as a firm understanding of the wider context in which these references were used. This places high demands on both the understanding of language and the legal background, including the more hidden, shadowy life of decisions embedded in the social and cultural particularities of every society. The use of mixed methods should bring comprehensive understanding to the problem at hand, uncovering both the big picture and also more fine--grained processes. On one hand, solely quantitative research of references does not tell us much about how important the role of the international case law is in domestic judgments, if it is followed, and what long-term consequences it brings. Only legal experts with deep expertise in the functioning of the apex courts can alert the research team when the data show something unexpected (but hidden to a layperson).[19] On the other hand, detailed qualitative legal studies of the most important judgments can paint an overly optimistic picture of the influence of international case law on domestic case law and overlook the (possibly low) extent of the overall use of the international case law.

Joining forces with social science methods brings huge promise for legal scholarship. Automated, computer-driven text analysis promises to reduce the costs of reading enormous collections of decisions so that we are able to explore the thus-far unreachable and unknown territory of courts'

[18] King, G. (2011) Ensuring the Data-Rich Future of the Social Sciences. *Science,* 331 (6018), pp. 719–721.

[19] For example, when a judge who does not have a reputation for being a human rights champion (which is a piece of information known only to the expert legal community) records a very high number of references to ECtHR case law. Only then does one check in more detail and finds that the high numbers are due to copy-pasting a short passage of text including a reference to an ECtHR judgment in decisions rejecting petitions as manifestly unfounded.

decision-making. Applying these methods to case law seems to be especially useful in jurisdictions where apex courts have very weak filtering mechanisms and thus issue many thousands of decisions each year, which makes a complex academic examination close to impossible.

The most immediate inspiration for our work was Wind's article, which used automated techniques to count the frequency of references to ECtHR case law by Scandinavian courts.[20] Such an approach however does not say anything about how ECtHR case law is used (What was the purpose of the reference?) or what its significance is (Would the case be decided differently without the reference?). Nor does it distinguish if a domestic court used the reference in its own reasoning, or if it appeared only in the summary of the proceedings before lower courts or of the arguments of the parties. The next section thus presents an overview of our three-level approach, which also answers these important questions, and shows the benefits of including automated techniques.

3. THREE-LEVEL APPROACH TO THE STUDY OF JUDICIAL COMPLIANCE

As noted above, the cooperation of domestic courts is indispensable for international judicial bodies. International human rights norms come to life with their domestic application. In order to understand the domestic judicial compliance with international case law, we first have to identify the set of domestic decisions which use it. Then we can focus on the extent of the use of the international case law – i.e. the frequency of references to international cases in domestic decisions and its development over time. This basic descriptive statistical exercise is important for a rough mapping of the terrain, but does not tell us much about how the international case law is used by domestic judges. Specifically, we are interested in the significance of international case law (i.e. Is it important for deciding domestic cases?), to what extent domestic judges follow their international peers, how extensively they consider international case law and how carefully they refer to it. We employ a dynamic perspective, which means that we are interested in developments in all these categories over time.

For our research, we developed a more nuanced understanding of compliance and attempted to implement it with a mix of quantitative and

[20] Wind, M. (2016), *op. cit.*

qualitative methods such as descriptive statistics (frequencies and crosstabs) and traditional legal analysis (rich description of cases in context). We argue that judicial compliance might be understood in both a broader and a narrower sense. The narrow understanding of judicial compliance reflects only the implementation of adverse ECtHR judgments against a particular country by domestic courts. In other words, narrow judicial compliance focuses only on how domestic courts implement judgments that found that the country in question violated the Convention.

We are convinced that a broad understanding of judicial compliance is better for the systemic research of international case law's impact on the domestic judicial practice than the narrow one because it oversteps the limitation of compliance focusing solely on adverse judgments against the home country. A broad understanding enables us to include all mutual interactions in the case law of both the domestic and international levels and thus more comprehensively examine domestic judicial compliance with the international case law.

First, the macro-level encompasses all references that domestic apex courts have ever made to ECtHR case law. The macro-level asks how frequently courts refer over time to ECtHR case law. We provide the answer by measuring the annual development in frequency of domestic apex courts' references to ECtHR case law. In other words, we record the number of references (as well as the number of decisions with references) and compare it against the population (i.e. the total number) of all decisions of the respective apex courts in order to have a rough idea how often ECtHR case law is used and how the frequency develops over time.

The automated text analysis allows us to instruct computer programs to detect the use of certain words and phrases in texts. It replaces human hand coding, but still needs some human involvement.[21] While computers can learn clustering, whether supervised by human beings or not, the validation of the results requires precise and often time consuming human involvement.[22] As Grimmer and Steward point out, all automated methods, due to the complexity of the language, and particularly so of legal reasoning, are based on inexact language models. The following sections

[21] Grimmer, J. and Stewart, B. M. (2013) Text as Data: The Promise and Pitfalls of Automatic Content Analysis Methods for Political Texts. *Political Analysis,* 21 (3), pp. 267–297.

[22] Ibid.

therefore introduce our model and validation process in detail (see particularly Section 5).[23]

After the quantitative macro-level analysis of all domestic apex court judgments referring to ECtHR case law, there is only a stratified sample of few hundred judgments that work with a reference ECtHR case law in their reasoning. This sample is more closely examined in order to understand what the typical mode of use of the ECtHR's case law is and what significance it has. Do the domestic courts follow the ECtHR's case law? To what extent do they engage with it (automatically accept, or critically discuss)? Is the ECtHR's case law important for the outcome of the case, or would the case be decided in the same way even in the absence of the reference to ECtHR case law? This meso-level analysis relies on close reading by humans, as coding requires expert understanding of judicial interpretation (see Section 5.3).

Finally, the qualitative micro-level analysis of a few carefully hand--picked cases enables us to focus, based on the knowledge gained from the macro- and meso-level analyses, on both typical and atypical features of referencing ECtHR case law, and to evaluate the more far-reaching consequences of ECtHR case law in domestic judicial practice (see Section 5.4).

Level	Main question	Sampling	Coding	Analysis
Macro	**How much do the apex courts refer to ECtHR case law?** What are the most cited ECtHR cases? Which judges cite ECtHR case law the most?	All cases including references to ECtHR case law in reasoning	Automated with manual validation	Descriptive statistics (frequencies and crosstabs)
Meso	**How do the apex courts use ECtHR case law?** What is its significance for deciding domestic cases? Do domestic judges follow ECtHR case law? How detailed is the engagement of domestic judges with ECtHR case law How carefully do domestic judges cite ECtHR case law?	Stratified sampling based on the macro-level sample	Hand-coding based on the detailed codebook	Descriptive statistics (frequencies and crosstabs)
Micro	**What are the consequences of the use of the ECtHR case law for domestic legal practice?** Significant importance of ECtHR case law for selected fields (e.g. discrimination) Adoption of techniques used by the ECtHR by domestic courts (e.g. proportionality test)	Purposive sampling		Contextually rich legal case studies

Table 1: Three-level Approach to Judicial Compliance[24]

[23] Grimmer, J. and Stewart, B. M. (2013) *op. cit.*, p. 270.

[24] Source: authors.

4. RESEARCH CHALLENGES AND POTENTIAL INACCURACIES

There are several caveats which need to be addressed in relation to research of this complexity. We identified four possible problematic factors that challenge the research aim and the results. These are: 1) reduction of the research scope to the apex courts, 2) reference to ECtHR case law as a relevant indicator of judicial compliance, 3) the problem of silent (indirect) references, and 4) identification of cases in which courts do not refer to ECtHR case law.

First, in our case study, we decided to analyse the case law of apex courts, disregarding the courts of lower instances. Lower courts play a similarly important role in bringing ECtHR case law into practice. Nevertheless, the top courts are typically seen as key actors in judicial compliance. This is especially true in the Czech context, where the Constitutional Court oversees the protection of human rights and other two apex courts are responsible for unifying the case law of domestic courts.

We therefore believe that the apex courts function as transmission belts for international human rights bodies. They transmit the respective information and good practices in two directions: towards lower domestic courts, and towards other state actors and bodies.

Furthermore, in Czechia, similarly to many other countries,[25] obtaining databases of lower courts' decisions is virtually impossible. Apart from the data being heavily protected, lower courts have rarely developed their own online databases. Most typically, lower courts store only written files, which makes any sort of research highly difficult. That being said, it would undoubtedly be interesting for future research to probe at least a sample study into the lower courts' case law and their comprehension of ECtHR case law, particularly so due to the different personal characteristics of judges sitting on the courts (education, profile, academic background), or the material factors influencing the performance of courts (presence of analytical units, assistants to judges, etc.).

Second, some readers might wonder whether references to ECtHR case law are indeed a relevant indicator for assessing the role of apex courts in judicial compliance with ECtHR case law. Merely counting references

[25] Wind, M. (2016), *op. cit.*

to ECtHR case law hardly amounts to measuring the impact and importance the courts assign that case law. Being conscious of the fact that not all references are of equal importance, we tackled this issue by incorporating a qualitative content analysis on the meso-level, looking deeper into how exactly the courts use references, in what instances, what their position in the reasoning is and their influence on the result of the case.

Third, it often happens that once the domestic court delivers a very detailed, well-reasoned judgment referring to ECtHR case law and pioneering a new line of jurisprudence, future similar cases refer only to this domestic pioneering judgment and omit the baseline ECtHR case law that originally inspired the domestic court. We are convinced, however, that the mere decision of a judge to cite or disregard a reference to ECtHR case law has a certain symbolic meaning and value and repercussion for the ECtHR's legitimacy as perceived by domestic judges. The future research might, however, attempt to build on our results and address the "silent references" through a network analysis. It will be helpful to collect and analyse indirect references to these very important domestic pioneer cases that transmitted the ECtHR's case law into the domestic jurisprudence for the very first time.

Lastly, some references remain unattributed. Courts might often comply with the ECtHR's opinions without explicitly referring to its case law, either consciously, when trying to avoid controversies potentially caused by adhering to an opinion of an international body in politically and socially salient cases,[26] or unconsciously, mostly when quoting and referring to a plethora of consistent domestic law. One might argue that without including the cases in which the apex courts should have referred but did not (either intentionally or unintentionally, and either when complying or non-complying with ECtHR case law), our analysis paints only an incomplete picture. Nevertheless, we built our research on the pre--understanding that only direct, explicit references are a valid indicator of the position of domestic courts towards ECtHR case law. The reason for using a reference in a case is to strengthen the persuasive authority of the court's reasoning. In order to add another layer of legitimacy for its

[26] Rytter, J. E. and Wind, M. (2011) In need of juristocracy? The silence of Denmark in the development of European legal norms. *International Journal of Constitutional Law*, 9 (2), pp. 470–504.

claims and findings, judges refer to judgments and decisions of those domestic and international bodies which they consider legitimate and authoritative.[27] References therefore hold a strategic place in judicial reasoning and judges enhance the prestige of other institutions by incorporating references to their case law.[28]

5. DATA COLLECTION AND CODING

Most of the existing studies treat all references as relevant arguments and reasoning sources. Such a pre-understanding fails to capture the real practice of domestic courts. Great many references appear in other parts of judgments than reasoning (especially in the introductory part of a decision summing up the facts of the case and the arguments raised by the parties to proceedings, or in separate opinions). These references do not have the capacity to influence the core dispute underlying the case. When examining judicial compliance, it is vital to filter out those references which do not appear in substantive reasoning. Still, distinguishing the placement of the reference does not tell us much about its impact on the result of the case. To tackle these significant issues, we developed a funnel-like filtering mechanism (Figure 1), which 1) cleaned our dataset of references which did not appear in a court's reasoning, and 2) further categorised references due to their impact on the result of a case (the substance).

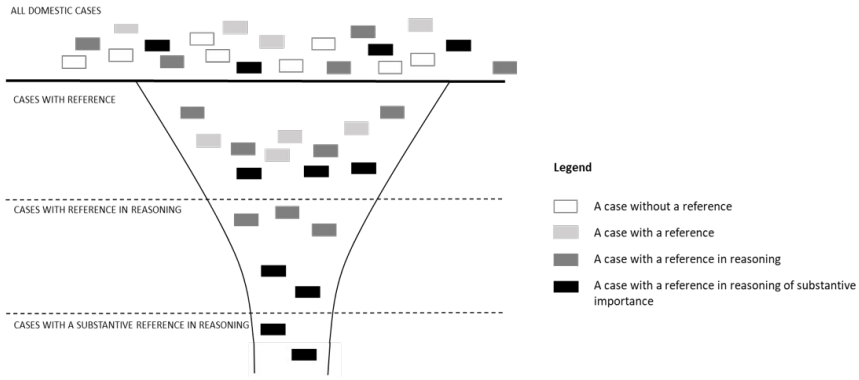


Figure 1: Visualisation of Filtering/Reduction of the Unit of Analysis[29]

[27] Lupu, Y. and Voeten, E. (2012) Precedent in International Courts: A Network Analysis of Case Citations by the European Court of Human Rights. *British Journal of Political Science*, 42 (2), p. 438.

[28] Helfer, L. R. and Slaughter, A. M. (1997) Toward a Theory of Effective Supranational Adjudication. *Yale Law Journal*, 107 (2), pp. 325–326.

[29] Source: authors.

In order to capture these different levels and understandings of judicial compliance, we divided our research into 3 levels: the macro-level, focusing on general patterns present in domestic case law, the meso-level, which digs deeper and inquires into the impact of references on the substance of domestic disputes, and finally, the micro-level, which offers an in-depth qualitative analysis of individual cases. The following section serves not only as an overview of the problems related to automated coding, but also offers a guidebook for future research.

5.1 IN SEARCH OF THE DATA

One of the reasons why there is no comprehensive research on the use of references to international HR bodies' case law by domestic courts dwells, undoubtedly, in the accessibility of the data. In many jurisdictions, access to the case law of lower courts is virtually non-existent; some courts do not have online databases, and if they do, they usually do not cover older decisions. Although these courts do have their own archives, obtaining and processing actual case files is highly costly. In most European countries, the situation is a little less gruesome when it comes to apex courts (as is also the case in Czechia). Yet some difficulties still remain. As previously mentioned, our research project builds on the assumption that apex courts function as transmission belts, promoting the domestic application and compliance with ECtHR case law. A proxy for measuring this compliance is a reference to the ECtHR's case law, i.e. a citation of respective decisions delivered by the ECtHR (for more on the composition of the reference see below). First, we therefore had to collect entire datasets of cases delivered by the top three Czech apex courts: the Constitutional Court ("CC"), the Supreme Court ("SC") and the Supreme Administrative Court ("SAC"). All three databases are publicly accessible; nevertheless, not all of these databases allow a user--friendly download of metadata. We also realized that some courts do not publish some of their decisions online.[30] We had to implement data scraping for some metadata in the cases of the CC and the SAC (subject area, judge rapporteur, etc.). The CC's dataset lacked case file numbers in their identification, so we had to proceed with automatically obtaining the file numbers from the text of the decisions. Lastly, all obtained documents have

[30] Sometimes by omission, sometimes intentionally, e.g. purely technical decisions, some decisions on recognition of judgments, etc.

been converted to UTF8 format, which, compared to .doc, does not have a structure and allows for smooth processing in the programme R. Special and lengthy attention was devoted to optimizing special characters, mostly typical for the Czech language. For the CC, our dataset encompasses 60,403 decisions[31] delivered between 1.1.1993 and 31.12.2015. For the SC we collected 84,374 decisions delivered between 1.1.1993 and 31.12.2015. The case law of the SAC covers a shorter period, from 1.1.2003 to 31.12.2015, as the court was established only in 2002. This dataset covers altogether 39,477 decisions.

After obtaining the domestic datasets, we devoted similar attention to the ECtHR's case law. Similarly, we data scraped the HUDOC database[32] for all decisions and judgments delivered by the Strasbourg Court and its predecessor (European Commission for Human Rights), together with metadata identifying the title of the case (name of the party to the proceedings), date of issuance, ECHR body that issued the decision, subject area, result of the case (violation – non-violation), respective Convention rights, and adverse country. We scraped these data using the Excel macro VBA. This phase resulted in the creation of a list of ECtHR cases which could have potentially appeared as an object of a reference in domestic apex courts cases. We then proceeded with tracing these references on the macro-level.

5.2 MACRO-LEVEL ANALYSIS: GOTTA CATCH 'EM ALL

As previously mentioned, the macro-level of our analysis aims to uncover very broad patterns in which domestic apex courts refer to ECtHR case law.

One of the crucial issues was therefore to establish the population for our research. As it is virtually impossible to identify the cases of non--application (i.e. cases where a domestic court should have or could have referred to the ECtHR case law[33], but did not do so), we eliminated all cases where the courts did not refer to the ECtHR case law and focused only on cases with a reference to the ECtHR case law.

The core puzzle of the macro-level part of the research was how to tease out the information on the presence of a reference in the text

[31] Here, we use the broad term decision, meaning both decisions and judgments.

[32] www.hudoc.echr.coe.int.

[33] We use the general term "ECtHR case law" even if sometimes the courts refer only to the ECtHR (or Strasbourg court) without any further specification. It is obvious that when referring, the case law of the ECtHR is being meant, not the ECtHR as such.

of the judgment automatically. Similarly to the ECtHR, the Czech apex courts also face a crisis in the overflowing number of petitions. Since 1993,[34] the top three courts combined decided over 180 thousand cases. As it would be impossible to manually code such an amount of case law, we decided to use an automated text analysis consisting of a three-step process. First, we defined "a reference to ECtHR case law" and identified its constituents (see below). Second, we created an R algorithm able to recognise a reference according to these constituents. Third, we amended the algorithm in order to semi-automatically recognise which part of the domestic decision the reference was raised in. Each one of these steps has been manually validated.

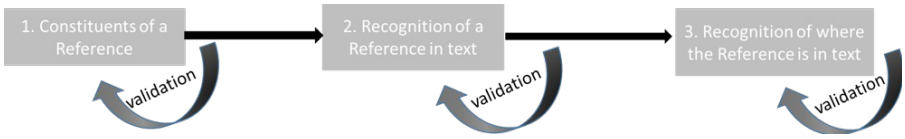


Figure 2: Process of Automated Recognition of References[35]

As illustrated in Figure 2, our first step was to identify constituents of a reference to ECtHR's case law, i.e. indicators that a particular set of words represents a reference. For this purpose, we constructed an R algorithm based on several gazetteers.

Having data scraped the HUDOC database, we created a list of all ECtHR case file numbers and consequently searched for the presence of these file numbers in domestic decisions. If we found the respective file number, the algorithm extracted a small paragraph of text surrounding the reference, which allowed us to validate the results. This first stage left us with many false positives. Typically, shorter ECtHR case file numbers coincided with file numbers of decisions issued by domestic courts, particularly so in the case of the CC. Eventually, we eliminated all false positives with further amendments of the algorithm after several rounds of manual validation. During this first phase, we also validated eventual false negatives (sample of 200 cases), checking whether cases where the algorithm did not report any reference indeed did not encompass one.

Nevertheless, using an ECtHR file number is only one way in which domestic courts refer to its case law and, both from our first validation and

[34] 2002 for the Supreme Administrative Court.

[35] Source: authors.

from practical experience, we knew that Czech apex courts are not particularly consistent in using the file numbers. We therefore amended the constituents of a reference to include either a file number or a name of the party to the proceedings (Table 2). A word of caution should be raised here, however. Some ECtHR judgments are better known by popular titles rather than by the names of the parties to the proceedings (e.g. Skoullos family, no. 55819/00) and some names are translated differently into Czech (e.g. Handölsdalen Sami village, no. 39013/04, in Czech referred to as "Sámská vesnice Handölsdalen"). We therefore created a new list of popular titles and Czech translations and added them to the respective titles in our algorithm. Yet, given the particularly high number of cases and the length of the texts, we had to proceed further, as adding the extensive list of names and popular titles into our algorithm for all domestic cases would lead to extremely lengthy and time-consuming processing. Therefore, we opted to start with a presumption that every time a domestic court refers to a particular ECtHR case, it also mentions the ECtHR itself. In other words, we first searched for all references to the 'ECtHR' and its Czech variations (Figure 3) and then searched for the case titles and names in the vicinity of 1000 words surrounding the general reference to ECtHR. Those results that did not match with any name of a party/title of a case were deleted as void general references.[36]

General reference to ECtHR	ESLP
	Evrop* soud*
Reference to a case	File number
	Name of the party to the proceedings

Table 2: Constituents of a Reference[37]

During the process of validation, we had to amend our algorithm several times in order to capture various acronyms, typos, or incorrect terms. The most tedious part of the analysis was a validation of whether the found reference was not in fact a reference to the CJEU (often simply called the European Court) or if the file number did not match with some other

[36] It is quite common practice with Czech courts to refer to international bodies in very general terms ('as follows also from the case law of the European Court…'). Nevertheless, we did not consider such broad references as adding to the concept of judicial compliance as they did not, in fact, refer to a particular decision of the ECtHR.

[37] Source: authors.

domestic authority file number. Nevertheless, after the second phase, we managed to interactively assign broad references to the ECtHR to individual respective ECtHR file numbers.

During the process of validation, we had to amend our algorithm several times in order to capture various acronyms, typos, or incorrect terms. The most tedious part of the analysis was a validation of whether the found reference was not in fact a reference to the CJEU (often simply called the European Court) or if the file number did not match with some other domestic authority file number. Nevertheless, after the second phase, we managed to interactively assign broad references to the ECtHR to individual respective ECtHR file numbers.

The macro-analysis also allowed us to prepare samples for the meso--level of analysis, which focuses on a more nuanced analysis of how domestic courts use the references in their reasoning (Figure 3).

POPULATION	SAC	SC	CC
All cases 1993[38]–2015	39 477	84 374	60 403
MACRO-level			
cases	1 913	1 309	4 184
references	5 894	7 122	11 977
MESO-level			
cases	1 594	1 080	3 908
references	4 344	4 161	10 399

Figure 3: Populations for our Macro- and Meso-level Analyses[39]

5.3 MESO-LEVEL: ONLY CATCH SOME, BUT CATCH THE ONES THAT COUNT

For the purposes of the meso-level analysis, we went one step further and examined the *mode of application* of the references. As previously mentioned, in the last step of the macro analysis we reduced the original population of references by eliminating references in the narrative parts and the separate opinions of domestic decisions. From the remaining cases, we selected samples of a few hundred judgments for each Czech apex court. We then, with the help of a team of coders, manually coded the *form, the quality* of the reference in these samples, and *its impact* on the dispute

[38] 2003 for the Supreme Administrative Court.

[39] Source: authors.

at the heart of the case. This means that apart from looking at the formal characteristics of references (Does the reference contain a direct quote? Does the reference refer to a particular paragraph of the ECtHR's case? Did the court use a full file number, the name of the party, etc.? Was the reference accompanied by a literature review?), we also reviewed *how* and *why* the apex court referred to ECtHR case law. We asked whether domestic courts used references only to support a reasoning based in domestic provisions, or to substantively change the outcome of the case; whether the apex courts' use of the reference conforms to the ECtHR's reasoning or, on the contrary, whether domestic courts refer to the ECtHR's judgment only to refuse its application. Accordingly, the meso-level analysis proceeded based on a detailed and elaborated codebook (Figure 4).

How the domestic court follows IHRB ruling	1	2	3		
	Following	Distinguishing	Refusing		
Influence of the IHRB ruling on domestic decision	1	2			
	Supportive	Substantive			
How the IHRB ruling is used	1	2	3	4	5
	Invalidation of a domestic legal norm	Direct application	Conforming interpretation of the domestic legal norm	Filling the gap in domestic law	Confirmation of domestic law
Level of the detail of the reference	1	2	3		
	Generic reference	Reference to a specific IHRB ruling	Reference to a specific part of the IHRB ruling		

Figure 4: Meso-level Reference Coding – Clipping from the Codebook[40]

If we were to return to the reduction-funnel (Figure 1), the aim of the meso-level analysis was to get to the narrowest part of the funnel and learn which references do indeed have a substantive impact on domestic cases. The clipping from the codebook (Figure 4) therefore captures the most important categories coded manually for every decision in the meso-level sample:

> A) How is the ECtHR's decision followed in a domestic decision: with the apex court either following (and confirming) the ECtHR's finding, distinguishing that the case at hand and the legal question raised is different from the ECtHR's case (therefore, the ECtHR judgment cannot be applied), or directly refusing to implement the ECtHR's finding in the domestic case at hand.

[40] Source: authors.

B) Influence of the ECtHR's decision on a domestic decision: which can either play a merely supporting role (used as a mere ornament) or can substantively change the result of the case (i.e. the domestic court would decide differently should there be no ECtHR case law).

C) Technique of the use of the reference: here, only in case that the reference is of substantive relevance, we presume that apex courts can use it either to invalidate a domestic legal norm (using the argument of the strength and primacy of international obligations), assign the ECtHR judgment primacy without invalidating any legal norm, interpret the domestic legal provisions in conformity to the referred case, use the reference to the ECtHR decision to fill in the gaps in domestic legislation, or, to confirm the content of the domestic law.

We should, however, raise a few notions regarding the sampling method implemented in our meso-level of analysis. We already noted that in order to code the references manually, we used stratified samples capturing the various importance of decisions within apex courts' case law. The consideration underlying this decision reflected the over-representation of procedural, unpublished decisions in the case law of apex courts that have a lower probability of citing a reference that substantively influences the result of the case. Each sample therefore captures a certain percentage of published and unpublished decisions and judgments, corresponding to the composition of these categories in the respective years (Figure 5).

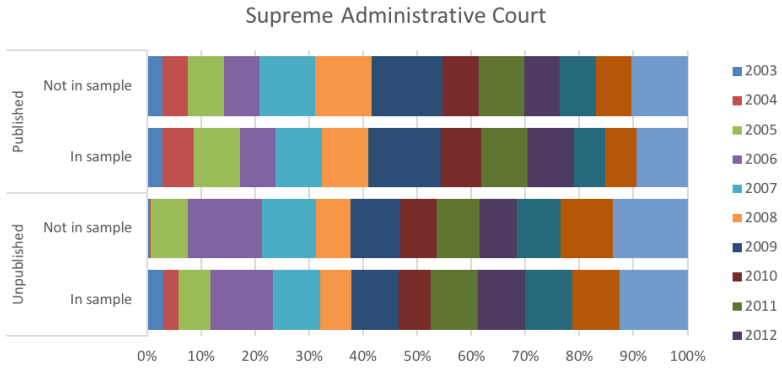


Figure 5: Clipping from the Stratification of Samples[41]

[41] Source: authors.

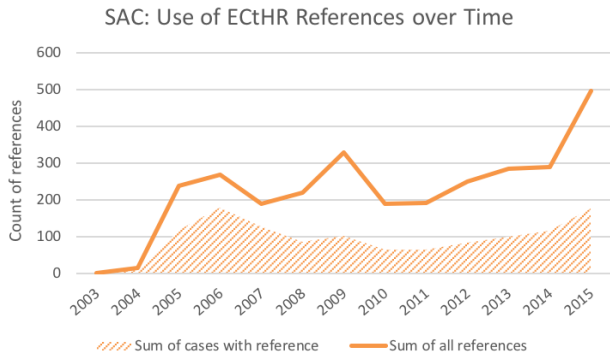
5.4 MICRO-LEVEL ANALYSIS: GOTTA CATCH THE UNIQUE ONES

In the micro-level analysis, we use an in-depth qualitative analysis to address some of the issues uncovered in the previous part. We concentrate on compliance in a narrow sense, looking at the development in selected adverse cases held against Czechia, particularly those in which domestic courts' interpretations contributed to a violation of the Convention rights. Close examination of individual cases should enhance our knowledge of the system, especially in the cases which are exceptional in some sense.

6. PILOT STUDY

In order to make the methodology of our project as comprehensible as possible, we tested it out on a pilot study of the SAC. In this pilot, we were particularly interested in whether the youngest of the Czech top judicial bodies (1) uses the references to ECtHR case law, (2) how often, (3) with what impact, and, (4) how its reputation as a young, liberal, active and pro-international body translates into the use of references.

We first analysed all existing cases issued by the SAC between 1 January 2003 and 31 December 2015. In accordance with theories on judicial dialogues and existing scholarly works on the SAC, we expected the SAC to be a particularly active actor. Figure 6 captures the development of the use of references to the ECtHR case law both by the count of references (orange line) and the count of the SAC's decisions containing a reference (orange area).



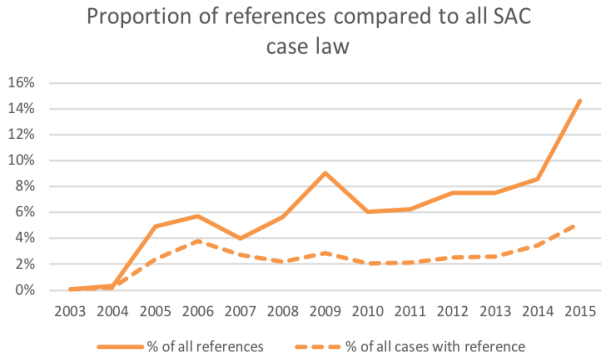


Figure 6: How Often the SAC Refers to the ECtHR's Case Law (Any Placement)?[42]

Perhaps surprisingly, the lower part of Figure 6, does not clearly support this expectation, as, although the Court refers quite significantly, especially so in the last 2 or 3 years, the orange dashed line shows that it does so in fact only in a very limited percentage of all its case law (3% on average, a little over 5% at most).

There are, however, some minor difficulties which should be mentioned before diving into the next level of the funnel-filter. The SAC is in a peculiar position as, generally, the ECHR does not cover the whole area of administrative law. Therefore, although substantively permeating e.g. asylum protection, the right to freedom of assembly, regulation of political parties, or questions of a fair trial, there are certain areas of the SAC's decision-making where the SAC cannot rely on the Convention or on ECtHR case law. This might suggest that further reduction of the population of cases substantially related to the SAC's jurisdiction would be helpful, nevertheless, such a reduction is not feasible. When further analysing the metadata of the ECtHR's decisions referred to most often by the SAC, we found that when it comes to alleged violations of Convention articles, the composition of these decisions is quite diverse, and not necessarily limited to the jurisdiction *ratio materiae* of the SAC.

We then proceeded with the next step of the macro-level analysis and filtered out those references which appeared outside the SAC's own reasoning. In this respect, Figure 7 reports very interesting results. While at the very beginning of the SAC's functioning, most of the references to ECtHR case law occurred in the parts summarizing previous proceedings

[42] Source: authors.

and arguments of the parties (i.e. outside the SAC's own reasoning), this trend changed around 2008 with references in the SAC's own reasoning becoming dominant. Several explanations come to mind here. Either the SAC significantly changed the language of its decisions and of the overall drafting process, or, in the first years of its existence, references to ECtHR decisions were raised significantly more often by parties to proceedings than by the SAC itself. It is true that our analysis confirmed the suggestions of previous scholarship about common flaws in the formal treatment of the ECtHR's case law by domestic courts,[43] especially the excessive anonymization, which not only complicated the recognition of references, but also made their use in reasoning weaker and less persuasive. Either way, the results clearly suggest that work with ECtHR case law has gradually gained prominence in the SAC's own reasoning. This conclusion would be obscured if we relied only on the initial rough count of references.

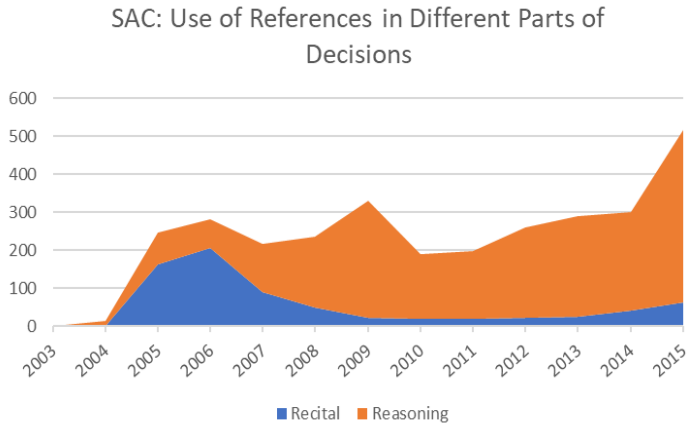


Figure 7: Do the SAC's References to ECtHR Case Law Appear in Recitals or in Reasoning?[44]

Yet, even the count of references cleaned of references outside of the SAC's reasoning does not tell us much about how courts work with the references, why and on what occasions they use them. The meso--analysis of references allows us here to dig deeper and to zero in on those areas where the SAC's case law is significantly influenced by the ECtHR's

[43] Bobek, M. and Kosař, D. (2010) Report on the Czech Republic and Slovakia. In: Giuseppe Martinico and Oreste Pollicino (eds.) *The National Judicial Treatment of the ECHR and EU Laws. A Comparative Constitutional Perspective.* Groningen: Europa Law Publishing, pp. 117–150.

[44] Source: authors.

decisions. We therefore coded cases where the SAC uses references of substantive influence, or, on the contrary, references merely supporting the reasoning and conclusion derived from the national law. Figure 8 (introducing the results of our meso-analysis) indeed shows that on most occasions, the SAC uses the references to the ECtHR's decisions as supportive arguments in its reasoning. Moreover, we also found that the quality of the work with references changes in clear patterns: when the SAC invokes a reference in order to substantially influence its reasoning, the treatment of the ECtHR's case law has a higher quality, offering more precise references and longer explanations.

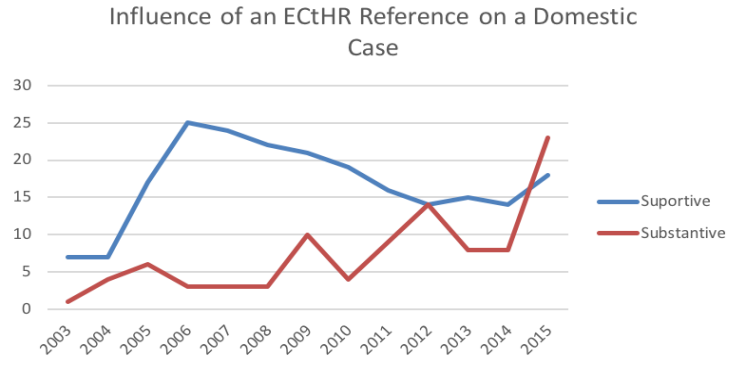


Figure 8: The Importance of References to ECtHR Case Law in SAC's Decisions[45]

A further step in the meso-analysis was then to concentrate on the most important patterns of reference techniques (Figure 9). While supportive references to ECtHR case law are undoubtedly also important for the ex--post control of domestic decision-making, the core interest of judicial compliance lies with cases where the apex court might push forward the compliance with the ECtHR case law despite its discord with the domestic legislation. Figure 9, in this respect, also shows that the SAC quite often uses references to ECtHR case law in order to decide on novel questions and problems unanswered by domestic legal norms (see "Fill in the gaps"), and, on the contrary, almost never – at least openly – refuses to implement the ECtHR's findings.

[45] Source: authors.

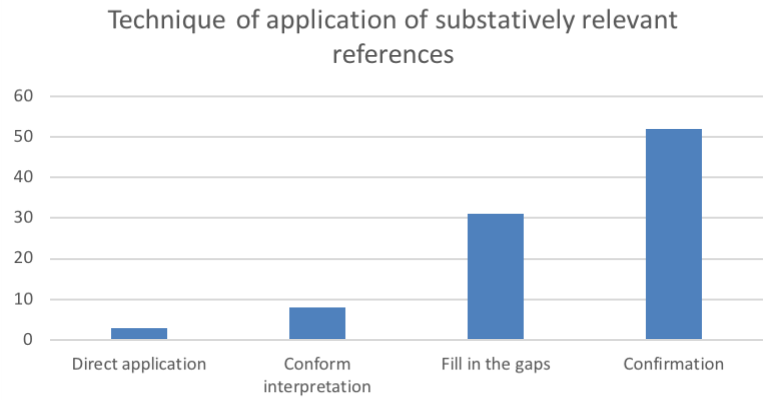


Figure 9: Technique of Application of Substantively Relevant References[46]

The abovementioned conclusions clearly illustrate the deficiencies of the automated text analysis used as a sole method for the research on judicial compliance. Although the automated text analysis is essential for the processing of huge datasets and for getting a rough overview, we need to know more about the content of judgments using references to the ECtHR case law and their context in order to form a proper understanding of judicial compliance. An analysis based purely on an automated text analysis does not provide us with the information of whether the reference on its own adds up to a court's compliance with the ECtHR, or whether its use is purely incidental, or, even more importantly, if a domestic court rebels against the ECtHR and does not follow its case law. A rough count of references cannot provide us with this deeper understanding of compliance, and therefore a combination of various methods, as envisaged by our three-level analysis, is vital.

7. CONCLUSION

Empirical research methods have seen significant progress in the last decades, especially due to the use of computers. Vast volumes of data can be analysed in a user-friendly way with software for both quantitative and qualitative methods. Data accessibility goes hand in hand with developments in analysis methods. Were the data not accessible, even the most sophisticated methods would be useless if they could not be applied to anything. Vice versa, research with highly accessible data would

[46] Source: authors.

be a horrendously time consuming exercise without the assistance of information technology.

Even law, as a rather conservative research field that does not usually stand at the forefront of scientific discoveries, has slowly attracted the increasing attention of researchers using the new tools of inquiry. Legal institutions, especially courts, produce huge quantities of text and machines can help in examining their outputs. While computers can prove extremely useful in acquiring, storing, processing, and analysing data, human supervision and creative input is needed throughout the whole process. Validation of the results returned from an automated text analysis is vital to the success of the whole research endeavour. Although reports on the successes of algorithms in predicting results of legal disputes sound marvellous and computers might even outperform legal experts,[47] they are not free from criticism. They arguably gloss over the question of social and human meaning in legal systems, their use might reinforce existing biases and might exacerbate inequality in access to justice, and thus undermine the legitimacy of the legal system.[48]

The use of machines for text analysis is only slowly permeating our subfield – compliance and international human rights case law – and we perceive automated text analysis to be a helpful tool, but not a panacea. Previous works inspired us, especially Wind's,[49] but at the same time we sought to rectify some of its drawbacks. Particularly, one should not equate a reference to ECtHR case law in the narrative part of a domestic judicial decision (where courts only sum up the proceedings and submissions of the parties) with references to ECtHR case law in a reasoning that includes a court's own judicial consideration of ECtHR case law and its impact on the case under consideration. The use of automated text analysis helped immensely for sorting out the references in the narrative and reasoning parts of the judgments, but at the same time required extensive

[47] Katz et al. report an over 70% success rate in predicting decisions of the US Supreme Court (Katz, D. M., Bommarito II, M. J. and Blackman, J. (2017) A general approach for predicting the behavior of the Supreme Court of the United States. *PloS one*, 12 (4). Available from: https://doi.org/10.1371/journal.pone.0174698 [Accessed 22 January 2018]) and Aletras et al. almost 80% in case of the ECtHR (Aletras, N. et al. (2016) Predicting judicial decisions of the European Court of Human Rights: A natural language processing perspective. *PeerJ Computer Science*, 2. Available from: https://peerj.com/articles/cs-93.pdf [Accessed 22 January 2018]).

[48] Pasquale, F. and Cashwell, G. (2018) Prediction, Persuasion, and the Jurisprudence of Behaviourism. *University of Toronto Law Journal*, 68 (supplement 1), pp. 63–81.

[49] Wind, M. (2016), *op. cit.*

validation due to quite widespread incidence of false positives and false negatives.

The macro-level analysis depended on the computerized techniques, as going through the complete, massive body of domestic apex courts case law is an impossible task. The macro-level analysis can thus provide an overall picture of the main characteristics of the use of the ECtHR's case law by Czech apex courts and it served as a building block for the selection of a sample of cases that was then used in the meso-level analysis. Hand-coding at the meso-level, which required good understanding of the reasoning, was able to capture more finely nuanced usage of ECtHR case law. The micro-level analysis demanded deep immersion into the subtleties of individual cases, which is still better done by human researchers than by machines. Our three-level analysis combining automated and traditional methods to collect and code data with a mix of quantitative and qualitative methods of analysis has the potential to contribute to a better understanding of the use of references to ECtHR case law and might shed more light on the concept of judicial compliance.

Our project on the judicial compliance of domestic apex courts cannot and does not aspire to cover all research questions of the field. However, it does contribute to a more nuanced and more systematic picture of judicial compliance, through discussion of the domestic judicial use of ECtHR case law. We move beyond standard compliance debates and analyse more broadly how ECtHR case law affects domestic jurisprudence and how it permeates the judicial reasoning of national courts. Such a thorough analysis gives us a more accurate picture of how domestic courts actually make use of ECtHR case law and how it affects their approach and their legal reasoning.

Finally, one of the main contributions of our three-level approach is its wide applicability, which stretches far beyond the ECtHR's and the Czech apex courts' case law. Not only it can be used on any given country and any given international human rights regime, but can also include any domestic or international law, case law or even literature (in short – any element used by anybody). The framework is especially useful when the number of cases referring to the element of interest is large, which would otherwise make an in-depth study of all cases in the population unfeasible.

LIST OF REFERENCES

[1] Aletras, N. et al. (2016) Predicting judicial decisions of the European Court of Human Rights: A natural language processing perspective. *PeerJ Computer Science*, 2. Available from: https://peerj.com/articles/cs-93.pdf [Accessed 22 January 2018].

[2] Alter K. (2014) *The New Terrain of International Law: Courts, Politics, Rights*. Princeton: Princeton UP.

[3] Alter. K. J. (2010) *Establishing the Supremacy of European Law: The Making of an International Rule of Law in Europe*. Oxford: Oxford UP.

[4] Anagnostou, D. (2014) *The European Court of Human Rights. Implementing Strasbourg's Judgments on Domestic Policy*. Edinburgh: Edinburgh UP.

[5] Bobek, M. and Kosař, D. (2010) Report on the Czech Republic and Slovakia. In: Giuseppe Martinico and Oreste Pollicino (eds.) *The National Judicial Treatment of the ECHR and EU Laws. A Comparative Constitutional Perspective.* Groningen: Europa Law Publishing, pp. 117–150.

[6] Bourdieu, P. (1987) The Force of Law: Toward a Sociology of the Juridical Field. *Hastings Law Journal*, 38 (5), pp. 814–853.

[7] Creswell, J. W., and Plano Clark, V. L. (2018) *Designing and Conducting Mixed Methods Research*. 3rd ed. Thousand Oaks, CA: Sage.

[8] Dyevre, A. (2015) The Promise and Pitfalls of Automated Text-Scaling Techniques for the Analysis of Judicial Opinions. *SSRN*. Available from: http://dx.doi.org/10.2139/ssrn.2626370 [Accessed 10 February 2018].

[9] Epstein, L., Friedman, B. and Stone, G. R. (2015) Testing the Constitution. *New York University Law Review*, 90 (4), pp. 1001–1040.

[10] Gerards J. and Fleuren J. (eds., 2014) *Implementation of the European Convention on Human Rights and of the Judgments of the ECtHR in National Case-Law: A Comparative Analysis*. Antwerp: Intersentia.

[11] Grimmer, J. and Stewart, B. M. (2013) Text as Data: The Promise and Pitfalls of Automatic Content Analysis Methods for Political Texts. *Political Analysis,* 21 (3), pp. 267–297.

[12] Harašta, J. and Šavelka, J. (2017) Toward Linking Heterogenous References in Czech Court Decisions to Content. In: Adam Wyner and Giovanni Casini (eds.) *Legal Knowledge and Information Systems*, pp. 177–182.

[13] Helfer, L. R. and Slaughter, A. M. (1997) Toward a Theory of Effective Supranational Adjudication. *Yale Law Journal*, 107 (2), pp. 273–391.

[14] Hildebrandt, M. (2018) Law as Computation in the Era of Artificial Legal Intelligence: Speaking Law to the Power of Statistics. *University of Toronto Law Journal*, 68 (supplement 1), pp. 12–35.

[15] Hillebrecht C. (2017) Compliance: Actors, Context and Causal Processes. In: Wayne Sandholtz and Christopher Whytock (eds.) *Research Handbook on the Politics of International Law*. Cheltenham: Edward Elgar, pp. 27–54.

[16] Janis, M. W., Kay, R. S. and Bradley, A. W. (2008) *European Human Rights Law: Text and Materials*. Oxford: Oxford UP, USA.

[17] Katz, D. M., Bommarito II, M. J. and Blackman, J. (2017) A general approach for predicting the behavior of the Supreme Court of the United States. *PloS one*, 12 (4). Available from: https://doi.org/10.1371/journal.pone.0174698 [Accessed 22 January 2018].

[18] King, G. (2011) Ensuring the Data-Rich Future of the Social Sciences. *Science,* 331 (6018), pp. 719–721.

[19] Kingsbury B. (1998) The Concept of Compliance as a Function of Competing Conceptions of International Law. *Michigan Journal of International Law*, 19 (2), pp. 345–372.

[20] Kosař, D. and Lixinski, L. (2015) Domestic Judicial Design by International Human Rights Courts. *American Journal of International Law*, 109 (4), pp. 713–760.

[21] Kosař, D. (2016) *Perils of Judicial Self-Government in Transitional Societies.* Cambridge: Cambridge University Press.

[22] Kosař, D. and Šipulová, K. (2018). The Strasbourg Court Meets Abusive Constitutionalism: Baka v. Hungary and the Rule of Law. *Hague Journal on Rule of Law*, 10, pp. 83–110.

[23] Lupu, Y. and Voeten, E. (2012) Precedent in International Courts: A Network Analysis of Case Citations by the European Court of Human Rights. *British Journal of Political Science*, 42 (2), pp. 413–439.

[25] Moravcsik, A. (2000) The Origins of Human Rights Regimes: Democratic Delegation in Postwar Europe. *International Organization*, 54 (2), pp. 217–252.

[26] Nollkaemper, A. (2012) The Role of National Courts in Inducing Compliance with International and European Law – A Comparison. In: Marise Cremona (ed.) *Compliance and the enforcement of EU law*. Oxford: Oxford UP.

[27] Pasquale, F. and Cashwell, G. (2018) Prediction, Persuasion, and the Jurisprudence of Behaviourism. *University of Toronto Law Journal*, 68 (supplement 1), pp. 63–81.

[28] Roberts A. (2011) Comparative International Law? The Role of National Courts in Creating and Enforcing International Law. *The International and Comparative Law Quarterly*, 60 (1), pp. 57–92.

[29] Romano, C. (1999) The Proliferation of International Judicial Bodies: The Pieces of the Puzzle. *New York University Journal of International Law and Politics*, 31 (4), pp. 709–751.

[30] Romano, C., Alter, K. and Shany, Y. (2014) Mapping International Adjudicative Bodies, the Issues, and Players. In: Cesare Romano, Karen Alter, and Yuval Shany (eds.) *The Oxford Handbook of International Adjudication*. Oxford: OUP, pp. 1–26.

[31] Rytter, J. E. and Wind, M. (2011) In need of juristocracy? The silence of Denmark in the development of European legal norms. *International Journal of Constitutional Law*, 9 (2), pp. 470–504.

[32] Scheeck, L. (2007) Competition, Conflict and Cooperation between European Courts and the Diplomacy of Supranational Judicial Networks, *GARNET Working Paper 2307*. Available from: http://www.ucd.ie/t4cms/06_wish_paper_laurent_scheeck.pdf [Accessed 1 March 2018].

[33] Stone Sweet, A. and Brunell, T. (2013) Trustee Courts and the Judicialization of International Regimes: The Politics of Majoritarian Activism in the European Convention on Human Rights, the European Union, and the World Trade Organization. *Journal of Law and Courts*, (1) 1, pp. 61–88.

[34] Wind, M. (2016) Do Scandinavians Care about International Law? A Study of Scandinavian Judges' Citation Practice to International Law and Courts. *Nordic Journal of International Law*, 85 (4), pp. 281–302.

DOI 10.5817/MUJLT2018-2-3

ONLINE BEHAVIOR RECOGNITION: CAN WE CONSIDER IT BIOMETRIC DATA UNDER GDPR?*

by

ALŽBĚTA KRAUSOVÁ**

Our everyday use of electronic devices and search for various contents online provides valuable insights into our functioning and preferences. Companies usually extract and analyze this data in order to predict our future behavior and to tailor their marketing accordingly. In terms of the General Data Protection Regulation such practice is called profiling and is subject to specific rules. However, the behavior analysis can be used also for unique identification or verification of identity of a person. Therefore, this paper claims that under certain conditions data about online behavior of an individual fall into the category of biometric data within the meaning defined by the GDPR. Moreover, this paper claims that profiling of a person can not only be done upon existing biometric data as biometric profiling but it can also lead to creation of new biometric data by constituting a new biometric template. This claim is based both on legal interpretation of the concepts of biometric data, unique identification, and profiling as well as analysis of existing technologies. This article also explains under which conditions online behavior can be considered biometric data under the GDPR, at which point profiling results in creation of new biometric data and what are the consequences for a controller and data subjects.

KEY WORDS

Behavior Analysis, Behavior-based Tracking, Behavioral Biometrics, Biometric Data, General Data Protection Regulation, Personal Data, Privacy, Profiling, Unique Identification

* This paper was supported by the Czech Science Foundation (GA ČR) under grant No. 16-26910S Biometric Data and Their Specific Legal Protection.

** alzbeta.krausova@ilaw.cas.cz, Head of CICeRo – Center for Innovations and Cyberlaw Research, Institute of State and Law of the Czech Academy of Sciences, Czech Republic (www.cicero.ilaw.cas.cz).

1. INTRODUCTION

According to Eurostat, in 2017 92 % of European citizens aged 16 to 24 years, 81 % of European citizens aged 25 to 54 years, and 57 % of European citizens aged 55 to 64 years use the Internet on a daily basis.[1] Their activity leaves traces about their online behavior. Identity of these individuals can be verified[2] or determined with help of cookies, i.e. pieces of data stored in a device that provides information to servers with which a device is communicating.[3] Determination and verification of users' identities with help of cookies is called explicit tracking and it relies on the cooperation of either users or their web browsers.[4] However, Internet users can be identified also solely based on their online behavior with behavior-based tracking techniques that do not need cookies or any other explicit identifiers.[5] Such identification happens unobtrusively and, in principle, without the knowledge of people whose behavior is being monitored. This technique exploits methods of pattern recognition and applies them either on web surfing behavior, activity of applications installed on a device, or environmental peculiarities.[6] With regard to its purpose, behavior-based tracking partly corresponds to the definition of behavioral biometrics that seeks to

> *"quantify behavioral traits exhibited by users and use resulting feature profiles to successfully verify identity".*[7]

---

1 Eurostat. (2017) *Individuals – frequency of internet use [isoc_ci_ifp_fu]*. [online] European Commission. Available from: https://ec.europa.eu/eurostat/web/products-datasets/-/isoc_ci_ifp_fu [Accessed 29 August 2018].

2 See Recital 25 of ePrivacy directive. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). *Official Journal of the European Union* (2002/L 201/45) 31 July. Available from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML [Accessed 1 November 2017].

3 European Commission. (2016) *Cookies*. [online] European Commission. Available from: http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm [Accessed 22 December 2017].

4 Banse, C., Herrman, D. and Federrath, H. (2012) Tracking Users on the Internet with Behavioral Patterns: Evaluation of its Practical Feasibility. In: Gritzalis, D., Furnell, S. and Theoharidou, M. (eds.) *27th IFIP TC 11 Information Security and Privacy Conference, SEC 2012*, Heraklion, Crete, 4–6 June. Berlin: Springer, p. 235. Available from: https://link.springer.com/chapter/10.1007/978-3-642-30436-1_20 [Accessed 24 November 2017].

5 Op. cit., pp. 235 and 246.

6 Op. cit., p. 242.

7 Yampolskiy, R. V. and Govindaraju, V. (2010) Taxonomy of Behavioral Biometrics. In: Wang, L. and Geng, X. (eds.) *Behavioral Biometrics for Human Identification: Intelligent Applications*. [online] IGI Global, p. 2. Available from: https://www.researchgate.net/publication/254217766_Taxonomy_of_Behavioural_Biometrics [Accessed 15 September 2017].

With regard to the techniques used, behavior-based tracking can also partly correspond to the definition of profiling within the meaning of the EU General Data Protection Regulation[8] (GDPR) as certain aspects relating to a natural person are being analyzed and evaluated in order to establish profiles for this type of tracking.[9] Both biometric data as well as profiling are concepts that have been researched in law substantially due to their potential to seriously infringe privacy of individuals.

From a legal point of view, biometric data is a specific type of personal data that is *"directly linked to an individual"*[10] as it refers to her biological or behavioral characteristics. Biometric data that allow or confirm unique identification of an individual is recognized by the General Data Protection Regulation as a special category of personal data under Art. 9. Due to their potential to significantly increase vulnerability of individuals, processing of special categories of personal data is subject to stricter rules and prohibited in general.

In order to assure the appropriate level of protection of individuals with regard to their personal data, it is legitimate to ask whether profiles set up based on behavior-tracking fulfill the definition of biometric data under the General Data Protection Regulation and, thus, whether service providers who monitor web requests of users and create users' profiles leading to their identification need to comply with specific obligations such as gaining an explicit consent with this practice, appointing a data protection officer, or carrying out a data protection impact assessment. Until now, the literature has dealt only with the question of biometric profiling that aims to extract additional information from existing biometric data and

---

[8] 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) (Text with EEA relevance). *Official Journal of the European Union* (2016/L 119/1) 4 May. Available from: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679 [Accessed 1 November 2017].

[9] Technical papers in the field specifically use the term "profile". See for instance Gu, X., Yang, M., Shi, C., Ling, Z. and Luo, J. (2016) A novel attack to track users based on the behavior patterns. *Concurrency and Computation Practice and Experience*, 29(6). Available from: https://onlinelibrary-wiley-com.ezproxy.techlib.cz/doi/full/10.1002/cpe.3891 [Accessed 24 July 2018]; or Herrmann, D, Banse, C. and Federrath, H. (2013) Behavior-based tracking: Exploiting characteristic patterns in DNS traffic. *Computers & Security*, 39 Part A. Available from: https://www-sciencedirect-com.ezproxy.techlib.cz/science/article/pii/S0167404813000576 [Accessed 24 July 2018].

[10] Article 29 – Data Protection Working Party. (2012) *Opinion 3/2012 on developments in biometric technologies*. 00720/12/EN WP 193. Brussels: Directorate C of the European Commission. Available from: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf [Accessed 20 October 2017].

with *"enriching online profiling data gathered for e-commerce purposes"* with biometric characteristics for instance in order to assess emotional states of a human.[11] However, a possibility of constituting a biometric profile from data gathered for the purpose of profiling based on online behavioral data needs to be discussed as processing this type of data has serious legal consequences for operation of businesses processing these kinds of data. In this regard, the relationship between biometric templates and profiles arising from profiling that can be used for identification of a person also needs to be clarified.

This paper claims that under certain conditions data about online behavior of an individual fall into the category of biometric data within the meaning defined by the GDPR. Moreover, this paper claims that profiling of a person can not only be done upon existing biometric data as biometric profiling but it can also lead to creation of new biometric data by constituting a new biometric template. This claim is based both on legal interpretation of the concepts of biometric data, unique identification, and profiling as well as analysis of existing technologies. This article also explains under which conditions online behavior can be considered biometric data under the GDPR, at which point profiling results in creation of new biometric data and what are the consequences for a controller and data subjects.

2. BIOMETRIC DATA UNDER THE GDPR

GDPR defines biometric data in Art. 4 point 14) as

> *"personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data."*[12]

The term behavioral characteristic is not defined in the GDPR. Behavioral-based biometric data are considered dynamic while still having general characteristics of being universal to all people, unique for each

[11] Kindt, E. (2008) Need for Legal Analysis of Biometric Profiling. In: Hildebrandt, M. and Gutwirth, S. (eds.) *Profiling the European Citizen. Cross-Disciplinary Perspectives*. Dordrecht: Springer.

[12] Op. cit.

person, and permanent.[13] According to Article 29 Data Protection Working Party (A29 WP), an advisory body set up by EU Data Protection Directive,[14] that was replaced by European Data Protection Board but whose opinions stay valid, typical behavioral biometric data

> *"include hand-written signature verification, keystroke analysis, gait analysis, way of walking or moving, patterns indicating some subconscious thinking like telling a lie, etc."*[15]

As this definition refers to patterns of thinking and moving that are then manifested and recorded in an objectively perceivable manner, online behavior of a person perceivable through her specific usage of devices or contents searching patterns should also fall under the definition of behavioral data if it serves as a means for unique identification.

Unique identification is the key term of the definition that determines whether behavioral data will fall in the category of biometrics. The term unique identification is used only at two places in the GDPR – in the very definition of biometric data in Art. 4 point 14) and in the Recital 51. However, the GDPR does not provide any explanation as to the meaning of unique identification.

From a semantic point of view, "unique identification" can refer to recognizing someone as being the one and only person.[16] According to A29 WP, however, this term is relative as it

---

[13] Article 29 – Data Protection Working Party. (2003) *Working document on biometrics*. 12168/02/EN WP 80. Brussels: Directorate E of the European Commission, p. 3. Available from: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp80_en.pdf [Accessed 15 November 2017].

[14] 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. *Official Journal of the European Union* (1995/L 281/38) 23 November. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046 [Accessed 1 November 2017].

[15] Article 29 – Data Protection Working Party. (2012) *Opinion 3/2012 on developments in biometric technologies*. 00720/12/EN WP 193. Brussels: Directorate C of the European Commission, p. 4. Available from: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf [Accessed 20 October 2017].

[16] According to a dictionary, the term "to identify" means *"to recognize or establish as being a particular person or thing"*, while "unique" can be understood as *"existing as the only one or as the sole example; single; solitary in type or characteristics"*. See (1996) *Webster's Encyclopedic Unabridged Dictionary of the English Language*. New York: Random House, pp. 950 and 2074.

> *"depends on different factors including the size of the database and the type of biometrics used"*.[17]

Moreover, it is generally known that no type of biometrics is fully reliable. Biometric accuracy differs with regard to the technology used. In order to achieve higher degree of accuracy, dual biometrics is sometimes recommended.[18] Unimodal biometric systems often suffer from inaccurate data caused for instance by noise that occurred during extraction of features, non-universality of extracted features or due to lack of their individuality.[19] Nevertheless, if no biometric system can guarantee unique identification in all cases, it is then questionable what degree of probability would be sufficient to classify a technology as processing biometric data within the meaning of the GDPR. It is questionable whether reliability should be assessed individually in each case taking into account for instance a number of people enrolled in a system or whether a certain type of error rate should be preferred.[20] As the Recital 15 of the GDPR states that

> *"the protection of natural persons should be technologically neutral and should not depend on the techniques used,"*

various biometric technologies should not be discriminated with regard to their performance. Rather, effects of a particular technology need to be considered.[21] That is to say that the potential level of uniqueness in a biometric system should not *per se* exclude a less reliable system such as one based on behavioral biometrics from the definition of a system

---

[17] Article 29 – Data Protection Working Party. (2003) *Working document on biometrics*. 12168/02/EN WP 80. Brussels: Directorate E of the European Commission, p. 2. Available from: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp80_en.pdf [Accessed 15 November 2017].

[18] See for instance Meena, K. and Malarvizhi, N. (2017) An Efficient Human Identification through MultiModal Biometric System. *Brazilian Archives of Biology and Technology*, 59(2). Available from: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1516-89132016000300403&lng=en&tlng=en [Accessed 24 July 2018]; or earlier Wilson, C. R. (2003) *Biometric Accuracy Standards*. [online] National Institute of Standards and Technology. Available from: https://csrc.nist.gov/CSRC/media/Events/ISPAB-MARCH-2003-MEETING/documents/March2003-Biometric-Accuracy-Standards.pdf [Accessed 20 November 2017].

[19] Meena, K. and Malarvizhi, N. (2017) An Efficient Human Identification through MultiModal Biometric System. *Brazilian Archives of Biology and Technology*, 59(2). Available from: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1516-89132016000300403&lng=en&tlng=en [Accessed 24 July 2018];

[20] In some systems, higher false rejection rate (the ratio of individuals wrongly denied access to a system) may be considered safer than higher false acceptance rate (the ratio of individuals wrongly authorized to access a system).

[21] Koops, B. J. (2006) Should ICT Regulation Be Technology-Neutral? In: Koops, B. J., Lips, M., Prins, C. and Schellekens, M. (eds.) *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*. The Hague: T. M. C. Asser Press.

in which biometric data is processed. In the opposite case, this might lead to circumvention of obligations set out in the GDPR and result in harm to data subjects, i.e. natural persons whose personal data is processed. Determining acceptability of an accuracy level is then a different question that should not influence classification of a system as being a biometric system.[22]

Technological neutrality is crucial also in determining whether mere monitoring users' online behavior, its analysis for creating identification profiles, and consequent application of these profiles qualifies as biometrics. Some may argue that special sensors are needed for a system to be considered as biometric system. For instance, traditional biometric systems use sensors, such as cameras (facial recognition) or microphone (voice recognition), that directly measure some natural property of a human and modify it into an electric signal.[23] In biometric systems monitoring users' online behavior the functions of sensors are performed by the very devices of these users. Data gathered from these devices are then remotely analyzed just as data from sensors that are traditionally considered as biometric sensors. Utilization of a keyboard, mouse or touchpad in fact provides information about behavior that is converted into an electric signal. Identity of users is digitalized[24] such as with any other type of biometrics. Specific templates can be created based on these data as well.

The term biometric data within the meaning of the GDPR then includes any data resulting from electronic processing of data gathered based on physical, physiological or behavioral characteristics of a person regardless of sensors used if such resulting data are used for the purpose of unique identification. With regard to the technological neutrality and importance of effects of a technology, errors in accuracy should not *per se* discriminate a system from being considered as processing biometric data.

---

[22] A29 WP formulated several criteria for assessing acceptability of accuracy: the purpose of processing, false accept rate (probability of incorrect identification), false reject rate (probability of incorrect rejection during identification), population size, and "the ability to detect a live sample". Article 29 – Data Protection Working Party. (2012) *Opinion 3/2012 on developments in biometric technologies*. 00720/12/EN WP 193. Brussels: Directorate C of the European Commission, p. 6. Available from: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf [Accessed 20 October 2017].

[23] Mordini, E., Tzovaras, D. and Ashton, H. (2012) Introduction. In: Emilio, Mordini, Dimitros Tzovaras (eds.) *Second Generation Biometrics: The Ethical, Legal and Social Context*. Dordrecht: Springer, p. 7.

[24] Ghilardi, G. and Keller, F. (2012) Epistemological Foundation of Biometrics. In: Emilio, Mordini, Dimitros Tzovaras (eds.) *Second Generation Biometrics: The Ethical, Legal and Social Context*. Dordrecht: Springer, p. 40.

The resulting data become biometric data at the moment when they enable a system to recognize a person from all other people enrolled in the system.[25]

3. ONLINE BEHAVIOR RECOGNITION AS BEHAVIORAL BIOMETRICS UNDER THE GDPR

Online behavior recognition in the meaning of determining or verifying identity falls under the category of behavioral biometrics defined from the technical point of view. In general, there are five categories of behavioral biometrics and each of them is based on analysis of different features.[26] Online behavior recognition is based on monitoring the activity of a device. This activity can be caused either by a user (active use of applications as well as regular breaks and switching between applications that may result in identification of original patterns of behavior) or by a device itself.

With regard to the very nature of biometrics and the purpose of protecting personality of humans, only templates based on activity originating from a natural person can be considered as biometric data within the meaning of the GDPR. Behavioral patterns are expressions of one's own identity and, therefore, deserve strict legal protection. These patterns can be observed also indirectly from *"observable low-level actions of computer software"* such as call traces, audit logs, program execution traces etc.[27] On the other hand, activity of a device itself does not constitute a link to a personality of their users. Therefore, when assessing whether a certain template falls in a category of biometric data, one needs to analyze what types of data were used for creating this template. Activity of a device could

---

[25] According to A29 WP *"a natural person can be considered as ''identified'' when, within a group of persons, he or she is ''distinguished'' from all other members of the group"*. Article 29 – Data Protection Working Party. (2007) *Opinion 4/2007 on the concept of personal data*. 01248/07/EN WP 136. Brussels: Directorate C of the European Commission, p. 12. Available from: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf [Accessed 20 October 2017].

[26] These are authorship-based biometrics, biometrics based on monitoring human-computer interaction, indirect biometrics based on monitoring low level actions of SW, kinetics based on monitoring motor skills of people, and purely behavioral biometrics based on monitoring a human while performing mentally demanding tasks. For details see Yampolskiy, R. V. and Govindaraju, V. (2010) Taxonomy of Behavioral Biometrics. In: Wang, L. and Geng, X. (eds.) *Behavioral Biometrics for Human Identification: Intelligent Applications*. [online] IGI Global, pp. 1–43. Available from: https://www.researchgate.net/publication/254217766_Taxonomy_of_Behavioural_Biometrics [Accessed 15 September 2017].

[27] Op. cit., pp. 2–3.

constitute a link to a natural person only with help of additional information, including personalization of a device. So called device fingerprint that is based purely on data related to functional specificities unconnected to any activities of a user cannot be considered personal data for obvious reasons.

If both user's activity as well as device's activity would be analyzed together in order to create a device fingerprint, such analysis would result in a combined biometric template. How should one determine which data is biometric and whether a stricter legal regime would apply? The technique of combining more types of input data typically happens in multi-modal biometric systems and is called information fusion.[28] The fusion can be performed at three levels – at the feature extraction level when the system merges data from all sensors, at the matching score level when the system combines values of matching scores from various sensors, and at the decision level when decisions based on matching scores (accept/reject decision) are combined.[29] From the legal point of view, the problem arises only when data from all sensors would be merged (at the feature extraction level) so the resulting identification data would not be based solely on *"the physical, physiological or behavioural characteristics"* as defined in the GDPR. There are already solutions utilizing so called hybrid information fusion that combine a biometric component with a numerical component.[30] In special environments, especially in the online behavior recognition area, systems might start to utilize various types of data, including activity initiated solely by a device. Such identification data based on hybrid information fusion should be, however, considered as biometric data. The GDPR does not impose a requirement that specific technical processing needs to relate solely *"to the physical, physiological or behavioural characteristics"*. It only needs to relate to it and combination with a different kind of information should not prevent the data from being awarded a higher level of protection. However, a different situation would arise if behavioral data of a user would be unknowingly merged from a number

[28] Ross, A. and Jain, A. (2003) Information Fusion in Biometrics. *Pattern Recognition Letters*, 21(13), p. 2117. Available from: https://www.sciencedirect.com/science/article/pii/S0167865503000795?via%3Dihub [Accessed 2 November 2017].

[29] Ibid.

[30] Iovane, G., Bisogni, C., De Maio, L. and M. Nappi (2018) An encryption approach using Information Fusion techniques involving prime numbers and Face Biometrics. *IEEE Transactions on Sustainable Computing*, (99). Available from: http://ieeexplore.ieee.org/document/8259031/ [Accessed 15 January 2018].

of users falsely classified as one user. In that case, such inaccurate data could not be considered as a biometric template even though it could be used to identify for instance members of one family.

Creation of biometric behavioral templates relies on spotting patterns in behavior as well as in analysis of psychological traits of a person. Psychological-based biometric techniques measure individual's *"response to concrete situations or specific tests to conform to a psychological profile"*.[31] Therefore, utilization of such techniques might be also considered as profiling[32] within the meaning of the GDPR. Profiling is defined in its Art. 14 point 4) as

> *"any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements."*

In general, the difference of profiling and biometrics lies in their purpose. Biometrics is used for determining or verifying an identity of a person, while profiling aims at evaluation of a natural person and possibly placing that person in a certain group or a category. Profiling can be even based on biometric data themselves as a special category of personal data. It has been established a number of times that biometric data contains information that can be used for evaluation of certain aspects of a person, such as her health, gender, ethnicity, or emotional state.[33] In such case special obligations apply.[34] However, even the GDPR uses the term "profile" as a means of possible identification of a person.[35] Although the GDPR may not specifically refer to "profiling", this illustrates the technical interconnectedness of profiling and identification.

---

[31] Article 29 – Data Protection Working Party. (2012) *Opinion 3/2012 on developments in biometric technologies*. 00720/12/EN WP 193. Brussels: Directorate C of the European Commission, p. 4. Available from: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf [Accessed 20 October 2017].

[32] Profiling is based on use of algorithms *"to locate unexpected correlations and patterns"*. See Hildebrandt, M. (2015) *Smart Technologies and the End(s) of Law*. Cheltenham: Edward Elgar Publishing, p. 241.

[33] See for instance Yannopoulos, A., Androniku, A. and Varvarigou T. (2008) Behavioural Biometric Profiling and Ambient Intelligence. In: Mireille Hildebrandt, Serge Gutwirth (eds.) *Profiling the European Citizen: Cross-Disciplinary Perspectives*. [online] Dordrecht: Springer, pp. 89–110. Available from: http://www.springer.com/gp/book/9781402069130 [Accessed 21 August 2017]. Springer; or Kindt, E. (2013) *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis*. Dordrecht: Springer.

The question is whether profiling itself can result in creation of biometric data, i.e. if a specific profile of a person based on her behavior that enables her identification is created, should it be considered as biometric data even if the initial intention of a controller was not to process biometric data?

The answer is yes. Determining an identity of a natural person for instance in cases when abnormal behavior is monitored is based on behavioral modelling which overlaps with the legal definition of profiling in the GDPR. Behavior-based tracking relies heavily on models of behavior. Information about such online behavior of a person relates to her physical, physiological, behavioral, or psychological characteristics as it refers to her state of mind (typically search for specific contents) or her ability and manners in using a device that serves as a sensor. A profile combining such gathered information can be compared to a biometric template created based on multi-modal biometrics. Accuracy of linking behavior to a person can vary. However, research suggests that on datasets of 3,800 users up to 87 % of users can be identified based on their behavior[36] and on datasets of 55 users up to 100 % of users can be identified.[37] Moreover, each session in which behavior of a user is monitored and used for updating a model of her behavior, needs to be considered as biometric features extraction and treated as such with regard to legal obligations defined in the GDPR.

From a legal perspective, it is worth to note that even though the main purpose of profiling is evaluation, the profiling does not need to include inference, i.e. any judgment based on the data.[38] This argument could not be used in order to avoid considering profiling also as constituting biometric

---

[34] See Art. 22 of the GDPR and for details Article 29 – Data Protection Working Party. (2017) *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*. 17/EN WP 251. Brussels: Directorate C of the European Commission. Available from: http://ec.europa.eu/newsroom/document.cfm?doc_id=47742 [Accessed 15 November 2017].

[35] Recital 30 of the GDPR stipulates the following: *"Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them."*

[36] Herrmann, D., Kirchler, M., Lindemann, J. and Kloft, M. (2016) Behavior-based tracking of Internet users with semi-supervised learning. *14th Annual Conference on Privacy, Security and Trust (PST)*, Auckland, New Zealand, 12–14 December. IEEE. Available from: https://ieeexplore-ieee-org.ezproxy.techlib.cz/document/7906992/ [Accessed 24 July 2018].

[37] Gu, X., Yang, M., Feit, J., Ling, Z. and Luo, J. (2015) A Novel Behavior-Based Tracking Attack for User Identification. *Third International Conference on Advanced Cloud and Big Data*, Yangzhou, China, 30 October – 1 November. IEEE. Available from: https://ieeexplore-ieee-org.ezproxy.techlib.cz/document/7435478/ [Accessed 24 July 2018].

data. Even though establishing a biometric template based on behavioral data was not initially on mind of a controller, identified behavior models can later serve for a different purpose which is a possibility presumed by the GDPR in Art. 6 par. 4. Moreover, identification is typically achieved based on evaluation of data through their comparison. Here the profiling represents a case of a function creep when certain technology develops and gains new unforeseen functionalities.

However, the condition for a profile to qualify as biometric data depends on its ability to distinguish a person to whom it relates from a group of people. The profile can be associated with a certain group (in biometric systems there are for instance groups of users with different access rights) but in order to be considered as biometric data, it must be possible to exclude the profile from that group (requirement of unique identification). On the other hand, the exact identity of a person does not need to be determined. The reason is that biometric data can be used also only to *"verify the identity without actually identifying the individual"*.[39]

If a controller creates a profile of a person based on her online behavior which allows her unique identification, then such creation has legal consequences both for controllers as well as data subjects. The most important obligation of controllers relates to respecting principles relating to processing personal data. In order to comply with the GDPR requirements, controllers must continually examine their data and profiles based on the data in order to determine whether they process biometric data or not. The crucial element here is the potential of the data to allow unique identification.[40] However, processing of biometric profiles needs to fulfill requirements for processing special categories of data under Art. 9 of the GDPR only if a controller uses the profile among other to distinguish a particular person from others. Especially in the context of an online environment where exceptions for processing biometric data other than

[38] Article 29 – Data Protection Working Party. (2017) *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*. 17/EN WP 251. Brussels: Directorate C of the European Commission, p. 7. Available from: http://ec.europa.eu/newsroom/document.cfm?doc_id=47742 [Accessed 15 November 2017]).

[39] Article 29 – Data Protection Working Party. (2012) *Opinion 01/2012 on the data protection reform proposals*. 00530/12/EN WP 191. Brussels: Directorate C of the European Commission, p. 10. Available from: http://www.europarl.europa.eu/document/activities/cont/201305/20130508ATT65841/20130508ATT65841EN.pdf [Accessed 15 October 2017].

[40] This can be perceived as parallel to the very definition of personal data as any information relating to an identifiable natural person.

explicit consent, controllers need to make sure to be able to prove that a data subject granted them an explicit consent.[41]

4. CONCLUSION

The paper argues that processing users' profiles based on analysis of their online behavior for the purpose of identifying them falls under the category of biometric data within the meaning of the GDPR. However, this applies on the profiles that are based on activity originating from a natural person, not on the activity of a device itself. Activity of a device could be considered as personal data in case additional information is provided and the activity of a device can be linked to an individual. In case of hybrid information fusion, one needs to distinguish at which level various kinds of data are combined. In case of merging biometric data with other type of data on a sensor level, the resulting data should still be considered as biometric data. At other levels of fusion, biometric data is distinguishable from other types of data.

Behavioral biometrics in the online environment overlaps with so called profiling. Biometric data can be used for profiling to evaluate qualities of a person. However, profiling can also lead to creation of a profile corresponding to a biometric template. This must be taken in account by controllers who at a certain moment need to assess whether they shall comply with a stricter regime of data processing. Distinguishing the purpose of processing will then determine the legal regime and requirements on the processing.

Qualification of behavior-based tracking has consequences for instance for service providers who monitor activity of users online that would be otherwise considered anonymous. If these providers are able to identify a person from a group of people based on her behavior regardless of the fact whether they can contact her in the offline world by other means, they process biometric data and must comply with all requirements set out by the GDPR.

Creation of online behavioral profiles can have serious consequences for the protection of privacy. These profiles could become so called identifiers of general application which would put an end to anonymous and

[41] For details about requirements on explicit consent see Article 29 – Data Protection Working Party. (2017) *Guidelines on Consent under Regulation 2016/679*. 17/EN WP 259. Brussels. Available from: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611232 [Accessed 8 January 2018].

untraceable behavior. This would seriously influence fundamental rights and freedoms of individuals on a large scale. Impacts of such practice shall be analyzed in further research.

LIST OF REFERENCES

[1] (1996) *Webster's Encyclopedic Unabridged Dictionary of the English Language*. New York: Random House.

[2] Article 29 – Data Protection Working Party. (2003) *Working document on biometrics.* 12168/02/EN WP 80. Brussels: Directorate E of the European Commission. Available from: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp80_en.pdf [Accessed 15 November 2017].

[3] Article 29 – Data Protection Working Party. (2007) *Opinion 4/2007 on the concept of personal data.* 01248/07/EN WP 136. Brussels: Directorate C of the European Commission. Available from: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf [Accessed 20 October 2017].

[4] Article 29 – Data Protection Working Party. (2012) *Opinion 01/2012 on the data protection reform proposals.* 00530/12/EN WP 191. Brussels: Directorate C of the European Commission. Available from: http://www.europarl.europa.eu/document/activities/cont/201305/20130508ATT65841/20130508ATT65841EN.pdf [Accessed 15 October 2017].

[5] Article 29 – Data Protection Working Party. (2012) *Opinion 3/2012 on developments in biometric technologies.* 00720/12/EN WP 193. Brussels: Directorate C of the European Commission. Available from: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf [Accessed 20 October 2017].

[6] Article 29 – Data Protection Working Party. (2017) *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.* 17/EN WP 251. Brussels: Directorate C of the European Commission. Available from: http://ec.europa.eu/newsroom/document.cfm?doc_id=47742 [Accessed 15 November 2017].

[7] Article 29 – Data Protection Working Party. (2017) *Guidelines on Consent under Regulation 2016/679. 17*/EN WP 259. Brussels. Available from: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611232 [Accessed 8 January 2018].

[8] Banse, C., Herrman, D. and Federrath, H. (2012) Tracking Users on the Internet with Behavioral Patterns: Evaluation of its Practical Feasibility. In: Gritzalis, D., Furnell, S. and

Theoharidou, M. (eds.) *27th IFIP TC 11 Information Security and Privacy Conference*, Heraklion, Crete, 4–6 June. Berlin: Springer, pp. 235–248. Available from: https://link.springer.com/chapter/10.1007/978-3-642-30436-1_20 [Accessed 24 November 2017].

[9] 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. *Official Journal of the European Union* (1995/L 281/38) 23 November. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046 [Accessed 1 November 2017].

[10] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). *Official Journal of the European Union* (2002/L 201/45) 31 July. Available from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML [Accessed 1 November 2017].

[11] European Commission. (2016) *Cookies*. [online] European Commission. Available from: http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm [Accessed 22 December 2017].

[12] Eurostat. (2017) *Individuals – frequency of internet use* [isoc_ci_ifp_fu]. [online] European Commission. Available from: http://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do [Accessed 22 December 2017].

[13] Ghilardi, G. and Keller, F. (2012) Epistemological Foundation of Biometrics. In: Mordini, E., Tzovaras, D. (eds.) *Second Generation Biometrics: The Ethical, Legal and Social Context.* Dordrecht: Springer.

[14] Gu, X., Yang, M., Feit, J., Ling, Z. and Luo, J. (2015) A Novel Behavior-Based Tracking Attack for User Identification. *Third International Conference on Advanced Cloud and Big Data*, Yangzhou, China, 30 October – 1 November. IEEE. Available from: https://ieeexplore-ieee-org.ezproxy.techlib.cz/document/7435478/ [Accessed 24 July 2018].

[15] Gu, X., Yang, M., Shi, C., Ling, Z. and Luo, J. (2016) A novel attack to track users based on the behavior patterns. *Concurrency and Computation Practice and Experience*, 29(6). Available from: https://onlinelibrary-wiley-com.ezproxy.techlib.cz/doi/full/10.1002/cpe.3891 [Accessed 24 July 2018].

[16] Herrmann, D., Banse, C. and Federrath, H. (2013) Behavior-based tracking: Exploiting characteristic patterns in DNS traffic. *Computers & Security*, 39 Part A. Available from:

https://www-sciencedirect-com.ezproxy.techlib.cz/science/article/pii/S0167404813000576 [Accessed 24 July 2018].

[17] Herrmann, D., Kirchler, M., Lindemann, J. and Kloft, M. (2016) Behavior-based tracking of Internet users with semi-supervised learning. *14th Annual Conference on Privacy, Security and Trust (PST)*, Auckland, New Zealand, 12–14 December. IEEE. Available from: https://ieeexplore-ieee-org.ezproxy.techlib.cz/document/7906992/ [Accessed 24 July 2018].

[18] Hildebrandt, M. (2015) *Smart Technologies and the End(s) of Law*. Cheltenham: Edward Elgar Publishing.

[19] Iovane, G., Bisogni, C., De Maio, L. and Nappi, M. (2018) An encryption approach using Information Fusion techniques involving prime numbers and Face Biometrics. IEEE *Transactions on Sustainable Computing,* (99). Available from: http://ieeexplore.ieee.org/document/8259031/ [Accessed 15 January 2018].

[20] Kindt, E. (2008) Need for Legal Analysis of Biometric Profiling. In: Hildebrandt, M. And Gutwirth, S. (eds.) *Profiling the European Citizen. Cross-Disciplinary Perspectives*. Dordrecht: Springer.

[21] Kindt, E. (2013) *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis*. Dordrecht: Springer.

[22] Koops, B. J. (2006) Should ICT Regulation Be Technology-Neutral? In: Koops, B. J., Lips, M., Prins, C. and Schellekens, M. (eds.) *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*. The Hague: T. M. C. Asser Press.

[23] Meena, K. and Malarvizhi, N. (2017) An Efficient Human Identification through MultiModal Biometric System. *Brazilian Archives of Biology and Technology*, 59(2). Available from: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1516-89132016000300403&lng=en&tlng=en [Accessed 24 July 2018].

[24] Mordini, E., Tzovaras, D. and Ashton, H. (2012) Introduction. In: Mordini, E. And Tzovaras, D. (eds.) *Second Generation Biometrics: The Ethical, Legal and Social Context*. Dordrecht: Springer.

[25] 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) (Text with EEA relevance). *Official Journal of the European Union* (2016/L 119/1) 4 May. Available from: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679 [Accessed 1 November 2017].

[26] Ross, A. and Jain, A. (2003) Information Fusion in Biometrics. *Pattern Recognition Letters*, 21 (13), pp. 2115–2125. Available from: https://www.sciencedirect.com/science/article/pii/S0167865503000795?via%3Dihub [Accessed 2 November 2017].

[27] Z. Li, S., Anil, K. Jain (eds.) (2009*) Encyclopedia of Biometrics*. [online] Dordrecht: Springer. Available from: https://link.springer.com/referencework/10.1007/978-3-642-27733-7 [Accessed 27 October 2017].

[28] Wilson, C. R. (2003) *Biometric Accuracy Standards.* [online] National Institute of Standards and Technology. Available from: https://csrc.nist.gov/CSRC/media/Events/ISPAB-MARCH-2003-MEETING/documents/March2003-Biometric-Accuracy-Standards.pdf [Accessed 20 November 2017].

[29] Yampolskiy, R. V. and Govindaraju, V. (2010) Taxonomy of Behavioral Biometrics. In: Wang, L. andGeng, X. (eds.*) Behavioral Biometrics for Human Identification: Intelligent Applications*. [online] IGI Global, pp. 1–43. Available from: https://www.researchgate.net/publication/254217766_Taxonomy_of_Behavioural_Biometrics [Accessed 15 September 2017].

[30] Yannopoulos, A., Androniku, A. and Varvarigou T. (2008) Behavioural Biometric Profiling and Ambient Intelligence. In: Mireille Hildebrandt, Serge Gutwirth (eds.) *Profiling the European Citizen: Cross-Disciplinary Perspectives*. [online] Dordrecht: Springer, pp. 89–110. Available from: http://www.springer.com/gp/book/9781402069130 [Accessed 21 August 2017].

DOI 10.5817/MUJLT2018-2-4

QUO VADIS OPEN DATA?

by

JOZEF ANDRAŠKO[*], MATÚŠ MESARČÍK[**]

New technologies have irreversibly changed the nature of the traditional way of exercising the right to free access to information. In the current information society, the information available to public authorities is not just a tool for controlling the public administration and increasing its transparency. Information has become an asset that individuals and legal entities also seek to use for business purposes. PSI particularly in form of open data create new opportunities for developing and improving the performance of public administration.

In that regard, authors analyze the term open data and its legal framework from the perspective of European Union law, Slovak legal order and Czech legal order. Furthermore, authors focus is on the relation between open data regime, public sector information re-use regime and free access to information regime.

New data protection regime represented by General Data Protection Regulation poses several challenges when it comes to processing of public sector information in form of open data. The article highlights the most important challenges of new regime being compliance with purpose specification, selection of legal ground and other important issues.

KEY WORDS

Data Protection, GDPR, Open Data, PSI Directive, Public Sector Information

[*] jozef.andrasko@flaw.uniba.sk, JUDr. Jozef Andraško, PhD. is an assistant professor at Institute of Information Technology Law and Intellectual Property Law, Faculty of Law, Comenius University in Bratislava, Slovakia.

[**] matus.mesarcik@flaw.uniba.sk, Mgr. Matúš Mesarčík, LL.M. is an internal PhD. candidate at the Department of Administrative and Environmental Law and Institute of Information Technology Law and Intellectual Property Law, Faculty of Law, Comenius University in Bratislava, Slovakia.

1. INTRODUCTION

Public administration faces several challenges in the context of modernization and development of new technologies. Increasing transparency and participation of citizens in public affairs is a legitimate question and issue for many (especially) post-communist countries. Publication of information related to public administration is a strong tool to develop aforementioned issues connected to transparency. Re-use of public sector information and open data are concepts that oscillate in the current discussions.

The first part of the article is devoted to the analysis of public sector information and open data. The emphasis is put on differences and similarities between notions and selected issues. The assessment is conducted in the light of legal orders of Slovak Republic and Czech Republic including the evaluation of related legislation of the European Union.

The second part of the article focuses on processing of open data in the context of data protection. General Data Protection Regulation and national data protection laws "after GDPR" significantly challenge simple facilitation of using previously published personal data. Issues of purpose and legal ground for processing are of the primary interest. The emphasis is put on the legislation and soft law of the European Union and short remarks are made towards related data protection issues in Slovak Republic and Czech Republic.

2. PUBLIC SECTOR INFORMATION AND OPEN DATA – TODAY AND TOMORROW

2.1 OPEN DATA[1]

The open data regime is based on the assumption that public administration authorities produce, collect and process a large amount of public data in different areas like transport, culture, finance, science and research, the environment or various statistics. In the context of the release of open

[1] The term open data is neither defined by generally binding legal act in the Slovak legal order, nor are there defined relations between the term information and data. These two terms are often understood to be synonymous what is not true. Olejár claims that information is the content of the data, and the data is only a form of record of information. in other words, the same information can be recorded in different forms, e.g. information 10 can be recorded as ten, zehn, X. See Olejár, D. et al. (2015) *Manažment informačnej bezpečnosti a základy* PKI. Bratislava, p. 5. More on the issue of difference between data and information see Polčák, R. (2016) Informace a data v právu. *Revue pro právo a technologie 7*, pp. 67–91.

data, it should be borne in mind that public administration has an important position. First of all, public administration creates a large amount of information within fulfilling its tasks. Secondly, a large amount of this information is public and should, therefore, be made available for re--use. Despite the fact that public administration has a large amount of information, it publishes them in a limited amount or in an inappropriate format. Such information can be considered as public data but not open data that can be processed by machine in an automatic way.

By opening public administration data[2] for commercial or non--commercial purposes in the form of different application development, the economic potential of public administration data can be fully exploited.[3] Despite the undeniable economic potential of public administration data, it should be noted that the main purpose of the open data regime is to ensure transparency in public administration and to increase public interest in public administration.[4]

The importance of public administration open data also lies in the fact that experts (researchers, scientists, journalists, web developers, mobile or other software applications) can use the open data repeatedly and create new commercial or non-commercial services that can serve the public.

In accordance with the definition of the Open Knowledge Foundation, open data may be defined as information which is published on the Internet in a way that does not impose any technical or legal obstacles in its use. All users are authorized to further dissemination of this information under the condition that they will indicate the author of the information in question, as well as, other users have the same rights to handle distributed information.[5]

The non-profit organization Sunlight Foundation has defined 10 principles for opening up government information. These principles provide a lens to evaluate the extent to which government data is open and accessible to the public. The principles are completeness, primacy,

---

[2] Term public administration data is a synonym of the term government data.

[3] The estimated market value of open public administration data in the EU is € 55.3 billion for 2016, up to 325 billion by 2025 what is representing about 25,000 new jobs in the field of open data. [online] Available from: http://www.europeandataportal.eu/en/content/creating-value-through-open-data [Accessed 1 March 2018].

[4] For more information about transparency in the context of free access to information see: Munk, R. (2017) *Attempt to increase the transparency*. Bratislava law review, Vol. 1, No. 2, pp. 167–173.

[5] *Open Knowledge Foundation:* The Open Data Manual (2011). [online] Available from: http://opendatahandbook.org/ [Accessed 1 March 2018].

timeliness, ease of physical and electronic access, machine readability, non--discrimination, use of commonly owned standards, licensing, permanence and usage costs.[6]

2.2 TYPES OF OPEN DATA USED IN PUBLIC ADMINISTRATION

International initiatives such as the Open Data Charter[7], signed on 18 June 2013 by G8 leaders and the Open Government Partnership, place emphasis on making public administration information available to strategic datasets that represent a valuable asset for society as a whole.

Based on the abovementioned international initiatives and on the preferences expressed in the open consultation, *Guidelines on recommended standard licenses, datasets and charging for the reuse of documents 2014/C 240/01* defined that users who want to re-use public administration data require the following five thematic dataset categories:

Category	Examples of Datasets
1. Geospatial data	Postcodes, national and local maps (cadastral, topographic, marine, administrative boundaries, etc.)
2. Earth Observation and Environment	Space and *in situ* data (monitoring of weather, land and water quality, energy consumption, emission levels, etc.)
3. Transport Data	Public transport timetables (all modes of transport) at national, regional and local levels, road works, traffic information, etc.
4. Statistics	National, regional and local statistical data with main demographic and economic indicators (GDP, age, health, unemployment, income, education, etc.)
5. Companies	Company and business registers (lists of registered companies, ownership and management data, registration identifiers, balance sheets, etc.)

Table 1: Dataset categories

Other categories may be considered as core or high-value data, depending on circumstances like importance for strategic objectives, market developments, social trends, etc. It is also recommended that the responsible public authorities assess which dataset should be released as a priority.

[6] Exhaustive description of principles. [online] Available from: https://sunlightfoundation.com/policy/documents/ten-open-data-principles/ [Accessed 1 March 2018].

[7] Available from: http://opendatacharter.net/history/# [Accessed 1 March 2018].

2.3 OPEN DATA IN PRACTICE

The best-known example of the use of public administration data in the Slovak Republic is the open-ended project, created by the Fair-Play Alliance and Transparency International Slovakia. The project was initiated when the compulsory publication of all contracts relating to the public funds and state or self-government property was applied in 2011. The main role of the open contracts website is to help citizens to read, search and evaluate the advantageousness of contracts concluded by state and state institutions.[8]

Open government data can also be used to analyze voting in Parliament. One of the examples is the Czech project *KohoVolit.eu*, through which citizens can monitor the work of members of Parliament, their attendance and voting. Users of this app may even contact parliamentarians.[9]

Transport data comprise an important source of public administration open data. After London traffic data was released, more than 500 applications were made available to enable the public to obtain up-to--date information on the use of individual lines to optimize the operation of urban public transport.[10] The availability of information by the British Ministry of Transport allows searching for current restrictions on the roads, such as work on motorways, detours or motorway closures. This information helps drivers make travel time more efficient.[11]

Another example is the use of crime data from Santa Cruz, California, where local police began to record crime data in detail. With the analysis of collected data, the police have been able to predict at what street is in a certain time a high risk of committing various crimes, such as car theft or burglary.[12] The release of the data on criminality also affected the real estate market. Buyers began to buy real estate according to the security of the specific area.

In 2005, the Guardian daily requested data on the success of 400,000 cardiology operations over the last 5 years. Journalists analyzed cardiology

[8] Otvorené zmluvy. [online] Available from: http://otvorenezmluvy.sk [Accessed 20 September 2018].

[9] KohoVolit.eu. [online] Available from: http://kohovolit.eu [Accessed 20 September 2018].

[10] London datastore. [online] Available from: http://data.london.gov.uk/ [Accessed 20 September 2018].

[11] Live map of London Underground. [online] Available from: http://traintimes.org.uk/map/tbe/ [Accessed 20 September 2018].

[12] Crimereports.com. [online] Available from: https://www.crimereports.com/agency/santa cruzpd [Accessed 20 September 2018].

information and published the results of the analysis. As a result of this activity, people began to select hospitals with statistically the highest success rate for their operations, which had an impact on citizens' lives. The mortality fell by 21% or by one-third in specific types of surgery, even though the number of patients has risen.[13]

The most classic example of the use of open data is data on legislation. In the UK, all laws, legal regulations, and legislation changes since 1267 can be found in one place.[14] In the context of the publication of legislation in the Slovak Republic, the portal *Slov-Lex* operated by the Ministry of Justice of the Slovak Republic can be mentioned.[15]

The issue of open data plays a major role at European Union (hereinafter referred to as the "EU") level. The EU Open Data Portal (hereinafter referred to as the "Portal") has been created as a single point of access to the data of the institutions as well as other EU bodies. These data are freely available for re-use, both for non-commercial and commercial purposes. The Portal aims at utilizing the economic potential of information as well as to increase transparency and accountability of institutions and other bodies in the EU.[16]

2.4 EU APPROACH TO OPEN DATA

Discussions on information collected, produced and disseminated by public authorities within their competences extend to the 1970s and 1980s. With the advent of the Internet, information began to be considered as assets of economic value. Efforts to adopt legislation on the re-use of information created by public authorities have been completed by the adoption of Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information (hereinafter referred to as the "PSI Directive").[17]

The PSI Directive was amended by Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending

---

[13] Boseley, S.,UK heart operation death rates fall after data published. *The Guardian.* [online] Available from: https://www.theguardian.com/lifeandstyle/2009/jul/30/heart-surgery-death-rates-fall [Accessed 20 September 2018].

[14] Legislation.gov.uk. [online] Available from: hhttp://www.legislation.gov.uk/ [Accessed 20 September 2018].

[15] Slov-lex.sk. [online] Available from: https://www.slov-lex.sk/domov [Accessed 20 September 2018].

[16] Datasets from: Data.europa.eu. [online] Available from: https://data.europa.eu/euodp/en/data [Accessed 20 September 2018].

Directive 2003/98/EC on the re-use of public sector information Text with EEA relevance (hereinafter referred to as the "PSI Directive 2013") in 2013.[18]

We use terms PSI Directive and PSI Directive 2013 in the text of this article. When using the term PSI Directive 2013 in the text of this article, we point out the new legislation. If we use the term PSI Directive we refer to its consolidated version.

The PSI directive focuses on the economic aspects of re-use of information rather than on the access of citizens to information. It encourages the EU Member States to make as much information available for re-use as possible. The directive in question provides a common legal framework for a European market for government-held data.[19]

The term public sector information (hereinafter referred to as the "PSI") is not directly defined in the PSI Directive. Therefore, terms such as a document, a public sector body and finally the term re-use will help us to clarify the term in question.

Document means any content whatever its medium (written on paper or stored in electronic form or as a sound, visual or audiovisual recording) as well as any part of such content.[20]

The PSI Directive defines public sector body as

> *"state, regional or local authorities, bodies governed by public law and associations formed by one or several such authorities or one or several such bodies governed by public law."*[21]

---

[17] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information. *Official Journal of the European Union* (2003/L345/90). 31 December. [online] Available from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32003L0098 [Accessed 3 March 2018]. More on the issue of PSI Directive and its transposition into particular EU Member States legal orders see Janssen, K. (2011). The influence of the PSI directive on open government data: an overview of recent developments. *Government. Information Quarterly*, 28, pp. 446–456.

[18] Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information Text with EEA relevance. *Official Journal of the European Union* (2013/L1751/1) 27 June. Available from: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32013L0037 [Accessed 3 March 2018].

[19] The European Commission proposed a new PSI Directive on 25 April 2018. Proposal for a directive of the European parliament and of the Council on the re-use of public sector information (recast) COM/2018/234 final – 2018/0111 (COD). 25 April 2018. [online] Available from: https://ec.europa.eu/digital-single-market/en/news/proposal-revision-directive-200398ec-reuse-public-sector-information [Accessed 11 September 2018].

[20] PSI Directive, Article 2 (3).

[21] Ibid., Article 2 (2) (c).

Body governed by public law is defined as any body:

"a) established for the specific purpose of meeting needs in the general interest, not having an industrial or commercial character; and

b) having legal personality; and

c) financed, for the most part by the State, or regional or local authorities, or other bodies governed by public law; or subject to management supervision by those bodies; or having an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional or local authorities or by other bodies governed by public law."[22]

European legislature defined the term re-use as the

"use by persons or legal entities of documents held by public sector bodies, for commercial or non-commercial purposes other than the initial purpose within the public task for which the documents were produced."[23]

In other words, public sector documents are information that a public sector body handles and there is a demand for further processing and use outside the public sector. This process is called re-use of public sector information.

The PSI Directive 2013 has brought a significant shift in the obligation for the EU Member States to make all documents available for re-use unless they are restricted or excluded by national rules and are not subject to other exceptions stated in the PSI Directive. Prior to the adoption of the PSI Directive 2013, EU Member States had the option, not the obligation to make documents available.

In that regard, the PSI Directive applies only to documents that may be made publicly available on the basis of the rules laid down in the legislation of the EU Member States. In this case, it is possible to talk about a general approach to documents. On the other hand, if citizens or businesses have to prove a particular interest in obtaining access to documents, we talk about the privileged approach when access to documents is restricted.

[22] Ibid., Article 2 (2) (c).
[23] Ibid., Article 2 (4).

It is necessary to point out that PSI Directive does not contain provisions on access to information which is the basic precondition for their re-use. The European legislator has left access to information on the legislation of the EU Member States. This may be justified, in particular by the limited legislative powers of the EU in regulating the right of access to information. It is not the intention of the authors to focus on the issue of access to information.

Consequently, in the light of the foregoing considerations, it could be said that the EU legal framework regarding re-use of information held by the public administration is focusing more on PSI rather than on open data. It is necessary to point out that open data can be considered as information that is freely available on the Internet in a structured and machine-readable format and accessible in a manner which does not impose any technical or legal obstacles in its use.[24]

2.5 OPEN DATA IN THE SLOVAK LEGAL ORDER

The issue of open data is partially regulated by *Act No. 211/2000 Coll., On Free Access to Information and on changes and amendments to certain acts* (hereinafter referred to as the "Freedom of Information Act"). In the case of Slovak legal order, the issue of open data is connected with the PSI re-use regime that is regulated by the Freedom of Information Act.[25]

Act No. 340/2015 Coll., amending the Freedom of Information Act created more favorable legal conditions for the re-use of information created by public authorities.[26] In particular, the disclosure of information in electronic form is preferred and where possible and appropriate, as open

[24] More on the issue of open data concept see Verhulst, S., & Young, A. (2016). O*pen Data impact, when demand and supply meet. Key finding of the open data Impact case studies*. Opgehaald van. thegovlab.org. [online] Available from: http://odimpact.org/key-findings.html; Attard, J., Orlandi, F., Scerri, S., & Auer, S. (2015). A systematic review of open government data initiatives. *Government Information Quarterly*, 32 (4), pp. 399–418; Dawes, S., & Helbig, N. (2010). Information strategies for open government: Challenges and prospects for deriving public value from government transparency. *Electronic Government*, 6228, pp. 50–60; Janssen, M., Charalabidis, Y., & Zuiderwijk, A. (2012). Benefits, adoption barriers and myths of open data and open government. Information Systems Management, 29, pp. 258–268; Huijboom, N., & Van den Broek, T. (2011). Open data: an international comparison of strategies. *European Journal of ePractice,* pp. 1–13.

[25] Specific provisions on the re-use of information were transposed into Slovak legal order by Act No. 341/2012 Coll., amending the Freedom of Information Act (with effect from 1 December 2012). By adopting the act in question, a new independent regime of the right to freedom of access to information was created.

[26] The Freedom of Information Act is defining entities that are obliged to provide information. These entities are defined in the act in question as obliged persons. List of obliged persons is stated in Section 2 of the Freedom of Information Act.

data. However, in the context of public administration open data, citizens can gather only some data that are collected by public authorities. In this regard, it should be noted that the main idea of the open data regime is that public authorities publish public data automatically and that they can be easily downloaded via the Internet.

Notwithstanding the above, the term open data is stated in *Regulation of Ministry of Finance of the Slovak Republic No. 55/2014 Coll., On standards for public administration information systems* (hereinafter referred to as the "Regulation on Standards"). According to the Regulation on Standards is standard for the indication of data as open data:

> *"a) provision of data in a dataset[27] in the quality of the provided dataset of at least level 3[28],*
>
> *b) provision of data in the open way of use that is fulfilled if:*
>
> *1. the legal aspects of access to data and use of the data are explicitly settled,*
> *2. it is possible to create legal relations for the use of the data via anonymous remote automated access,*
> *3. access to data is made available to all persons under the same conditions while these conditions being explicitly defined,*
> *4. the data may be used for non-commercial and commercial purposes and may be combined with other data, added, corrected, modified or used from the dataset without the obligation to use other dataset data,*
> *5. the activities under the fourth point are free of charge."[29]*

If the dataset contains at least one open data, it is referred to as a dataset with open data.[30]

The dataset catalog of public administration can be found on the Open Data Portal, created under the Open Government Initiative. The goal

---

[27] Pursuant to Section 2 (r) of the Regulation on Standards is a dataset defined as *"a coherent and self-employed group of related data created and maintained for a particular purpose and stored together under the same scheme."*

[28] Dataset quality levels are divided into 6 levels of quality. Pursuant to Section 51 (1) of the Regulation on Standards is the dataset at level 3 considered as a dataset that is available in the web environment, the content of the dataset is structured to allow automated processing and the dataset is provided in an open format independent of a particular proprietary software.

[29] Regulation on Standards, Section 52.

[30] Ibid., Section 52 (2).

of the Open Data Portal is to make accessible data and metadata in distance and in a machine-readable form using open standards and public licenses.[31]

The Open Data Portal is part of the Central Public Administration Portal of the Slovak Republic (hereinafter referred to as the "Central Portal"). The Central Portal contains 1382 datasets which were published by 63 organizations.[32]

In the Global Open Data Index survey that examines the openness of government data from all countries of the world, the Slovak Republic took the 32nd place.[33] At EU level, the degree of disclosure of open data is examined within the Digital Economy and Society Index (DESI). The Slovak Republic took in 2016 as part of this evaluation in terms of the open data criterion the 21st place among all EU countries.[34]

2.6 THE FUTURE OF OPEN DATA IN THE SLOVAK REPUBLIC

The purpose of this subchapter is neither comprehensive comparison of the open data issue in the Slovak Republic and the Czech Republic nor implementation of PSI Directive into Slovak and Czech legal order. We are aiming at pointing out main legal differences regarding the issue of open data, especially its legal definition.

The Government of the Slovak Republic adopted the Action Plan of the Initiative for Open Government in the Slovak Republic for 2017–2019 (hereinafter referred to as the "Action Plan 2017–2019") at its meeting on 1 March 2017. Open Information is one of the priorities of the Action Plan 2017–2019. Other priorities are open education and open science, government open to dialogue and open justice and public prosecution.

Open data is one of the strategic priorities of the National Concept of Informatization of Public Administration of the Slovak Republic for the years 2016–2020 (hereinafter referred to as the "National Concept 2016")[35]. The National Concept 2016 clarifies that

---

[31] Available from: https://data.gov.sk/about [Accessed March 2018].

[32] Available from: https://data.gov.sk/ [Accessed 6 March 2018].

[33] Available from: https://index.okfn.org/place/ [Accessed 18 September 2018].

[34] Available from: https://ec.europa.eu/digital-single-market/en/scoreboard/slovakia [Accessed 6 March 2018].

[35] Available from: http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=25951 [Accessed 6 March 2018].

> *"the basic type of released data is so-called public sector information that public authorities create, collect or pay for it."*[36]

The National Concept 2016 proposes the adoption of the Open Data Act which would regulate both the issue of licensing as well as restrictions on the provision of certain public administration data.[37] According to the Open Data Strategic Priority which specifies the goals of the National Concept 2016 in the field of open data, it should be an act that transposes the PSI Directive in a clear manner. In our opinion, the adoption of a comprehensive act that would regulate the issue of open data is not the only appropriate solution.

Open data legislation in the Czech Republic could serve as an example for the Slovak Republic. The issue of open data is regulated by Act No. 106/1999 Coll., On Free Access to Information, as amended (hereinafter referred to as the "Czech Freedom of Information Act"). The open data regime was created by amendment of the Czech Freedom of Information Act in 2017.[38] The purpose of this amendment was to

> *"ensure the simplest, reusable use of data provided by the public sector as open data for the creation of commercial and non-commercial services by the professional public."*[39]

The new legal framework also contains the legal definition of the term open data. According to the Czech Freedom of Information Act, open data is defined as

> *"information disclosed in a way allowing remote access in an open and machine-readable format when neither manner nor purpose of re-use is limited and which are recorded in the national catalog of open data."*[40]

Information from registries or lists held or managed by public authorities which are lawfully accessible to anyone and can be used for commercial or other profitable activities, for study or for scientific purposes or for public inspection of public authorities shall be disclosed as open data.

[36] The National Concept 2016, p. 45.

[37] Ibid.

[38] Czech Freedom of Information Act. [online] Available from: http://www.senat.cz/xqw/xervlet/pssenat/htmlhled?action=doc&value=80874 [Accessed 8 March 2018].

[39] Statement of reasons of the act that amended Czech Freedom of Information Act [online]. Available from: https://www.psp.cz/sqw/text/orig2.sqw?idd=112562 [Accessed 9 March 2018].

[40] Czech Freedom of Information Act, Section 3 (11).

The data in question is recorded in the national catalog of open data[41] which is an information system of the public administration and operated by the Ministry of the Interior of the Czech Republic.[42]

The list of information to be published as open data is defined in the implementing legal regulation, in particular, the Government Order No. 425/2016 Coll., On the list of information published as open data.[43]

2.6.1 OPEN DATA REGIME V. PSI RE-USE REGIME V. FREE ACCESS TO INFORMATION REGIME

In general, we could say that open data is special type of PSI made available to public. The European Commission defines open (public) data as

> *"PSI that can be readily and widely accessible and re-used, sometimes under non-restrictive conditions."*[44]

From the perspective of Slovak legal order, especially Freedom of Information Act, we can find some differences between the open data regime and PSI regime and the traditional regime of free access to information.[45] The main distinguishing characteristics are the purpose of the regime, the scope of released information, periodicity of information releasing and the requirement of application submission.

---

[41] Available from: https://portal.gov.cz/otevrena-data/datove-sady/2018-01 [Accessed 9 March 2018].

[42] Czech Freedom of Information Act, Section 4b (2) and Section 4c.

[43] Government Order No. 425/2016 Coll., On the list of information published as open data. [online] Available from: http://www.epi.sk/zzcr/2016-425 [Accessed 9 March 2018].

[44] Digital single market open data. [online] Available from: https://ec.europa.eu/digital-single-market/en/open-data [Accessed 20 September 2018].

[45] Following the successful transposition of PSI Directive into the Slovak legal order, three categories of providing information can be mentioned: (I) mandatory disclosure of information (Section 5), contracts (Section 5a), invoices and orders (Section 5b), (II) disclosure of information on request (Section 14 et seq.), (III) disclosure of information for re-use purposes (Section 21b et seq.). Clear legal obligation to disclose PSI as open data is absent in Slovak legal order. in accordance with aforementioned, we can distinguish between free access to information regime (I and II), PSI re-use regime (III) and open data regime. the main idea of defining separate open data regime is the fact that the regime in question is based on disclosure of information in datasets that are available online where no request is required in comparison to PSI re-use regime. Furthermore, on the basis of aforementioned, we could say that Freedom of Information Act regulates providing of information by publishing (I) and providing information on request (II and III). It is necessary to point out that in the case of disclosure of information for re-use purposes (III) is obliged person obliged to make the information available for re-use purposes on request. However, pursuant to Section 21d (1) of the Freedom to Information Act, information for re-use may be disclosed by the obliged person without a request. The Czech Freedom to Information Act regulates providing information by disclosure (Section 4b) and providing information on request (Section 4).

It should be borne in mind that in the case of the free access to information regime, the purpose is achieving transparency and increasing control in public administration. The main aim of the regime in question is the realization of the right to information. The PSI re-use regime is aimed at achieving a commercial objective.[46] Moreover, the PSI re--use regime can be considered as the realization of the right to business.[47] In the case of open data regime, despite the undeniable economic potential of public administration data, open data fosters participation of citizens in political and social life and increases transparency of government and public control. Furthermore, having more data openly available will help discover new and innovative solutions to address societal challenges.[48]

Other differences are the scope of released information, the periodicity of information releasing as well as the requirement of application submission. In the case of the free access to information regime, the information is made available one-time and irregularly. Furthermore, a person has to submit an application to access the information. On the other hand, in the case of PSI re-use regime, the disclosure of the information is regular and vast amount of information is provided. A person usually has to submit an application to obtain information for re--use purposes.[49] In the case of open data regime, the emphasis is placed on the publication of entire datasets of public authorities and these datasets are still available on the Internet. The submission of application is not required.

2.6.2 THE FORMAT OF PROVIDED INFORMATION

One of the most serious obstacles why PSI cannot be published as open data is the structure of information that is released for re-use purposes. Public sector bodies are advised to release documents in available formats or languages.[50] Where appropriate and possible, the documents in question

---

[46] Janssen, K. (2011). The influence of the PSI directive on open government data: an overview of recent developments. *Government. Information Quarterly*, 28, pp. 453.

[47] Myška, M. et al. (2014) *Veřejné licence v České republice*. Brno: Masarykova univerzita, pp. 97–98.

[48] Digital single market open data. [online] Available from: https://ec.europa.eu/digital-single-market/en/open-data [Accessed 20 September 2018].

[49] Pursuant to Section 21d (1) of the Freedom of Information Act, information for re-use purposes can be disclosed by the obliged persons without a request.

[50] PSI Directive 2013, Article 5 (1).

should be made available in an open, machine-readable format along with their metadata.

Documents, as well as metadata, should, to the fullest extent possible, meet official open standards. These standards have been established in writing and contain detailed specifications how interoperability of software has to be ensured. The specifications in question are freely available.[51]

A document in a machine-readable format can be considered a document if it is in a file format structured so that software applications can easily identify, recognize, and extract specific data from the document. In terms of machine-readable format, it can be open format or subject to ownership. In the case of an open format, it is meant as file format that is publicly available without any restriction that would prevent re-use. The machine-readable format may also be formally standardized or not.[52] At present, in the field of open data, technologies are introduced that allow the interconnection of data from different sources to create open interconnected data. In the light of aforementioned, the Resource Description Framework (RDF) format is used. Another recommended format is XML format. It should be noted that Portable Document Format (PDF) is an open standard but is not machine-readable and is therefore not suitable as an open data format.[53]

Public sector bodies are not obliged to create or adapt documents or provide extracts in order to ensure that documents are in a machine--readable format where this would involve disproportionate effort, going beyond a simple operation.[54]

In accordance with the Freedom of Information Act, the form and method of making the information available for re-use depend on the technical conditions of the public authority. The legislator explicitly prefers the electronic form of disclosure and it is possible and appropriate as open data[55] allowing automated processing[56] with their metadata.

[51] Ibid., Article 2 (8). The open standard is characterized by the fact that it does not belong to anyone and can be used by everyone. in particular, we can consider as open standard: XML (eXtensible Markup Language), CSV (Comma Separated Values), JSON (Javascript Object Notation).

[52] PSI Directive 2013, Recital 21.

[53] More on the issue of open interconnected data in Geiger, CH., P., Von Lucke, J. (2012) Open Government and (Linked) (Open) (Government) (Data). *JeDEM Vol. 4, No. 1*, pp. 265–278.

[54] PSI Directive 2013, Article 5 (2).

[55] Regulation on Standards, Section 52.

[56] Ibid., Section 51 (2).

The disclosure of information for the purpose of its re-use arranged in a structure or formats according to the criteria specified by the applicant is not an obligation of the public authority. If the requirements of the applicant go beyond the simple operation, the public authority is not obliged to provide a specific technical solution for the connection or connection of the applicant. Furthermore, public authority is not obliged to continue the preparation and storage of information for the purpose of its re-use through another person.[57]

The Czech Freedom of Information Act states that public authorities are obliged to disclose specific types of information[58] as open data. Such an obligation is absent in the case of the Slovak Freedom of Information Act. According to the the Czech Freedom of Information Act, specific information have to be disclosed in an open and machine-readable format.[59] Open format is defined as

> *"the format of a data file that is not dependent on specific technical and software equipment and is made available to the public without any restriction that would make it impossible to use the information contained in the data file."*[60]

Machine-readable format is defined as

> *"format of a data file with a structure that enables software to easily find, recognize and extract from that data set specific information, including individual data and their internal structure."*[61]

In connection with the format of information provided on request, the Czech Freedom of Information Act states that the information is provided in the formats and languages according to the content of the request for information, including the relevant metadata unless otherwise provided in the act in question. However, the obliged entity[62] is

[57] Freedom of Information Act, Section 21g (2).

[58] Information from registries or lists held or managed by public authorities which are lawfully accessible to anyone and can be used for commercial or other profitable activities, for study or for scientific purposes or for public inspection of public authorities. Section 4b (2) of the Czech Freedom of Information Act.

[59] Czech Freedom of Information Act, Section 3 (11).

[60] Ibid., Section 3 (8).

[61] Ibid., Section 3 (7).

[62] Obliged entities are defined in Section 2 of the Czech Freedom of Information Act. Entities in question are obliged to provide information according to the Czech Freedom of Information Act.

not obliged to change the format or language of the information or to create metadata for information if such a change or the creation of metadata would be an unreasonable burden for the obliged entity. In this case, the obliged entity will comply with the request by providing information in the format or language in which it was created.[63] In addition, if possible, taking into account the nature of the application submitted and the manner of recording the information requested, the obliged entity will provide the information in electronic form.[64]

3. PROCESSING OF OPEN DATA AFTER GDPR

PSI in form open data facilitate free flow of information within public space. Respected datasets are comprised of non-personal and personal data. When data reveal any information related to an identified or identifiable individual, another piece of legislation plays an important role.

Protection of personal data is in the center of interest of politicians, academics and practicing lawyers in these days. The main reason for the buzz is the reform of data protection framework. The leading legal instrument in the area is adopted *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 – hereinafter referred to as the "GDPR")[65], coming into force on 25th May 2018. Second part of the EU data protection reform package constitutes of *directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*. The emphasis in this article is put solely on GPDR as a basic legal instrument governing data protection law in society.

---

[63] Ibid., Section 4a (1).

[64] Ibid.

[65] 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). *Official Journal of the European Union* (L 119/1) 4 May. [online] Available from: http://data.europa.eu/eli/reg/2016/679/oj [Accessed 3 March 2018].

This part of the article aims at data protection issues related to the processing of personal data that has been made public and re-use of published public sector information including personal data. First of all, it is of the essence to make the distinction between two potential options of publication of PSI as open data: (a) anonymized datasets or (b) datasets that include personal data (including pseudonymized datasets). If datasets are truly anonymized and it is not possible to e.g. via reverse identification to determine a person whom personal data are processed, the GDPR does not apply.[66] On the other hand, if published datasets contain information that are "relating to an identified or identifiable natural person", data protection laws apply and controllers and processors (entities processing personal data) shall comply with specific obligations laid down by GDPR. The same shall be held considering pseudonymized data. Pseudonymization may be defined as

> *"replacing one attribute (typically a unique attribute) in a record by another."*[67]

Pseudonymization is just a security measure to foster security of personal data processing. Although identification of individual is impeded, it is still possible due to unique key individualizing an identified individual.

Secondly, the distinction between first controllers and re-users[68] has to be made due to different issues connected with processing of personal data. First controllers are discussed only briefly and deeper analysis is made regarding potential re-users of open data as specific legal grounds for re--using of publicly available information is not provisioned in national laws of Slovak Republic and Czech Republic after GDPR.

---

[66] See 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). *Official Journal of the European Union* (L 119/1) 4 May. Recital 26. [online] Available from: http://data.europa.eu/eli/reg/2016/679/oj [Accessed 3 March 2018].

[67] Article 29 Data Protection Working Party 05/2014 on Opinion on Anonymisation Techniques, supra note 228, p. 20. [online] Availible from http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf [Accessed 10 August 2018].

[68] Terms are used in line with outcomes of LAPSI Policy Recommendation No. 4: Privacy and Personal data protection – LAPSI Working Group 2 Privacy aspects of PSI. [online] Available from: http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=8366 [Accessed 10 August 2018].

3.1 FIRST CONTROLLERS OF OPEN DATA

Public administration in general collects vast amount of data related to citizens of respective states. In many cases data collected by public authorities includes personal data e.g. related to identity of users of public administration services, sensitive information about health or social security. Furthermore, publicly available registers may contain personal data related to identifiable natural persons that are public officials or in a business relationship with state.[69]

From the personal data protection view, public authorities as first controllers shall be considered the original controllers of personal data. Data are directly (and in most cases voluntarily) provided to public authorities by data subjects. Personal data are collected mainly on legal grounds of legal obligation pursuant to Article 6 (1) c) GDPR as it is directly prescribed by law that public authorities process personal data within their competences or performance of a task carried out in the public interest or in the exercise of official authority in accordance with Article 6 (1) e) GDPR. The processing operation at stake is publishing some of the information and the issue is that using aforementioned legal grounds require (rather specific) provision of law of member state or EU law. It is of our opinion that personal data originally collected for the purpose of fostering transparency may be published with the same purpose in hand. On the other hand, consequences and effects on rights and freedoms have to be taken carefully into account and that might result in limited (either by scope or use) publication of personal data by public authorities.[70]

Balancing right to privacy and/or right to data protection and public interest via publication of information related to identifiable individuals is subject of debates not only within academics.[71] The issue is partially reflected in recital 154 GDPR.[72] After all, the European Court of Human Rights in case concerning publication of data of elected local councilor stated that

---

[69] E.g. *Register of Public Sector Partners in Slovak Republic.* [online] Available from https://rpvs.gov.sk/rpvs [Accessed 10 August 2018].

[70] See more in Borgesius, F.Z., Gray, J., Eechoud, M.V. (2015). Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework. *Berkeley Technology Law Journal.* 30, pp. 2073–2132.

[71] See e.g. outcomes of LAPSI 2.0 Thematic Network – D2.2 – Position paper access to data. [online] Available from: http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=8341 [Accessed 10 August 2018].

> *"the general public has a legitimate interest in ascertaining that local politics are transparent and Internet access to the declarations makes access to such information effective and easy. Without such access, the obligation would have no practical importance or genuine incidence on the degree to which the public is informed about the political process."*[73]

Therefore such processing operations require careful assessment of proportionality and balancing exercise.

Besides that, controllers including public authorities have to be in compliance with principles of processing of personal data as provisioned in Article 5 GDPR,[74] specific security and organizational measures have to be effectively implemented e.g. obligatory appointment of data protection officer.[75]

Concluding this section, public authorities are in better position from data protection perspective than potential re-users. The latter stems from the fact that public authorities are original controllers (original collectors) of personal data and legal exercise of public power delegated by law provides justification for fostering transparency in public administration by making relevant data publicly available.

---

[72] *"This Regulation allows the principle of public access to official documents to be taken into account when applying this Regulation. Public access to official documents may be considered to be in the public interest. Personal data in documents held by a public authority or a public body should be able to be publicly disclosed by that authority or body if the disclosure is provided for by Union or Member State law to which the public authority or public body is subject. Such laws should reconcile public access to official documents and the reuse of public sector information with the right to the protection of personal data and may therefore provide for the necessary reconciliation with the right to the protection of personal data pursuant to this Regulation. The reference to public authorities and bodies should in that context include all authorities or other bodies covered by Member State law on public access to documents. Directive 2003/98/EC of the European Parliament and of the Council (14) leaves intact and in no way affects the level of protection of natural persons with regard to the processing of personal data under the provisions of Union and Member State law, and in particular does not alter the obligations and rights set out in this Regulation. in particular, that Directive should not apply to documents to which access is excluded or restricted by virtue of the access regimes on the grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been provided for by law as being incompatible with the law concerning the protection of natural persons with regard to the processing of personal data."*

[73] *Wypych v. Poland*, No. 2428/05, ECHR 2005 (Admissability decision).

[74] For more elaborate discussion of issues connected to application of principles of data protection see Borgesius, F.Z., Gray, J., Eechoud, M.V. (2015). Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework. *Berkeley Technology Law Journal.* 30, pp. 2073–2132.

[75] 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). *Official Journal of the European Union* (L 119/1) 4 May. Art. 37 (1) a). [online] Available from: http://data.europa.eu/eli/reg/2016/679/oj [Accessed 3 March 2018].

3.2 RE-USERS OF OPEN DATA

"After GDPR era" caught controllers and processors of open data in the role of users or re-users, i.e. persons different from original controllers that made data publicly available in precarious situation. The reason is that GDPR does not explicitly provision further processing of personal data for re-use and implicitly left the issue for national legislators.

The question is particularly important for various non-governmental organizations (NGOs) and other bodies governed by the private law that serve as watchdogs of the government or public administration in general. When it comes to re-use of PSI (open data), national data protection acts traditionally offer a legal ground for further processing of PSI (open data). However, it seems that at least considering Slovakia, the game has changed. Slovak New Data Protection Law[76] does not contain the exception for processing of personal data that has already been published. Thus, the question arose: Is further processing of PSI particularly in form of open data dead for entities from private sector willing to participate in the public sphere?

3.2.1 PURPOSE OF RE-USE OF OPEN DATA FROM THE DATA PROTECTION PERSPECTIVE

Each processing operation with personal data needs to have a purpose and a legal ground. The aforementioned aspects are "alfa" and "omega" of data protection and are closely connected in a sense that each purpose shall be covered by one of the legal grounds. As mentioned in the previous parts of the article, the main purpose of open data is to ensure and promote transparency in public administration and increase the participation of citizens in the context of public matters.[77] Thus the primary aim of the discussed concept shall be perceived as broadly as possible due to its nature. However, using vague terms especially considering purpose specification for processing of personal data is a rather sensitive issue.

---

[76] Slovak Act No. 18/2018 Coll., On Protection of Personal Data and on Changing and amending of other acts. Slovakia.

[77] Taking into account Open Data interests as defined by Borgesius et. al the interest would fall within category of *„political accountability and democratic participation."* Two other interests are innovation and economic growth and public sector efficiency and service delivery. See Borgesius, F.Z., Gray, J., Eechoud, M.V. (2015). Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework. *Berkeley Technology Law Journal,* 30, pp. 2078–2084.

The question of purpose specification is analyzed in Working Party 29 (hereinafter referred to as the "WP29") Opinion on "purpose limitation".[78] GDPR stipulates that personal data shall be

> *"collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes."*[79]

The problem at stake is how to define the purpose of PSI in form of open data to be in compliance with requirements to be specific, explicit and legitimate.

The specification of the purpose lies in the requirement of a controller to determine how the processed personal data will be used for and assess the volume of personal data necessary for the processing operation. According to the Opinion of WP29

> *"the purpose of the collection must be clearly and specifically identified […] (and) […] it must be detailed enough to determine what kind of processing is and is not included within the specified purpose."*[80]

When it comes to the concept of open data, the provision of the wording of the purpose is challenging issue. a notice declaring that *"Your personal data may be used in public interest"* may not suffice as the declaration is too vague. What is more, the legal definition of public interest does not exist and the interpretation of pertinent notion continually changes through time and space. In our opinion, the emphasis shall be put on the purpose of the original processing operation resulting in the publication of pertinent information.

The second requirement of compliance with the principle of purpose specification is explicitness of the purpose. In layman´s words, the purpose

---

[78] Article 29 Data Protection Working Party Opinion 03/2013 on purpose limitation. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf [Accessed 3 March 2018]. The opinion is generally still applicable under GDPR as per the fact that from material point of view deals with principle of purpose limitation that is preserved in new regulation.

[79] 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). *Official Journal of the European Union* (L 119/1) 4 May. Art. 5 (1) (b). [online] Available from: http://data.europa.eu/eli/reg/2016/679/oj [Accessed 3 March 2018].

[80] Article 29 Data Protection Working Party Opinion 03/2013 on purpose limitation, p. 15. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. [Accessed 3 March 2018].

of the processing operation shall be openly and clearly stated by available means. According to the OECD

> *"such specification of purposes can be made in a number of alternative or complementary ways, e.g. by public declarations, information to data subjects, legislation, administrative decrees, and licenses provided by supervisory bodies."*[81]

Taking into account the nature of the concept of open data, the original purpose of the collection is provided by specific legislation or via other legal ground. Persons entering public domain shall reasonably expect re--publication and further use of their personal data once provided for the purpose of public control and transparency of public governance. What is more, if a person publishes his personal data as an obligation provided by law, further publication (in terms of re-use) of pertinent data for the same or similar purpose[82] should be deemed compatible with the requirement of a reasonable purpose.

Thirdly, the purpose must be legitimate. The legitimacy of the purpose may be perceived in two manners. On one hand, the purpose must be based on one of six legal grounds provided by the data protection legislation being consent, the performance of the contract, legal obligation, vital interest, public interest and legitimate interest. On the other hand, for the purpose to be legitimate compliance with aforementioned duty is not enough. The purpose as such shall be in accordance with the law in general. According to the WP29, the law

> *"includes all forms of written and common law, primary and secondary legislation, municipal decrees, judicial precedents, constitutional principles, fundamental rights, other legal principles, as well as jurisprudence, as such 'law' would be interpreted and taken into account by competent courts."*[83]

---

[81] Explanatory Memorandum to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Section 54. [online] Available from: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#memorandum [Accessed 3 March 2018].

[82] 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). *Official Journal of the European Union* (L 119/1) 4 May. Art. 6 (4). [online] Available from: http://data.europa.eu/eli/reg/2016/679/oj [Accessed 3 March 2018].

[83] Article 29 Data Protection Working Party Opinion 03/2013 on purpose limitation, p. 20. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf [Accessed 3 March 2018].

Re-use of open data concerning government and public authorities shall be considered in accordance with the law due to the nature of the activity as promoting transparency and participation of the citizens in public administration affairs. The aforementioned is in line with the idea of openness of public administration and "sousveillance"[84] as a method of control of the government executed by society.

The principle of purpose specification is constituted by two aspects – (i) specification of a purpose per se and (ii) compatibility test. The compatibility test is provisioned in Article 6 (4) of the GDPR.[85] In other words, if you process personal data and the purpose of the original processing operations changes, there is an obligation to find a new legal ground. However, if the new purpose is compatible with the original purpose, search for a new legal ground is not necessary. GDPR states five factors that shall be taken into consideration while assessing compatibility: (i) any link between your initial purpose and the new purpose, (ii) the context in which you collected the data – in particular, your relationship with the individual and what they would reasonably expect, (iii) the nature of the personal data – e.g. is it special category data or criminal offence data, (iv) the possible consequences for individuals of the new processing and (v) whether there are appropriate safeguards – e.g. encryption or pseudonymisation.[86]

It shall be emphasized that two strict limitations exist for using compatible purpose in general. First of them is explicitly mentioned in the GDPR stating that compatibility test does not apply to the (original) processing based on a consent as a legal ground. Secondly, a third party that is not an original controller conducting processing operations shall carefully follow the original purpose that had been specified. As WP29 notes:

---

[84] Mann, S. (2004). *Sousveillance: Inverse Surveillance in Multimedia Imaging. Computer Engineering,* pp. 620–627. [online] Available from: http://wearcam.org/acmmm2004 sousveillance/mann.pdf [Accessed 3 March 2018].

[85] *„Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected."*

[86] 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). *Official Journal of the European Union* (L 119/1) 4 May. Art. 6 (4). [online] Available from: http://data.europa.eu/eli/reg/2016/679/oj [Accessed 3 March 2018].

> *"the mere fact that personal data are publicly available for a specific purpose does not mean that such personal data are open for re-use for any other purpose."*[87]

Illustrating aforementioned on the example, in many countries it is obligatory for government officials to publish their asset declarations.[88] On one hand, it would be potentially compatible to gather all publicly available information and create a profile of a specific government official including tax return data to facilitate the transparency. On the other hand, using personal data in tax returns for sending commercial advertisements by a car reseller based on tax revenues would not be probably deemed compatible with the original purpose.

Coming back to the open data and re-use, the WP29 seems to be aware of challenges of the discussed institutes and calls for cautious impact assessment. It particularly notes that

> *"once personal data are publicly available for re-use, it will be increasingly difficult, if not impossible, to have any form of control on the nature of potential further use, be it for historical, statistical, scientific or other purposes."*[89]

Although the WP29 prefers to conduct anonymization techniques in disseminating personal data to the public sector for re-use, the anonymization would kill the purpose and task of open data as defined at the beginning of the article.

Concluding findings above the compatibility test of a purpose is not completely appropriate measure to use as a basis for processing of personal data in the context of re-use of open data by third parties e.g. NGOs acting as watchdogs of activities of public bodies.

---

[87] Article 29 Data Protection Working Party Opinion 06/2013 on open data and public sector information ('PSI') reuse, p. 20. [online] Availible from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp207_en.pdf [Accessed 3 March 2018]. As this opinion deals with basic issues with processing of open data from the data protection point of view it shall be applicable to certain extent also under GPDR.

[88] See Djankov, S. – La Porta, R. – Lopez-de-Silanes, F. – Schleifer, a (2009). Disclosure by Politicians. *American Economic Journal: Applied Economics, American Economic Association, vol. 2(2)*, pp. 179–209.

[89] Article 29 Data Protection Working Party Opinion 03/2013 on purpose limitation, p. 49. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf [Accessed 3 March 2018].

3.2.2 POTENTIAL LEGAL GROUNDS IN GDPR AND SLOVAK AND CZECH DATA PROTECTION ACTS

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.[90] Lawfulness of processing is developed in the Article 6 of GDPR explicitly stipulating legal grounds for processing of personal data (consent, the performance of the contract, legal obligation, vital interest, public interest and legitimate interest). WP29 in its opinion 06/2013 on open data and public sector information re-use also highlights that any further re-use must have an appropriate legal basis.[91] Taking into account re-use of PSI in form of open data legal grounds of the interest are public interest and legitimate interest.[92] This part of the article analyzes aforementioned legal grounds from the view of re--use of open data.

a) public interest

Article 5 (1) (e) GDPR stipulates that processing of personal data is lawful when it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The legal ground "public interest" contains two different scenarios where first is designed to govern processing operations with personal data of official authority as a controller and the second scenario anticipates tasks in (delegated) public interest conducted by private bodies. However, GDPR sets forth one limitation for using discussed legal ground for processing. The basis for the processing under the legal ground of public interest shall be laid down by Union law or Member state law to which a controller is subject.[93] In other words, a special law that provides the purpose of such

[90] Article 29 Data Protection Working Party Opinion 03/2013 on purpose limitation, p. 49. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf [Accessed 3 March 2018].

[91] 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). Official Journal of the European Union (L 119/1) 4 May. Art. 5 (1) a). [online] Available from: http://data.europa.eu/eli/reg/2016/679/oj [Accessed 3 March 2018].

[92] Article 29 Data Protection Working Party Opinion 06/2013 on open data and public sector information ('PSI') reuse, p. 19. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp207_en.pdf [Accessed 3 March 2018].

[93] 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). *Official Journal of the European Union* (L 119/1) 4 May. Art. 5 (3). [online] Available from: http://data.europa.eu/eli/reg/2016/679/oj [Accessed 3 March 2018].

processing, potential data subjects and types of personal data processed is needed. It is of the essence to note that many NGOs monitoring public servants or government officials are not established by specific acts but rather as entities regulated by private law and completely independent from the state. Deriving from this it may prove very challenging to argue a public interest as a lawful ground for processing personal data in the context of re-use of open data.

b) legitimate interest

According to the Article 6 (1) (f) processing shall be lawful if processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Compliance with the aforementioned legal ground for processing requires so-called "balancing test" sketched in Recital 47 of the GDPR. The legal ground of legitimate interest shall not be applied to processing carried out by public authorities in the performance of their tasks.

Taking into account the Opinion 06/2014 on the notion of legitimate interests of the data controller (hereinafter referred to as the "Opinion") drafted by Working Party 29 the interest shall be legitimate and legitimacy is embedded *inter alia* in exercise of the right to freedom of expression or information, including in the media and the arts and prevention of fraud, misuse of services, or money laundering.[94] The latter at least partially covers purposes of open data. The Opinion introduces four factors to be evaluated during the balancing test. It is of the essence to analyze (i) the controller's legitimate interest, (ii) impact on the data subjects, (iii) provisional balance and (iv) additional safeguards applied by the controller to prevent any undue impact on the data subjects.[95] Thus the analysis of these factors in the context of re-use of open data is necessary.

[94] Article 29 Data Protection Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p. 25. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf [Accessed 3 March 2018].

[95] Article 29 Data Protection Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p. 33 and further. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf [Accessed 3 March 2018].

When it comes to the *first factor*, WP29 explains that legitimate interest can stem from exercising of a fundamental right, public interest (interests of the wider community) or other legitimate interest. The European Charter of Fundamental Rights provisions Right to good administration in the Article 41. Due to the wording of pertinent article

> *"every person has the right to have his or her affairs handled impartially, fairly and within a reasonable time by the institutions, bodies, offices, and agencies of the Union."*[96]

The authors of the article are of the opinion, that the Right to good administration shall not be perceived only as a basis for a wide range of procedural rules. The relevant right may be also understood as a general obligation of a state to provide effective public administration that is closely connected to the transparency and accountability. Deriving from this, re-use of open data including personal data of government officials shall fall within the discussed right. It is also of the essence to note that in case of inability to rely on the exercise of human right as a basis for legitimate interest, the whole idea of open data and re-use in general related to public governance is definitely in public interest or the interests of the wider community as described in the Opinion. WP29 even explicitly uses the example of processing personal data by a non-profit organization in order to raise awareness of government corruption.[97]

The second factor of the balancing test is the analysis of the impact on data subjects. Aspects to be taken into consideration are the nature of personal data, the way the information is being processed, the reasonable expectations of the data subjects and the status of the controller and data subject.[98] Generally, the assessment of the impact should be perceived in a broad way to evaluate potential and actual threats to the freedoms and rights of data subjects including positive and negative consequences.

---

[96] Article 41 *Charter of Fundamental Rights of the European Union,*, 26 October 2012 (2012/C 326/02). [online] Available from: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A12012P%2FTXT [Accessed 18 August 2018].

[97] Article 29 Data Protection Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p. 35. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf [Accessed 3 March 2018].

[98] Article 29 Data Protection Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p. 36. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf [Accessed 3 March 2018].

However, specificity of open data is that pertinent data have already been published and processed on other legal ground (typically consent or statutory obligation) and therefore the data subject concerned shall be already aware of potential further processing operations. The requirement to assess the nature of the data reflects the dichotomy in the typology of personal data being personal data[99] and sensitive personal data[100]. As WP29 notes in the Opinion, it is also relevant if the data has already been made publicly available.

> *"The fact that personal data is publicly available may be considered as a factor in the assessment, especially if the publication was carried out with a reasonable expectation of further use of the data for certain purposes (e.g. for purposes of research or for purposes related to transparency and accountability)."*[101]

In case of open data the purpose of re-use is clearly in transparency and creating a public-friendly interface containing pertinent information and thus such processing operation with personal data shall be considered legitimate considering the nature of the data processed. Another aspect is the way data are being processed. In other words, it is of the essence to evaluate how data are processed, e.g if there is profiling, commercial profit, deep-packet inspection or predictions about data subjects are made. Again, it shall be emphasized that re-using of publicly available information in form of open data is just "processing of already processed". In this case, if data are already in the public sphere (online or in publicly available registers) it would be inappropriate to sanction controllers or processors for

---

[99] 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). *Official Journal of the European Union* (L 119/1) 4 May. Art. 4 (1). [online] Available from: http://data.europa.eu/eli/reg/2016/679/oj [Accessed 3 March 2018].

[100] 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). *Official Journal of the European Union* (L 119/1) 4 May. Art. 9 (1). [online] Available from: http://data.europa.eu/eli/reg/2016/679/oj [Accessed 3 March 2018]: *"personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."*

[101] Article 29 Data Protection Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p. 39. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf [Accessed 3 March 2018].

further processing in the (identical) public sphere. The same applies to the reasonable expectations of the data subject. Once data of persons concerned is published, it is reasonable to expect that data will be re-used or processed for the same purpose. On the other hand, any commercial profit from further processing operations deriving from open data may be considered as a crucial factor in assessing whether the interest of the controller is legitimate although WP29 notes that

> *"the assessment of compatibility should not be primarily based on whether the economic model of a potential re-user is based on profit or not."*[102]

Nevertheless, the close connection of re-using personal data would probably be a strong indication of incompatibility of processing operations. Lastly, it is important to weight status of the data controller and data subject. In case of re-use of publicly available information the "clash" is between government officials, politicians or highly ranked public servants (and sometimes their relatives) and non-governmental organizations conducting their activity without the help of public sector. The specific nature of the relationship sketched above shall be taken into account with regard to public interest.

The third factor to be considered is to carry out provisional balancing. the WP29 especially notes to include requirements of transparency and proportionality in the conducting provisional balancing. Put differently, adherence to the compliance with data protection rules

> *"should mean that the impact on individuals is reduced, that data subjects' interests or fundamental rights or freedoms are less likely to be interfered with and that therefore it is more likely that the data controller can rely on"*[103]

legitimate interest as a legal ground for processing.

The fourth factor in assessing whether the interest of the controller is legitimate lies in providing additional safeguards applied by the controller.

---

[102] Article 29 Data Protection Working Party Opinion 06/2013 on open data and public sector information ('PSI') re-use, p. 21. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp207_en.pdf [Accessed 3 March 2018].

[103] Article 29 Data Protection Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p. 41. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf [Accessed 3 March 2018].

In cases where the impact on the data subjects is more severe or significant, the more attention shall be given to applying additional safeguards. WP29 illustrates additional safeguards *inter alia* on the examples of strict limitations of a quantity of data collected or strict application of data minimization principle.[104] With regard to novelties of GDPR, it may be also of the essence to consider the use of data protection by design and data protection by default philosophies that are relevant for further processing of open data.

Another point in favor of using a legitimate interest as the legal ground for further processing of personal data is an example[105] drafted by WP29 describing a scenario where NGO republishes expanses of Members of Parliament. The expenses are published in the context of statutory obligation and NGO analyses and re-publishes the data in more informative and public-friendly way.

> *"Assuming the NGO carries out the re-publication and annotation in an accurate and proportionate manner, adopts appropriate safeguards, and more broadly, respects the rights of the individuals concerned, it should be able to rely on"*[106]

legitimate interest as a legal ground for processing. What is more, the fact that data has already been published weighs in favor of the legitimacy of the processing operations together with the reasonability of expectations of the data subjects. The balance between the legitimacy of the processing operation and impact on rights and freedoms of data subjects shall even be withheld the situations where criminal investigations or loss of elections are a consequence of re-publishing the data concerned. It is also essential to add that it is not relevant on which legal ground the original processing of personal data is conducted as all of them are equal from the point of data protection law.

---

[104] Ibid., p. 42.

[105] Ibid., p. 57.

[106] Article 29 Data Protection Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p. 41. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf [Accessed 3 March 2018].

c) potential legal grounds in Slovak Data Protection Act and Czech Data Protection Act

As mentioned earlier in the article, during the transposition of the old directive on personal data[107] many member states chose to implement specific provisions creating a legal ground for processing publicly available information. It shall be noted that GDPR leaves space for Member states to provide specific provisions in their national laws concerning balancing right to data protection and right to freedom of expression and free access to documents.[108]

Slovak act No. 122/2013 Coll., On Protection of Personal Data states that

> *"the controller shall process personal data without the data subject's consent also if processed personal data have already been disclosed pursuant to Law and the controller properly marked them as disclosed."*[109]

The aforementioned provision shall be deemed to be statutory legal ground for processing that has been widely used by NGOs in the context of further re-using of open data. However new Slovak Data Protection Act[110] does not contain such legal ground for processing with regard to re--use of publicly available information. According to authors of the article entities may rely on Section 78 (2) of Slovak Data Protection Act that provides an exception establishing that the controller shall process personal data without the data subject's consent also, if processing of personal data is necessary for needs of informing the society via mass media and if processing of personal data is conducted by the controller that has such informing in the object of its activity.[111] In other words, if NGO is set up as a watchdog of government officials or evaluating financial transactions

---

[107] Directive 95/46/EC of the 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. *Official Journal of the European Union* (1995/L 281/31) 23 November. [online] Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN:PDF [Accessed 3 March 2018].

[108] 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). *Official Journal of the European Union* (L 119/1) 4 May. Art. 85 and 86. [online] Available from: http://data.europa.eu/eli/reg/2016/679/oj [Accessed 3 March 2018].

[109] *Slovak act No. 122/2013 Coll., On Protection of Personal Data and on changing and amending of other acts*, resulting from amendments and additions executed by the Act. No. 84/2014 Coll., Slovakia. Section 10 (3) (e).

[110] *Slovak Act No. 18/2018 Coll., On Protection of Personal Data and on Changing and amending of other acts*. Slovakia. (Translation by Office for the protection of personal data of Slovak Republic).

in public funding (or any other open data), it would be possible to argue that informing the society via the Internet may be within the range of the statutory legal ground described above.

A similar provision in Czech Data Protection Act No. 101/2000 Coll. is allowing (that)

> *"the controller may process personal data only with the consent of data subject. Without such consent, the controller may process the data... if they were lawfully published in accordance with special legislation".*[112]

However, situation under proposal of new Czech Data Protection Act is different. Although this proposal contains exception for processing of personal data for journalistic purposes in section 16 and following, the legislative construction is more specific than e.g. in section 78 (2) of Slovak Data Protection Act due to the fact that journalistic purposes are explicitly mentioned and does not leave place for discretion (unlike in case of informing society via mass media). Seizing the "Czech" exception for re--use of open data is therefore more than questionable.

3.2.3 FURTHER GDPR CHALLENGES AND IMPACT OF THE PROCESSING

Even if a private body relies on one of the legal grounds for processing together with the fulfillment of requirements for purpose specification, it will be challenging to be in compliance with obligations laid down by GDPR. In this part of the article, The brief discussion of selected obligations shall take place.

First issue is connected to the principle of accuracy. The principle of accuracy means that personal data that are subject to the processing operation shall be accurate and, where necessary, kept up to date. What is more, every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.[113] In case of re-using open data the controller shall monitor the original source of data. Establishing

[111] *Slovak Act No.. 18/2018 Coll., On Protection of Personal Data and on Changing and amending of other acts.* Slovakia. (Translation by Office for the protection of personal data of Slovak Republic). Section 78 (2). (Translation by Matúš Mesarčík).

[112] *Czech Act No. 101/2000 Coll., On the protection of personal data and on the amendment on some acts*. Czech Republic. Section 5 (2) (d). (Translation by Office for the protection of personal data of Czech Republic).

a monitoring mechanism would be an essential according to the obligations in GDPR. Assessing the accuracy of huge amounts of datasets might be an onerous requirement for small entities acting as watchdogs.

Second issue is rights management. Data subjects have specific rights provided directly by GDPR. Controllers are obliged to be in compliance with management of motions and claims of data subjects concerning their rights. Taking into account that re-using of open data is usually made without knowledge of data subjects, it is absolutely necessary to adhere with the informational obligation of the controller where personal data have not been obtained from the data subject.[114] It has to be added that the Article 14 does not apply inter alia where the data subject already has the information (related to the processing of personal data) or the provision of such information proves impossible or would involve a disproportionate effort. GDPR states that

> *"in that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration."*[115]

In the context of re-use of open data it really might occur that especially number of data subjects is high. According to the WP29

> *"the impossibility or disproportionate effort must be directly connected to the fact that the personal data was obtained other than from the data subject."*[116]

The example stated in this part of the article emphasizes challenges adhering to the rights management in compliance with GDPR might be for

[113] 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). *Official Journal of the European Union* (L 119/1) 4 May. Art. 5 (1) d). [online] Available from: http://data.europa.eu/eli/reg/2016/679/oj [Accessed 3 March 2018].

[114] 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). *Official Journal of the European Union* (L 119/1) 4 May. Art. 14. [online] Available from: http://data.europa.eu/eli/reg/2016/679/oj [Accessed 3 March 2018].

[115] 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). *Official Journal of the European Union* (L 119/1) 4 May. Recital 62. [online] Available from: http://data.europa.eu/eli/reg/2016/679/oj [Accessed 3 March 2018].

[116] Article 29 Data Protection Working Party Guidelines on transparency under Regulation 2016/679, p. 27. [online] Available from: http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025 [Accessed 3 March 2018].

controllers of processing operations with personal data that has already been published.

The issue of compatibility of further processing of open data has already been sketched while assessing purpose and legal grounds. It may be quite challenging for a third party to foresee the initial purpose of the publications and be in compliance with it in further processing operations. What is more, there might be situations where personal data are published only for limited amount of time. In this case, monitoring obligation of a controller shall be emphasized again and take into account potential issues related to lack of accountability.

Although GDPR provides implicit space for re-using of personal data for third parties, some of the issues have been outlined above. The most critical are connected to relying on relevant legal ground and purpose specification.[117] It shall be emphasized, that special legal regime (or exception e.g. presented in former Slovak and Czech Data Protection Acts) for processing already published personal data may still be the best option how to deal with uncertainty in processing open data from the data protection view. However, that requires actionability of national legislators and public debate on the topic. The first step has already been taken by European Commission with regard to proposal for a new PSI Directive.[118]

4. CONCLUSION

The analysis of the term open data and its regime from the perspective of Slovak legal order revealed some deficiencies. First of all, the disclosure of information in electronic form is only preferred and where possible and appropriate, as open data. Clear obligation to publish public administration data as open data is absent. Secondly, the term open data and the scope of disclosed open data is not defined in by generally binding legal act in Slovak legal order.

Open data legislation in the Czech Republic could serve as good example for the Slovak Republic. The Czech Freedom of Information Act

[117] For more elaborate discussion on coherency see *Study to support the review of Directive 2003/98/EC on the re-use of public sector information*, pp. 134–140. [online] Available from: https://publications.europa.eu/en/publication-detail/-/publication/45328d2e-4834-11e8-be1d-01aa75ed71a1/language-en [Accessed 11 September 2018].

[118] *Proposal for a revision of the Directive 2003/98/EC on the reuse of public sector information.* [online] Available from: https://ec.europa.eu/digital-single-market/en/news/proposal-revision-directive-200398ec-reuse-public-sector-information [Accessed 11 September 2018].

contains the legal definition of the term open data and the list of information to be published as open data is defined in the implementing legal regulation.

The PSI Directive focuses on the economic aspects of re-use of information rather than on the access of citizens to information. It has no intention to regulate access to information that are held by public sector bodies. Such a situation in connection with the unwillingness of public sector bodies to disclose PSI as open data hinders citizens and entrepreneurs from re-using of PSI for commercial or non-commercial purposes.

GDPR and national data protection acts offer several possibilities how to further conduct processing operations with regard to open data. The most suitable option seems to be careful delineation of the purpose and using a legitimate interest of the controller as a legal ground. However, GDPR challenges such processing of information by imposing strict obligations on the controllers and voices calling for more suitable regime in the context of more coherency may have a point.

LIST OF REFERENCES

[1] *Act No. 101/2000 Coll., On the protection of personal data and on the amendment on some acts.* Czech Republic. In Czech.

[2] *Act No. 106/1999 Coll., On Free Access to Information as amended*. Czech Republic. In Czech.

[3] *Act No. 18/2018 Coll., On Protection of Personal Data and on Changing and amending of other acts.* Slovakia. In Slovak.

[4] *Act No. 211/2000 Coll., On Free Access to Information and on changes and amendments to certain acts*. Slovakia. In Slovak.

[5] Action Plan of the Initiative for Open Government in the Slovak Republic for 2017–2019. [online] Available from: https://www.opengovpartnership.org/sites/default/files/Slovakia_NAP_2017-2019_EN.pdf [Accessed 20 September 2018].

[6] Article 29 Data Protection Working Party Opinion 03/2013 on purpose limitation. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. [Accessed 3 March 2018].

[7] Article 29 Data Protection Working Party Opinion 06/2013 on open data and public sector information ('PSI') reuse, p. 20. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinionrecommendation/files/2013/wp207_en.pdf

[Accessed 3 March 2018].

[8] Article 29 Data Protection Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p. 25. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/2014/wp217_en.pdf [Accessed 3 March 2018].

[9] Attard, J., Orlandi, F., Scerri, S., & Auer, S. (2015). A systematic review of open government data initiatives. *Government Information Quarterly*, 32 (4), pp. 399–418.

[10] Borgesius, F.Z., Gray, J., Eechoud, M.V. (2015). Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework. *Berkeley Technology Law Journal,* 30, pp. 2073–2132.

[11] Boseley, S. UK heart operation death rates fall after data published. *The Guardian*. [online] Available from: https://www.theguardian.com/lifeandstyle/2009/jul/30/heart-surgery-death-rates-fall [Accessed 20 September 2018].

[12] *Charter of Fundamental Rights of the European Union*, 26 October 2012 (2012/C 326/02). [online] Available from: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A12012P%2FTXT [Accessed 18 August 2018].

[13] *Creating value through open data.* [online] Available from: https://www.europeandataportal.eu/sites/default/files/edp_creating_value_through_open_data [Accessed 20 September 2018].

[14] *Crimereports.com.* [online] Available from: https://www.crimereports.com/agency/santacruzpd [Accessed 20 September 2018].

[15] *Data.europa.eu*. [online] Available from: https://data.europa.eu/euodp/en/data [Accessed 20 September 2018].

[16] Datasety. *Data.gov.sk.* [online] Available from: https://data.gov.sk/dataset [Accessed 20 September 2018].

[17] Dawes, S., & Helbig, N. (2010). Information strategies for open government: Challenges and prospects for deriving public value from government transparency. *Electronic Government, 6228*, pp. 50–60.

[18] *Digital single market – Slovakia.* [online] Available from: https://ec.europa.eu/digital-single-market/en/scoreboard/slovakia [Accessed 20 September 2018].

[19] *Digital single market open data.* [online] Available from: https://ec.europa.eu/digital-single-market/en/open-data [Accessed 20 September 2018].

[20] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information. *Official Journal of the European Union*

(2003/L345/90). 31 December. [online] Available from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32003L0098 [Accessed 3 March 2018].

[21] Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information Text with EEA relevance. *Official Journal of the European Union* (2013/L1751/1) 27 June. [online] Available from: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32013L0037 [Accessed 3 March 2018].

[22] Directive 95/46/EC of the 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. *Official Journal of the European Union* (1995/L 281/31). 23 November. [online] Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN:PDF [Accessed 3 March 2018].

[23] Djankov, S. – La Porta, R. – Lopez-de-Silanes, F. – Schleifer, A (2009). Disclosure by Politicians. *American Economic Journal: Applied Economics, American Economic Association, vol. 2(2)*, pp. 179–209.

[24] *Explanatory Memorandum to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Section 54. [online] Available from: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#memorandum [Accessed 3 March 2018].

[25] Geiger, CH., P., Von Lucke, J. (2012) Open Government and (Linked) (Open) (Government) (Data). *JeDEM, Vol. 4, No. 1*, pp. 265–278.

[26] *Global Open Data Index: Survey*. [online] Available from: http://global.census.okfn.org/ [Accessed 20 September 2018].

[27] Guidelines on recommended standard licences, datasets and charging for the reuse of documents 2014/C 240/01. [online] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2014.240.01.0001.01.ENG [Accessed 20 September 2018].

[28] Government Order No. 425/2016 Coll., On the list of information published as open data. Slovakia. In Slovak. [online] Available from: http://www.epi.sk/zzcr/2016-425 [Accessed 9 March 2018].

[29] *History – International Open Data Charter.* [online] Available from: http://opendatacharter.net/history/# [Accessed 20 September 2018].

[30] Huijboom, N., & Van den Broek, T. (2011). Open data: an international comparison of strategies. *European Journal of ePractice*, pp. 1–13.

[31] Janssen, K. (2011). The influence of the PSI directive on open government data: An overview of recent developments. *Government. Information Quarterly*, 28, pp. 446–456.

[32] Janssen, M., Charalabidis, Y., & Zuiderwijk, A. (2012). Benefits, adoption barriers and myths of open data and open government. *Information Systems Management*, 29, pp. 258–268.

[33] *KohoVolit.eu.* [online] Available from: http://kohovolit.eu [Accessed 20 September 2018].

[34] LAPSI 2. Thematic Network – D2 – Position paper access to data. [online] Available from: http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=8341 [Accessed 10 August 2018].

[35] LAPSI Working Group 2 Privacy aspects of PSI. [online] Available from: http://ec.europa .eu/newsroom/dae/document.cfm?action=display&doc_id=8366 [Accessed 10 August 2018].

[36] *Legislation.gov.uk.* [online] Available from: hhttp://www.legislation.gov.uk/ [Accessed 20 September 2018].

[37] *Live map of London Underground.* [online] Available from: http://traintimes.org.uk/map/ tube/ [Accessed 20 September 2018].

[38] *London datastore.* [online] Available from: http://data.london.gov.uk/ [Accessed 20 September 2018].

[39] Materiál programu rokovania. *Rokovania.sk.* [online] Available from: http://www. rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=25951 [Accessed 6 March 2018].

[40] Mann, S. (2004). *Sousveillance: Inverse Surveillance in Multimedia Imaging. Computer Engineering,* p. 620–627. [online] Available from: http://wearcam.org/acmmm2004 sousveillance/mann.pdf [Accessed 3 March 2018].

[41] Munk, R. (2017) Attempt to increase the transparency. *Bratislava law review, Vol. 1, No. 2*, pp. 167–173.

[42] Myška, M. et al. (2014) *Veřejné licence v České republice*. Brno: Masarykova univerzita, 192 p.

[43] National Concept of Informatization of Public Administration of the Slovak Republic for the years 2016–2020.

[44] *O nás.* Data.gov.sk. [online] Available from: https://data.gov.sk/about [Accessed 20 September 2018].

[45] Olejár, D. et al. (2015) *Manažment informačnej bezpečnosti a základy PKI*. Bratislava, 175 p.

[46] *Open Knowledge Foundation:* The Open Data Manual (2011). [online] Available from: http://opendatahandbook.org/ [Accessed 1 March 2018].

[47] *Otvorené zmluvy.* [online] Available from: http://otvorenezmluvy.sk [Accessed 20 September 2018].

[48] Polčák, R. (2016) Informace a data v právu. *Revue pro právo a technologie 7*, pp. 67–91.

[49] *Portál veřejné správy.* [online] Available from: https://portal.gov.cz [Accessed 20 September 2018].

[50] Proposal for a directive of the European parliament and of the Council on the re-use of public sector information (recast). COM/2018/234 final – 2018/0111 (COD). 25 April 2018. [online] Available from: https://ec.europa.eu/digital-single-market/en/news/proposal-revision-directive-200398ec-reuse-public-sector-information [Accessed 11 September 2018].

[51] Proposal for a revision of the Directive 2003/98/EC on the reuse of public sector information. [online] Available from: https://ec.europa.eu/digital-single-market/en/news/proposal-revision-directive-200398ec-reuse-public-sector-information [Accessed 11 September 2018].

[52] 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). *Official Journal of the European Union* (2016/L119/1). 4 May 2016. [online] Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1520438094012&uriCELEX:32016R0679 [Accessed 3 March 2018].

[53] *Regulation of Ministry of Finance of the Slovak Republic No. 55/2014 Coll., On standards for public administration information systems*. Slovakia. In Slovak.

[54] *Rpvs.gov.sk.* [online] Available from: https://rpvs.gov.sk/rpvs [Accessed 20 September 2018].

[55] *Slov-lex.sk.* [online] Available from: https://www.slov-lex.sk/domov [Accessed 20 September 2018].

[56] *Statement of reasons of the act that amended Czech Freedom of Information Act.* [online] Available from: https://www.psp.cz/sqw/text/orig2.sqw?idd=112562 [Accessed 9 March 2018].

[57] Study to support the review of Directive 2003/98/EC on the re-use of public sector information, pp. 134–140. [online] Available from: https://publications.europa.eu/en/pu

blication-detail/-/publication/45328d2e-4834-11e8-be1d-01aa75ed71a1/language-en [Accesed 11 September 2018].

[58] *Ten Principles For Opening Up Government Information.* Sunlight Foundation. [online] Available from: http://sunlightfoundation.com/policy/documents/ten-open-data principles/ [Accessed 20 September 2018].

[59] *The Open Data Handbook.* [online] Available from: http://opendatahandbook.org/ [Accessed 20 September 2018].

[60] Verhulst, S., & Young, A. (2016). *Open Data impact, when demand and supply meet. Key finding of the open data Impact case studies.* Opgehaald van. thegovlab.org. [online] Available from: http://odimpact.org/key-findings.html [Accessed 20 September 2018].

[61] *Wypych v. Poland*. (2005) No. 2428/05, ECHR (Admissability decision).

DOI 10.5817/MUJLT2018-2-5

RIGHT OF ACCESS UNDER GDPR AND COPYRIGHT

by

ANGELA SOBOLČIAKOVÁ*

The paper discusses the right to obtain a copy of personal data based on the access right guaranteed in Articles 15 (3) and limited in 15 (4) of the GDPR. Main question is to what extent the access right provided to data subject under the data protection rules is compatible with copyright. We argue that the subject matter of Article 15 (3) of the GDPR – copy of personal data – may infringe copyright protection of third parties but not a copyright protection attributed to the data controllers.

Firstly, because the right of access and copyright may be in certain circumstances incompatible. Secondly, the data controllers are primarily responsible for balancing conflicting rights and neutral balancing exercise could only be applied by the Data Protection Authorities. Thirdly, the case law of the CJEU regarding this issue will need to be developed because the copy as a result of access right may be considered as a new element in data protection law.

KEY WORDS

Balancing of Interests and Rights; Computer Program Directive, Copy of the Personal Data Undergoing Processing, Copyright, Database Directive, Data Controller, Data Protection Directive, Data Subject, General Data Protection Regulation, Right of Access

1. INTRODUCTION

Nowadays, the life of almost every natural person is lived simultaneously online and offline. The technological development of information society

* angelasobolciakova@gmail.com, external Ph.D. student at the Trnava University in Trnava, Law Faculty, Slovak Republic.

increases the value of personal data and allows for easy traceability of online behaviour of persons, in comparison with their offline life. Therefore, localisation and control over the personal data by data subjects is necessary. In order to improve the position of data subject *vis-à-vis* data controllers, the data protection legislation developed the *right of access by data subject*. This right is binding for data controllers and enhances transparency of personal data processing, especially as data controllers have exclusive control over the processing operations. In other words, the right of access

> *"effectively obliges organizations based anywhere in European Union to provide a copy of all personal data to relevant individual, upon a request being received from such individual."*[1]

The right of access is guaranteed to every natural person and the obligation to comply with the request is entitled to data controllers.

More specifically, this article discusses the obligation of data controller to provide a copy of processed personal data about a data subject upon request. This is a new element in the area of the right of access introduced by the General Data Protection Regulation (hereinafter "GDPR")[2]. Accordingly, this paper will discuss if, and to what extent, the access right provided to data subject under the data protection rules might conflict with copyright.

When reading this article, you need to take into account the following aspects:

First, protection of personal data is regulated through sector specific legislation previously by the Data Protection Directive[3] (hereinafter "DPD") which was replaced in May 2018 by the GDPR. The processing operations with data are solely in the power of data controllers. Therefore, the copy of processed personal data based on the right of access is created from

---

[1] Carey, P. (2009) *Data Protection, A Practical Guide to UK and EU Law*. 3rd ed. New York: Oxford University Press.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2017 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. *Official Journal of the European Union* (OJ L 119/1) 4 May. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN [Accessed 19 September 2018].

[3] 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. *Official Journal of the European Union* (OJ L 281/31) 23 November. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN [Accessed 19 September 2018].

the source, which is not available to the public. Data controllers nowadays collect personal data for different purposes and in different extent with different categories of personal data for each individual purpose or simply use provided personal data for different (compatible) purposes. The right of access by data subject enables to understand the internal business model of data controllers. Disclosure of business model encompasses risks not only connected with violation of the GDPR provisions, but also with competition power or reputation of data controllers.

Second, the paper discusses the issue based on the data protection legislation and its possible conflict with intellectual property (hereinafter "IP") law in particular with copyright legislation. Hence, while there is developed legal regime based on case law about the conflict between copyright or trade marks on one hand and data protection on the other hand, these cases[4] refer to access to information and personal data about the infringers of IP rights of right holders. This kind of access to personal data is based on IP law and national civil law rules, protecting the right holders and is therefore different from data subject's right of access based on data protection legislation.

Third, the paper does not intend to open question of the information concept of law, what is information and data.[5] The terminology used in the paper simply follows the GDPR terminology. Out of the scope of this paper is also the scope of personal data (and information as it is required in Article 15 (1) GDPR) which are eligible to be open to data subjects on the basis of the right of access. In this context, analogy with the right to data portability could be used, the data portability right should portpersonal data which concern data subjects and data which were provided by data subjects to data controllers.[6] However, the right of access covers in Article 15 (1) of GDPR personal data concerning data subject. It could be argued that the access right encompasses wider scope of personal

[4] See e.g. Judgment of 6 November 2003, Bodil Lindqvist, C-101/01, EU:C:2003:596, paragraphs 82 and 84; Judgment of 29 January 2008 Productores de Música de España (Promusicae) v. Telefónica de España SAU, C-275/06, EU:C:2008:54, paragraph 58; Judgment of the Court of 24 November 2011 Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), C-70/10, EU:C:2011:771, paragraph 50.

[5] Bygrave, L. A. (2015) Information Concepts in Law: Generic Dreams and Definitional Daylight. *Oxford Journal of Legal Studies*. 35, (1), pp. 91–120. Available from: http://ojls.oxfordjournals.org/content/35/1/91 [Accessed 19 September 2018]; Polčák, R. (2016) Informace a data v právu. *Revue pro právo a technologie*, 7 (13), pp. 67–91. Available from: https://journals.muni.cz/revue/article/view/4946 [Accessed 19 September 2018].

[6] Compare with Art. 20 (1) of the GDPR.

data than the right to data portability. The Article 29 Working Party, Guidance on the right to data portability[7] recognised following categories of personal data being eligible to be ported:

> "*raw data processed by a smart meter or other types of connected objects, activity logs, history of website usage or search activities*."

Data created by data controllers (which the Article 29 Working Party called "*inferred data*" and "*derived data*", e.g. personalisation or recommendation process for data subjects) are outside the right of data portability but possibly eligible for the right of access.

Finally, the right of access to personal data is a key principle of data protection framework as it permits individuals to exercise control over their data in order to check accuracy and lawfulness of data processing performed by data controllers. Consequently, this right is a prerequisite for exercising the other rights of data subject, e.g. to obtain the rectification, erasure or blocking of her/his personal data.

There are two objectives referred to in this paper. In the first place, it describes the legislative development of the right of access at the EU level in connection with copyright. In the second place, it discusses compatibility of the access right to the copy of personal data with its copyright protection.

2. RIGHT OF ACCESS IN LEGISLATIVE DEVELOPMENT

The GDPR entered into force on 25 May 2018. It replaced the DPD in force from 13 December 1995. Both legal acts define the principal rights of data subjects and both recognised the right of access by the data subject. The DPD acknowledged the right of access in Article 12 (a) and the GDPR stipulates the right of access in Article 15. Providing brief legislative history of the right of access of data subject is important for this article in order to interpret its compatibility with the terms IP and copyright.

The legislative development of the right of access in the EU was introduced 18 years after adopting the DPD. In January 2012, the European Commission introduced a new legislative proposal[8] and on 11 June 2015,

[7] Article 29 Working Party. (2016) *Guidelines on the right "to data portability"*. 16/EN WP 242 rev.01. Brussels: Directorate C of the European Commission, pp. 9–10. Available from: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233 [Accessed 19 September 2018].

the Council of the EU published the amended version of the proposal.[9] The paragraphs of the Council's version which are relevant for the scope of this paper were proposed in Article 15 (1b) and (2a) as follows:

"(1b) On request and without an excessive charge, the controller shall provide a copy of the personal data undergoing processing to the data subject."

"(2a) The right to obtain a copy referred to in paragraph 1b (…) shall not apply where such copy cannot be provided without disclosing personal data of other data subjects or confidential data of the controller. Furthermore, this right shall not apply if disclosing personal data would infringe intellectual property rights in relation to processing of those personal data."

The Article 15 and paragraphs (3) and (4) of the GDPR currently in force set forth the form and restriction of the right of access by the data subject as follows:

"3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form."

"4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others."

With regard to development of the copy of personal data currently used in the GDPR, the draft of the Article 15 (1b) above referred to the form of the controller's response on the right of access request as copy of the personal data undergoing processing, which represented a different approach compared to the wording of the DPD (*communication*

[8] European Commission. (2012) *Proposal for the Regulation 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' (General Data Protection Regulation)*. COM(2012) 11 final. Available from: http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf [Accessed 19 September 2018].

[9] Council of the European Union. *Proposal for the Regulation 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' (General Data Protection Regulation).* ST-9565-2015-INIT. Available from: http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf.

in an intelligible form) and the Commission's GDPR proposal wording (*communication of the personal data undergoing processing*).

With respect to the violation of rights and freedoms of others, the paragraph (2a) above enumerated in the normative part of the proposal which rights and freedoms may be affected the right of access by data subject. The paragraph (2a) provided that the right does not apply if disclosing personal data would infringe IP in relation to processing of those personal data. It is important to stress that paragraph (2a) did not specify whose IP rights (data controllers, others or data subjects) might be violated. However, the Article 15 (4) of the GDPR is more general and limited because relevant areas of law are not explicitly named (at least not in the normative provisions of the GDPR) and it refers only to the rights and freedoms of others. Therefore, it might be concluded that the GDPR does not provide any possibility for data controllers to deny access to personal data because of the infringement of their copyright. Similarly, the Article 13 (1) (g) of DPD limited the right of access with protection rights and freedoms of data subject and others.[10] The corresponding Recital 63 to the Article 15 (4) of the GDPR sets:

> *"That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software."*

These rights need to be considered by data controller before the copy is provided to the data subject, but this Recital also stipulates that

> *"the result of those considerations should not be refusal to provide all information to the data subject."*

The issues of (in)compatibility with copyright of other parties than data controllers with the impact of limiting the right of access is discussed further from the point of quantity and quality of personal data that should be provided in the copy.

[10] Article 13 (1) DPD: *"Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard: [...] g) the protection of the data subject or of the rights and freedoms of others."*

3. COPYRIGHT PROTECTION OF PERSONAL DATA

In order to answer question about copyright protection of personal data as such, the question of data controllers' property right over obtained personal data must be addressed. The response to this question has implications for the quantity and quality of personal and non-personal data[11], which have to be provided by data controllers in copy.

The Technical report prepared by the European Commission's in-house science service sums up that the Database Directive[12] gives

> *"some limited property rights to data collectors, inspired by copyright but limited in scope by ECJ jurisprudence"*[13]

and that the GDPR gives some specific rights to data subjects, but refrains from defining a residual ownership in personal data.

The authors of the Technical report argue that residual rights[14], which are not included in the specific rights of the GDPR (e.g. right of access, right to data portability, lawfulness of the processing of personal data), accrue[15] to the data controller. In other words, if the ownership of personal data attributed to data subject is not specifically granted in the GDPR, the ownership right to the processed data is assigned to the data controllers.[16] However, the report sets forth also a counter-argument that *"privacy is a basic human right that cannot be alienated"*[17] in the meaning that natural persons possess the non-tradable rights specified in our context in the GDPR which

---

[11] Non-personal data for the purpose of this article are understood as data which are accompanying the personal data as it is requested in the Article 15 (1) of the GDPR, e.g. purpose of processing, recipients to whom data are disclosed, explanation about the source of data or storage period.

[12] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. *Official Journal of the European Union* (OJ L 77/20) 27 March. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31996L0009&from=EN [Accessed 19 September 2018].

[13] Compared with European Commission. (2017) *JRC Technical Report. The economics of ownership, access and trade in digital data. JRC Digital Economy Working Paper 2017-01*. JRC104756. p. 18. Available from: https://ec.europa.eu/jrc/sites/jrcsh/files/jrc104756.pdf [Accessed 19 September 2018].

[14] Op. cit., p. 17. Residual rights are defined in the report in the context of the economic literature on property rights *"as the rights that remain unspecific after specific rights have been assigned to the other parties."*

[15] Ibid.

[16] Op. cit., p. 18. The technical report argues: *"Exclusive data ownership thereby becomes a de facto right: I have the data and can effectively prevent others from accessing the data, therefore I am the owner of all residual rights not explicitly assigned away to other parties through specific legal or contractual rights."*

> *"reduce whatever rights the data collector has as a creator of a database of personal data."*[18]

Distinguishing between residual rights of data controllers and rights of data subjects explicitly granted by law, authors of the Report described reality of the legal situation created by the GDPR. The *de facto* ownership of personal data by data controllers who can prevent data subjects from accessing their personal data increased the potential harm to data subjects and disproportionate violation with their human rights without even being aware of violation of their rights.

Zech brings to the discussion about legal ownership of informational aspects of personality an analytical perspective.[19] He speaks about three layers of information – semantic, syntactic and structural. He explains that:

> *"Informational aspects of personality can be data, pictures, voice recordings or genetic information. Such information can either be defined on a semantic level (a certain fact about a certain person) or on a syntactic level (photographic pictures, voice recordings, gene sequences). Both are attributed to the original right owner on the semantic level, meaning they belong to the individual concerned."*[20]

It can be argued that the personal data as certain facts about natural persons are attributed to the data subject concerned.

Another question is whether the personal data as such are not protected also by copyright.[21] Personal data have similar nature as the ideas, facts or mathematical concepts, which are excluded from copyright protection. In general, it is doubtful whether the personal data on a semantic level

---

[17] Op. cit., p. 16.; Judgement of 17 July 2014, YS v. Minister voor Immigratie, Integratie en Asiel, C-141/12, and Minister voor Immigratie, Integratie en Asiel v. M.S, C-372/12, EU:C:2014:2081. paragraph 54 confirms that provisions of DPD *"in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of fundamental rights […]."*

[18] European Commission. (2017) *JRC Technical Report. The economics of ownership, access and trade in digital data. JRC Digital Economy Working Paper 2017-01*. JRC104756. p. 16. Available from: https://ec.europa.eu/jrc/sites/jrcsh/files/jrc104756.pdf [Accessed 19 September 2018].

[19] Zech, H. (2015) Information as Property. *JIPITEC*, 6, pp. 192–197. Available from: https://www.jipitec.eu/issues/jipitec-6-3-2015/4315/zech%206%20%283%29.pdf [Accessed 19 September 2018].

[20] Op. cit., pp. 195–196.

[21] Article 9 (2) of the *Trade-Related Aspects of Intellectual Property Rights (TRIPS)*, 15 April 1994. Available from: https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm [Accessed 19 September 2018] says: *"Copyright protection shall extend to expressions and not to ideas, procedures, methods of operation or mathematical concepts as such."*

could be considered as literary work in the sense of qualifying for copyright protection, because they are usually insubstantial to be classified as a result of intellectual effort or usually have no degree of originality. Zech considers copyrighted information as syntactic information such as pictures or video showing data subjects, because copyright protects expressions *"as opposed to the free content (ideas) which qualifies as semantic information."*[22] The Technical report mentioned above came to a similar conclusion that data are not protected by copyright.[23]

According to Zech, the third layer represents the information contained in a physical carrier, such as CD or printed books.[24] Structural level refers to real property right of physical object, which is owned by the holder of this carrier. The electronic or printed copy of the personal data undergoing processing could be classified as real property right owned by the holder of the copy. Based on the circumstances, the holder might be data controller or data subject. The Article 15 (3) of the GDPR obliges data controllers to use processed personal data and create copy as an object on syntactic level and provide it to the data subject as a physical object. Understanding the copy created on the basis of the right of access in this context is a core requirement in order to discuss the copy as a subject matter of copyright protection.

To sum up, the human rights argument, in connection with Zech's three--level information model, could lead to the conclusion that personal data belong to data subject or in other words are intangible property of an individual person to whom they concern. However, the explicit recognition of the property (ownership) of personal data as such is missing in the EU legal framework. This grey area may be misused by data controllers if they try to reduce the number of personal data listed in the copy in order to restrict the overall picture about processed personal data[25] and consequently the right of access of data subject could be limited.

---

[22] Zech, H. (2015) Information as Property. *JIPITEC*, 6, p. 196. Available from: https://www.jipitec.eu/issues/jipitec-6-3-2015/4315/zech%206%20%283%29.pdf [Accessed 19 September 2018].

[23] European Commission. (2017) *JRC Technical Report. The economics of ownership, access and trade in digital data. JRC Digital Economy Working Paper 2017-01*. JRC104756. p. 8. Available from: https://ec.europa.eu/jrc/sites/jrcsh/files/jrc104756.pdf [Accessed 19 September 2018].

[24] Zech, H. (2015) Information as Property. *JIPITEC*, 6, p. 192. Available from: https://www.jipitec.eu/issues/jipitec-6-3-2015/4315/zech%206%20%283%29.pdf [Accessed 19 September 2018].

[25] E.g. in cases when data controller is not able to justify the lawfulness and purpose of personal data processing.

In terms of copyright protection, there is probably no legal argument for data controllers to refuse to provide a copy because of copyright infringement of personal data on the semantic level. However, in case of pictures or videos of data subjects, data controllers have to determine whether the copyright holder is data subject or someone else. If the picture was provided to data controller by data subject who is the author of the picture, the access right to the picture has to be provided. In case the author is not a data subject (e.g. the picture was uploaded on the social network by third person and data subject was tagged on the picture), it is not acknowledged by the GDPR if data controllers have obligation to acquire IP rights from third parties in order to provide right of access to data subjects.

4. COPY – PHYSICAL OBJECT AS A SUBJECT MATTER OF COPYRIGHT

This part describes a process of creating a copy of personal data according to the GDPR as a starting point for the discussion about a copy (physical object) as a subject matter protected by copyright.

First of all, the GDPR is applicable only to those controllers, who are processing personal data. These controllers process personal data, which are structured to specific criteria relating to individuals[26] in a filing system. The concept of a filing system in the DPD/GDPR is unique for the data protection and the definition is not comparable to generally known concept of database or electronic file. Filing system is a structural set of personal data accessible based on specific criteria (centralised, decentralised or distributed on geographical or functional basis).[27] The filing system contains structured and easily accessible personal data.

After receiving a request for access, the data controllers need to search for processed personal data of the requested natural person in filing systems, summarise matched data and provide copy of the data to the data subject. Carey added that

[26] See Recital 15 and 27 of the DPD, Recital 15 of the GDPR.
[27] See Article 2 (c) of the DPD, Article 4 (6) of the GDPR.

> *"when dealing with requests for access, data controllers are obliged to provide the information constituting the personal data, rather than the documents containing the data."*[28]

Similarly, CJEU in its decision in *YS v. Minister voor Immigratie and others*[29] explains that the form of communication on the basis of Article 12 (a) DPD is not the right to obtain a copy of the document or original file containing the data. However, data controller could decide to provide copy of the document or the original file and the CJEU concluded that in this case, other information or data in such copy must be redacted. It is important to add that each copy needs to be obligatorily accompanied with other data[30] e.g. about the purpose of processing, recipients to whom the data are disclosed, explanation about the source of data or explanation of the logic involved in automatic processing of data, storage period etc. Moreover, provided information must be concise, intelligible, using clear and plain language etc.[31]

The result of the right of access in the GDPR has two ways of interpretation: copy created as a summary of personal data or copy of original document with personal data.[32]

The data protection law obliges the data controllers to implement the right of access by providing copy, which fulfils all requirements described above. However, the question is whether copy which fulfils all GDPR's requirements, could be protected by copyright. On the contrary, it is not possible to argue that all future copies of the summary of processed personal data are automatically excluded from the copyright protection. Otherwise, there is no need for the Article 15 (4) in the GDPR. Moreover, Recital 63 of the GDPR requires that the qualifying criteria for the IP

---

[28] Carey, P. (2009) *Data Protection, A Practical Guide to UK and EU Law*. 3rd ed. New York: Oxford University Press, p 134.

[29] Judgement of 17 July 2014, YS v. Minister voor Immigratie, Integratie en Asiel, C-141/12, and Minister voor Immigratie, Integratie en Asiel v. M.S, C-372/12, EU:C:2014:2081, paragraph 58.

[30] See Article 15 (1) of the GDPR.

[31] See Article 12 (1) of the GDPR.

[32] Due to the limited scope of the Article, second form – a copy of the document or original file – is not being further discussed as possible subject matter of copyright protection. However, there might be cases when copy of the whole document is provided to data subject, e.g. list of marks, health documentation, emails. Such document may be protected by copyright as literary or artistic work. Therefore, before the copy of the document is provided to data subject, the controller must consider the authorship of the work. It is also possible that the author of the document is data subject or the third party. In latter case, the data controllers need to acquire approval to reproduce and distribute the work to data subjects.

protection of others needs to be assessed on the case by case basis by data controllers before the copy is provided to data subject. Therefore, discussion below provides arguments about copy being subject matter protected also by copyright.

4.1 COPY PER SE PROTECTED BY COPYRIGHT

Subject matter protected by copyright is the work created by the author. Švidroň summarised that the criteria for the work were as follows:

> *"1. literary, scientific or artistic expression of the work;*
>
> *2. intellectual creation;*
>
> *3. the work is objectively expressed, which enables repeating sensual perception."*[33]

Applying the above criteria to a copy of personal data, it could be considered:

Ad. 1: Copy of personal data might be a list of structured personal data, which provides information about the content of their life to data subject (e.g. copy of personal data from social platform wall). Such copy could be identified as literary work by data controller. The threshold necessary to qualify copy as a copyrighted work is its originality in creation of its author/data controller.

Ad. 2: Data controller (usually a commercial entity) can be an author or right holder of such copy because of her/his input in terms of creativity, in finding, selecting, organising and presenting relevant personal data forming a summary of personal data for each data subject requesting access. Along this line of reasoning, the Recital 63 does not allow to refuse to provide all information to the data subject. In practice this means that data controllers are always obliged to create (original) copy with some personal data or information. The data controllers may choose from different techniques or use of computer software to adopt the copy. Each copy provided to data subject from data controller could be different in a sense of original organisation/structure/arrangement or format

[33] Švidroň, J. (2000) *Základy práva duševného vlastníctva*. Bratislava: JUGA, pp. 69–72. Compare also with the judgement of 16 July 2009, Infopaq International A/S v. Danske Dagblades Forening, C-5/08, EU:C:2009:465, paragraphs 34–50; Judgement of 1 December 2011, Eva-Maria Painer v. Standard VerlagsGmbH, C-145/10, EU:C:2011:798, paragraph 87; Judgement of 22 December 2010, Bezpečnostní softwarová asociace – Svaz softwarové ochrany v. Ministerstvo kultury, C-393/09, EU:C:2010:816, paragraphs 45–49.

of the order/layout of personal data and other information. The formative freedom of data controller put in copy might represent his "personal touch".[34] Under the given scenario, the copy themselves as a subject matter of copyright protection could be protected as a collective work or a database. The Article 2 (5) of the Berne Convention[35] could protect copy as a compilation. However, personal data are not protected by copyright as literary or artistic works as it was argued in part 3 of this paper, therefore copy as such seems not to be protected as the compilation. The Berne Convention sets also criterion that the selection *and* arrangement of compilation's content constitutes intellectual creation. Compare to the Article 3 (1) of the Database Directive the required criterions for copyright protection are more general. The database is protected by copyright if the selection *or* arrangement of content of database constitutes the author's own intellectual creation. Moreover, the copyright protection of database does not extent to the content. If the copy *per se* could be protected by copyright, such protection is likely to be stipulated by the database protection which is analysed in part 4.2 of this paper.

Ad. 3: Article 15 (3) of the GDPR requires to provide a copy in writing or by electronic means. Therefore, such copy is objectively expressed for sensual perception.

In principle, copy of personal data (understood in a sense of the structure of data) created on the basis of the right of access in the GDPR could be protected by copyright. This conclusion was not excluded by the CJEU, which ruled that

> *"the format of SAS Institute's data files might be protected, as works, by copyright under Directive 2001/29 if they are their author's own intellectual creation."*[36]

---

[34] Compare with the judgement of 1 December 2011, Eva-Maria Painer v. Standard VerlagsGmbH, C-145/10, EU:C:2011:798, paragraphs 87–94.

[35] The Article 2 (5) of the *Berne Convention for the Protection off Literary and Artistic Works* says: "*Collections of literary or artistic works such as encyclopedias and anthologies which, by reason of the selection and arrangement of their contents, constitute intellectual creations shall be protected as such, without prejudice to the copyright in each of the works forming part of such collections.*" Berne Convention for the Protection off Literary and Artistic Works, 19 November 1984. Available from: http://www.wipo.int/wipolex/en/treaties/text.jsp?file_id=283693 [Accessed 19 September 2018]

[36] Judgement of 2 May 2012, SAS INSTITUTE v. World Programming Ltd, C-406/10, EU:C:2012:259, paragraph 45.

Another theoretical conflict between IP and data protection identifies Margaret Ann Wilkinson whose approach regards the Canadian jurisdiction. She argued that the right of access and subsequent right to obtain rectification of personal data may interfere with the copyright interests of the creators of the records because only creators have the right to make any change to their work. She recognises the moral right of the creator to the integrity of the work.[37] Developing further the moral right of the creator to the integrity of the work, argument could be found in the Article 29 Working Party Guidance on the right to data portability which explains:

> *"The right to data portability is not a right for an individual to misuse the information in a way that could be qualified as an unfair practice or that would constitute a violation of intellectual property rights."*[38]

That would imply that also in the EU if a copy is considered to be protected by copyright, such protection could limit the right of data subject to rectification or erasure (known as right to be forgotten) of personal data because data controllers have moral rights attributed to the copy e.g. to object modification or derogation of their work.[39]

Further, the obligation to provide copy under the GDPR could be seen as a reproduction of a protected work existing in the filing system of data controller and creating another work from the filing system. The accuracy of this argument might be supported by the CJEU, 2009, *Infopaq International A/S v. Danske Dagblades Forening* decision. The CJEU discussed whether the reproduction right extended to the reproduction of 11 words extracts. The Court concluded that the 11 consecutive words constitute reproduction under the meaning of Article 2 of Directive 2001/29/EC, but the determination if elements of reproduction of the words expressed author's own intellectual creation is kept for the decision of national court. Otherwise, there has been no case law to date regarding this issue, which

---

[37] Wilkinson, M.A. (2001) The Copyright Regime and Data Protection Legislation. In: Ysolde Gendreau (ed.). *Law Publications*. Cowansville, Les Editions Yvon Blais Inc., p. 88. Available from: http://works.bepress.com/ma_wilkinson/17/ [Accessed 19 September 2018].

[38] Article 29 Working Party. (2016) *Guidelines on the right "to data portability"*. 16/EN WP 242 rev.01. Brussels: Directorate C of the European Commission, p. 12. Available from: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233 [Accessed 19 September 2018].

[39] See Article 6bis (1) *Berne Convention for Protection off Literary and Artistic Works*, 19 November 1984. Available from: http://www.wipo.int/wipolex/en/treaties/text.jsp?file_id=283693 [Accessed 19 September 2018].

will exclude conclusion that copy of personal data *per se* is not eligible subject matter of copyright protection.

However, state-of-the-art technology makes copyright protection of the copy more theoretical question. Technological development of the Internet enables creation of copy without any human intervention (as computer-generated works). Therefore, data controller could not claim authorship in case a copy is generated by the automatic computer program. This situation might in some jurisdictions conflict with the definition of authorship in copyright protection.[40] Moreover, copy of similar structure/ arrangement is usually provided to each data subject, whose data are processed in the filing system for reasons of simplifying the creative process of the copy from data controllers' point of view. Such copy reflects almost no intellectual effort or original creativity of data controller. Finally, there is a difference in the purpose of copyright and right of access. The aim of copyright is to advance *"authorial autonomy and cultural diversity."*[41] On the other hand, the copy under the GDPR is created by the data controller for the benefit of one individual data subject with the aim to provide her/him control which personal data are processed by the data controller. Under the described circumstances, copy *per se* will not qualify for copyright protection.

To sum up, the European Commission Staff Working document dealing with machine-generated and industrial data states that these data

> *"do not benefit from protection by other intellectual property rights as they are deemed not to be the result of an intellectual effort. Results of data integration, analytics, etc. can be protected, on the other hand, as a result of a protection given to the intellectual effort made into the design of the data integration process or the analytics algorithm (software)."*[42]

---

[40] See Article 13 (1) Slovak Copyright Act No. 185/2015 Coll., which defines Author as natural person who created work. On the other hand, Article 9 (3) UK Copyright, Designs and Patents Act 1988 sets that: *"case literary, dramatic, musical artistic work which is computer-generated, author shall be taken to be person whom arrangements necessary for creation work are undertaken."* This may be programmer another person. Similarly, Guadamuz, A. (2017) *Artificial intelligence and copyright*. [online] WIPO Magazine. Available from: http://www.wipo.int/wipo_magazine/en/2017/05/article_0003.html [Accessed 19 September 2018] presented legal opinion that: *"There are two ways which copyright law can deal with works where human interaction is minimal non-existent. It can either deny copyright protection for works that have been generated computer it can attribute authorship such works to creator program."*

[41] Goldstein, P. and Hugenholtz, B. (2010) *International Copyright, Principles, Law, and Practice*. 2nd ed. Oxford University Press, p. 7.

The Articles 15 (3) and (4) of the GDPR can be understood as the legislator's intention not to determine eligibility for copyright protection for the copy *per se* or personal data as such, but for the intellectual effort invested into the design of the personal data integration process or software, on which computer program operates and from which the copy is generated. Consequently, in case the right holder of the computer program is the data controller, she/he could not claim that the copy is infringing her/his IP rights, because such copy is not infringing the rights or freedoms of others which is the condition set in the Article 15 (4). The right of access in the GDPR could be understood as the legal obligation to grant access or license to the requesting data subject even though the rights and freedoms of data controllers might be infringed by providing the copy of personal data to data subjects.

4.2 COPY PROTECTED AS DATABASE

The Database Directive in Article 1 (2) defines database as

> *"a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means."*

It is important to emphasize that computer software making or operating the database is not subject of the Database Directive protection.[43] The Database Directive provides two types of protection – copyright and *sui generis*. Databases are protected by copyright if the selection or the arrangement of content is the intellectual creation of an author himself/herself.[44] *Sui generis* right (protecting economic investment of the maker of the database) is not copyright or other IP right. Goldstein and Hugenholtz described the *sui generis* right as being similar to neighbouring rights of phonogram producers and film producers.[45]

---

[42] European Commission. (2017) *Commission Staff Working Document free flow data and emerging issues European data economy, Accompanying document, Communication Building European data economy*, SWD.(2017) 2 final. Brussels, p. 19. Available from: https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy [Accessed 19 September 2018].

[43] Article 1 (3) Database Directive.

[44] Article 3 (1) and Recital 15 Database Directive.

[45] Goldstein, P. and Hugenholtz, B. (2010) *International Copyright, Principles, Law, and Practice*. 2nd ed. Oxford University Press, p. 239.

Maker of database must substantially invest either in obtaining, verification or presentation of the content.[46]

Personal data processed by data controller may qualify for the protection under the Database Directive. Data controllers usually collect and store personal data of all data subject in data files in the form of databases. The collection is classified as database when it is arranged in a systematic or methodical way and is individually accessible by electronic means. The CJEU in the decision *Fixtures Marketing Ltd v. Organismos prognostikon agonon podosfairou AE (OPAP)*[47] specifies that the term "database" is defined in terms of its function, which distinguishes a database from other collection of materials providing information. The function of database contained technical means such as electronic, electromagnetic or electro--optical processes, index, a table of contents, or a particular plan or method of classification, which process the data of which the database consists and allow the retrieval of any independent material contained within it.[48] We are of the opinion that copy created on the basis of Article 15 (3) of the GDPR could be treated as reproduction of original electronic database or extraction of a part of database, because without the described functionality of electronic database, the data controller is not capable to organise personal data for the accessibility by data subject.

However, the electronic databases of personal data will usually not qualify for the copyright protection of the Database Directive, because the criteria of author's own selection or arrangements of content of the database is not met.[49] This conclusion is confirmed by the CJEU decision in *Football Dataco Ltd and Others against Yahoo! UK Ltd and Others*.[50]

---

[46] See Article 7 (1) Database Directive.

[47] Judgement 9 November 2004, Fixtures Marketing Ltd v. Organismos prognostikon agonon podosfairou AE (OPAP), C-444/02, EU:C:2004:697, paragraphs 29–32.

[48] Functional criterion *sui generis* right further described CJEU Fixtures Marketing Decision paragraph 43 as: "*expression 'investment […] verification […] contents' database must be understood to refer to resources used, with view to ensuring reliability information contained that database, to monitor accuracy materials collected when database was created and during its operation. expression 'investment […] presentation contents' database concerns, for its part, resources used for purpose giving database its function processing information, that is to say those used for systematic methodical arrangement materials contained that database and organisation their individual accessibility.*"

[49] See European Commission. (2016) Legal study Ownership and Access to Data. European Commission DG Communications Networks, Content & Technology, Osborne Clarke LL.P, p. 13. Available from: https://publications.europa.eu/en/publication-detail/-/publication/d0bec895-b603-11e6-9e3c-01aa75ed71a1 [Accessed 19 September 2018].

[50] Judgement 1 March 2012, Football Dataco Ltd and others against Yahoo! UK and others, C-604/10, EU:C:2012:115.

The CJEU ruled that the criterion of originality (as a stamp of its personal touch) is not met

> *"when the setting up of the database is dictated by technical considerations, rules or constraints which leave no room for creative freedom."*[51]

The eligibility for this criterion by the original database of data controller may not be met and the same may analogically apply for the copy of processed personal data. The level of originality required for selection or arrangement of content of databases (structure of database) is the same as it is required for the copy *per se* discussed in the previous 4.1 part of the paper.

The *sui generis* right is the right intended for protection of investment in obtaining, verifying or presenting the data or the content of database.[52] The main defining criterion for the protection of this kind of database is an investment (qualitative or quantitative and substantial). The substantial investment is assessed on the basis of human, financial or technical resources necessary for obtaining, verification or presentation of the content of database. The data controller, who is processing personal data in the filing system, might be eligible for *sui generis* protection of his/her database. In this case, the data controller has the right for extraction (as reproduction) and re-utilisation (understand as making available to the public) of the whole or a substantial part of database. Creating copy of personal data from database protected by *sui generis* right by data controller (maker of database) is extraction of the database. However, the right of access on the basis of Article 15 (3) of the GDPR does not deprive the maker of database of the *sui generis* rights because the act of extraction is not adversely affecting rights and freedoms of third parties only the rights attributed to the maker of database. Article 15 (4) of the GDPR limits the right of access only in case the right to obtain copy affects the rights and freedoms of others.

Even though, the *sui generis* right of the maker of database is in conflict with the right of access authorised by the GDPR, the *sui generis* right could not stand in a way of the access right under the GDPR.

---

[51] Op. cit., paragraph 39.

[52] Compare with Recital 40 Database Directive.

4.3 ACCESS RIGHT INFLUENCED BY COMPUTER PROGRAM PROTECTION

The Computer Program Directive[53] protects only the expression[54] of computer program (software). Since the conflict between the copyright protection of software in the context of protecting rights of others (not data controllers) and the right of access is explicitly mentioned in the Recital 63 of the GDPR, the software protection should be incompatible with the copy of personal data. The next part discusses if and to what extent is the access to personal data conflicting with the copyright protection of software.

As it is suggested in the Paragraph 4.1 above, protection of the copy is based on the copyright protection of software, on which computer program operates or from which the copy is generated and accessible. There are at least two scenarios of possible clash of the two rights.

Firstly, in practice, the right holder (author) of the computer program may decide not to provide copy because of his/her exclusive right – reproduction, defined in article 4 (1) (a) of the Computer Program Directive as:

> *"the permanent or temporary reproduction of a computer program by any means and in any form, in part or in whole; in so far as loading, displaying, running, transmission or storage of the computer program necessitate such reproduction, such acts shall be subject to authorisation by the right holder."*

E.g. in machine learning scenario, the data controllers may face an issue how to provide all available personal data, which are processed, about the data subjects together with the logic involved in such processing.[55] The issue may be caused by lack of knowledge of data controllers about processing operations[56] and the easiest way how to fulfil the right of access

---

[53] Directive 2009/24/EC European Parliament and Council 23 April 2009 legal protection computer programs. *Official Journal European Union* (OJ L 111/16) 5 May. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0024&from=EN [Accessed 19 September 2018].

[54] See Article 1 (2) Computer Program Directive.

[55] Article 15 (1) (h) GDPR.

[56] See Jánošík, J. (2017) *Transparency machine-learning algorithms is double-edged sword.* [online] welivesecurity. Available from: https://www.welivesecurity.com/2017/11/13/transparency-machine-learning-algorithms/ [Accessed 19 September 2018], where it is stated: *"Yes, other citizens' rights introduced expanded GDPR, like right to object to profiling, right to obtain copy personal data gathered, right to be forgotten — can all be costly to comply with. But many companies are finding themselves incapable providing an explanation results their personal data processing. And worse – they often simply can't figure out how to comply with this GDPR-imposed obligation."*

is to provide a copy of algorithm concerned. Creating such copy may qualify as exclusive act of partial reproduction of computer program.[57]

Second scenario may arise, if data controllers provide the electronic copy (consisting only of personal data) in a special format of software, which is not accessible to data subjects.[58] Consequently, copy cannot be opened by Microsoft Excel or Word installed in majority of computers owned by data subjects. In order to gain access to the copy, data subjects need to buy another computer program, which may be sold by data controllers themselves. In case data subjects do not have the right to use this software the possibility to open copy is refused on grounds of copyright protection of computer program.

The right of access in data protection may conflict with the Computer Program Directive if third parties' rights would be infringed. Both above--described scenarios might be considered as marginal cases, but they constitute possible arguments for data controllers, when they intend to limit access to personal data.

5. BALANCING EXCLUSIVE RIGHTS

The discussion in previous parts of this article focuses on possible conflicts between right of access and copyright. Both rights encompass values for their beneficiaries. They are recognised and well established in their legal frameworks and in the Charter of Fundamental Rights of the European Union (hereinafter "Charter").[59] In case of conflict of rights, Article 15 (4) of the GDPR obliges data controllers to balance these two fundamental rights with the rights and freedoms of others.

The task of balancing rights requires comparing/weighing opposing interests and deciding, which prevails. The Recital 63 of the GDPR permit

---

[57] SeeJudgement 2 May 2012, SAS INSTITUTE v. World Programming Ltd, C-406/10, EU:C:2012:259, paragraph 43: *"[...] should be made clear that, third party were to procure part source code object code relating to programming language to format data files used computer program, and that party were to create, with aid that code, similar elements its own computer program, that conduct would be liable to constitute partial reproduction within meaning Article 4 (a) Directive 91/250."*

[58] This scenario may contradict with Article 15 (3) GDPR which requires that *"information shall be provided commonly used electronic form."* However, situation when data subjects could not afford to buy even commonly used software because remuneration software copyright holders. GDPR should extent requirement to commonly used and freely obtainable software order to strengthen its technological neutrality.

[59] See Article 17 (2) *Charter Fundamental Rights European Union*, 26 October 2012, (2012/C 326/02) Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN [Accessed 19 September 2018], which guaranteed protection of IP and second sentence Article 8 (2) recognized everyone's right access to data which has been collected concerning him her, and right to have it rectified.

to exercise the power of balancing rights to data controllers. Data controllers act as gatekeepers, who decide on the quantity and quality of personal data provided to the data subject. This is a "tool" chosen by the legislator in data protection framework for determining the rights and freedoms of data subjects or third parties. However, each balancing of the interests and rights involved will depend on the circumstances of an individual case and needs to be exercised on case by case basis.

The practical example of the balancing exercise is described in the Opinion of Advocate General connected with the Article (7) (f) of the DPD.[60] The balancing exercise was weighing, whether to provide personal data of taxi driver to injured party from the police administrative decision for issuing civil proceeding by injured party. The Advocate General Bobek suggested balancing nature and sensitivity of the requested data (their degree of publicity, age of the data subject) and the gravity of the offence committed.

As it may be understood from the above example, balancing or weighing of competing interests by data controllers is a challenging requirement.[61] The discussion about copy as a subject matter of copyright protection shows that there are relatively rare circumstances, when the copy meets requirements of copyright protection. The GDPR provides data controllers with the option of refusing the full access to the processed personal data in a form of copy because of the rights of others. Consequently, the lawfulness of refusal is difficult to be verified by data subjects. The ability to neutrally weigh all interests at stake is vested in Data Protection Authorities, who might need to become also copyright law experts.

6. CONCLUSION

The subject matter of Article 15 (3) of the GDPR – copy of personal data – may infringe copyright protection of the data controller who is usually the right holder/author of the copy. According to our findings, the conflict with copyright protection could not deprive the data subject of the right

[60] Opinion Advocate General 26 January 2017, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA 'Rīgas satiksme', C-13/16, EU:C:2017:43, paragraphs 67–69.

[61] They need to compare positive benefits and effect restrictive act with its negative effect fundamental right. Positive interest third parties might be seen protecting their business models when processing and trading with personal data. Harm caused to data subject might have implication to data subject private life e.g. automated decision made algorithm could lead to negative legal effect data subject personal life.

of access. The copy of personal data is not infringing the rights or freedoms of others which is the limitation of the right of access sets in the Article 15 (4) of the GDPR. The proper and frequent application of the right of access by data subjects will increase interplay between copy of processed personal data and copyright protection and should prove this conclusion.

From data controllers' point of view, copyright protection of works of others[62] represents a simple argument how to limit the quality and quantity[63] of personal data provided on the basis of the right of access. Therefore, we are of the opinion that the copyright law will prevail over the right of access. Firstly, because these two rights as discussed above may be incompatible. Secondly, the data controllers are primarily responsible for balancing conflicting rights and neutral balancing exercise could only be applied by the Data Protection Authorities. Thirdly, the case law of the CJEU regarding this issue will need to be developed because the copy as a result of access right may be considered as a new element in data protection law introduced by the GDPR.

Possible solutions which will enable exercising the right of access in the form of copy without a risk of IP or copyright infringement claims are as follows:

(i) to create exception for data controllers. The exception will acknowledge providing personal data (e.g. videos or pictures) without consent of the right holder for exercising the right of access. The new exception could be limited to the use of the copy only for the private (or household) purposes of data subjects and for exercising rights of data subjects under the GDPR;

(ii) to include the obligation for data controller to provide also reasons of the refusal of providing copy which rights and freedoms of third parties were balanced by the data controller. The information about conflicting rights will increase legal certainty for data subjects. Data subjects will better assess whether the act of data controller was legitimate with consequence of smaller number of cases submitted to the Data Protection Authorities.

---

[62] Copyright protection works others is other than copyright protection held data controller.

[63] This discussion, compare with Recital 63 GDPR: *"[...] result those considerations should not be refusal to provide all information to data subject [...]"*.

The compatibility of the right of access with copyright protection of other parties poses a lot of open questions which were partially discussed in the paper, sometimes only briefly mentioned. In the near future, data subjects need to use the right of access, wait for its application by data controllers and finally case law of the CJEU will have to provide comprehensive answers.

LIST OF REFERENCES

[1] Article 29 Working Party. (2016) *Guidelines on the right "to data portability"*. 16/EN WP 242 rev.01. Brussels: Directorate C of the European Commission. Available from: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233 [Accessed 19 September 2018].

[2] *Berne Convention for the Protection off Literary and Artistic Works*, 19 November 1984. Available from: http://www.wipo.int/wipolex/en/treaties/text.jsp?file_id=283693 [Accessed 19 September 2018].

[3] Bygrave, L. A. (2015) Information Concepts in Law: Generic Dreams and Definitional Daylight. *Oxford Journal of Legal Studies*. 35, (1), pp. 91–120. Available from: http://ojls.oxfordjournals.org/content/35/1/91 [Accessed 19 September 2018].

[4] Carey, P. (2009) *Data Protection, A Practical Guide to UK and EU Law*. 3rd ed. New York: Oxford University Press.

[5] European Commission. (2017) *Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Accompanying the document, Communication Building a European data economy*, SWD. (2017) 2 final. Brussels. Available from: https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy [Accessed 19 September 2018].

[6] *Copyright Act 2015*, SI 185/2015. Slovak Republic. In Slovak.

[7] *Copyright, Designs and Patents Act 1988 (c. 48)*. United Kingdom of Great Britain and Northern Ireland. London: HMSO. In English.

[8] *Charter of Fundamental Rights of the European Union*, 26 October 2012, (2012/C 326/02) Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN [Accessed 19 September 2018].

[9] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs. *Official Journal of the European Union* (OJ L 111/16) 5 May. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0024&from=EN [Accessed 19 September 2018].

[10] 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. *Official Journal of the European Union* (OJ L 281/31) 23 November. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN [Accessed 19 September 2018].

[11] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. *Official Journal of the European Union* (OJ L 167/10) 22 June. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001L0029&from=EN [Accessed 19 September 2018].

[12] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. *Official Journal of the European Union* (OJ L 77/20) 27 March. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31996L0009&from=EN [Accessed 19 September 2018].

[13] Goldstein, P. and Hugenholtz, B. (2010) *International Copyright, Principles, Law, and Practice.* 2nd ed. Oxford University Press.

[14] Guadamuz, A. (2017) *Artificial intelligence and copyright*. [online] WIPO Magazine. Available from: http://www.wipo.int/wipo_magazine/en/2017/05/article_0003.html [Accessed 19 September 2018].

[15] Jánošík, J. (2017) *Transparency of machine-learning algorithms is a double-edged sword*. [online] welivesecurity. Available from: https://www.welivesecurity.com/2017/11/13/transparency-machine-learning-algorithms/ [Accessed 19 September 2018].

[16] European Commission. (2017) *JRC Technical Report. The economics of ownership, access and trade in digital data. JRC Digital Economy Working Paper 2017-01*. JRC104756. Available from: https://ec.europa.eu/jrc/sites/jrcsh/files/jrc104756.pdf [Accessed 19 September 2018].

[17] Judgement of 16 July 2009, Infopaq International A/S v. Danske Dagblades Forening, C-5/08, EU:C:2009:465.

[18] Judgement of 1 December 2011, Eva-Maria Painer v. Standard VerlagsGmbH, C-145/10, EU:C:2011:798.

[19] Judgement of 17 July 2014, YS v. Minister voor Immigratie, Integratie en Asiel, C-141/12, and Minister voor Immigratie, Integratie en Asiel v. M.S, C-372/12, EU:C:2014:2081.

[20] Judgement of 9 November 2004, Fixtures Marketing Ltd v. Organismos prognostikon agonon podosfairou AE (OPAP), C-444/02, EU:C:2004:697.

[21] Judgement of 2 May 2012, SAS INSTITUTE v. World Programming Ltd, C-406/10, EU:C:2012:259.

[22] Judgement of 1 March 2012, Football Dataco Ltd and others against Yahoo! UK and others, C-604/10, EU:C:2012:115.

[23] Judgement of 22 December 2010, Bezpečnostní softwarová asociace – Svaz softwarové ochrany v. Ministerstvo kultury, C-393/09, EU:C:2010:816.

[24] Judgment of 6 November 2003, Bodil Lindqvist, C-101/01, EU:C:2003:596.

[25] Judgment of 29 January 2008 Productores de Música de España (Promusicae) v. Telefónica de España SAU, C-275/06, EU:C:2008:54.

[26] Judgment of the Court of 24 November 2011 Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), C-70/10, EU:C:2011:771.

[27] European Commission. (2016) *Legal study on Ownership and Access to Data*. European Commission DG Communications Networks, Content & Technology, Osborne Clarke LL.P. Available from: https://publications.europa.eu/en/publication-detail/-/publication/d0bec895-b603-11e6-9e3c-01aa75ed71a1 [Accessed 19 September 2018].

[28] Opinion of Advocate General of 26 January 2017, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA 'Rīgas satiksme', C-13/16, EU:C:2017:43.

[29] Polčák, R. (2016) Informace a data v právu. *Revue pro právo a technologie*, 7 (13), pp. 67–91. Available from: https://journals.muni.cz/revue/article/view/4946 [Accessed 19 September 2018].

[30] European Commission. (2012) *Proposal for the Regulation 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' (General Data Protection Regulation).* COM(2012) 11 final. Available from: http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf [Accessed 19 September 2018].

[31] Council of the European Union. (2015) *Proposal for the Regulation 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' (General Data Protection Regulation).* ST-9565-2015-INIT. Available from: http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf [Accessed 19 September 2018].

[32] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2017 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. *Official Journal of the European Union* (OJ L 119/1) 4 May. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN [Accessed 19 September 2018].

[33] Švidroň, J. (2000) *Základy práva duševného vlastníctva*. Bratislava: JUGA.

[34] *Trade-Related Aspects of Intellectual Property Rights (TRIPS*), 15 April 1994. Available from: https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm [Accessed 19 September 2018].

[35] Wilkinson, M.A. (2001) The Copyright Regime and Data Protection Legislation. In: Ysolde Gendreau (ed.). *Law Publications*. Cowansville, Les Editions Yvon Blais Inc., pp. 77–100. Available from: http://works.bepress.com/ma_wilkinson/17/ [Accessed 19 September 2018].

[36] Zech, H. (2015) Information as Property. *JIPITEC, 6*, pp. 192–197. Available from: https://www.jipitec.eu/issues/jipitec-6-3-2015/4315/zech%206%20%283%29.pdf [Accessed 19 September 2018].

MUJLT Official Partner (Czech Republic)

ROWAN LEGAL, advokátní kancelář s.r.o.
www.rowanlegal.com/cz/

Cyberspace 2017 Partner

Wolters Kluwer ČR, a. s.
www.wkcr.cz

Cyberspace 2017 Partner

Zákony pro lidi.cz

Zákony pro lidi - AION CS
www.zakonyprolidi.cz

Cyberspace 2017 Media Partner

PRÁVNÍ PROSTOR.CZ
www.pravniprostor.cz

Notes for Contributors

Focus and Scope

Masaryk University Journal of Law and Technology (ISSN on-line 1802-5951, ISSN printed 1802-5943) is a peer-reviewed academic journal which publishes original articles in the field of information and communication technology law. All submissions should deal with phenomena related to law in modern technologies (e.g. privacy and data protection, intellectual property, biotechnologies, cyber security and cyber warfare, energy law). We prefer submissions dealing with contemporary issues.

Structure of research articles

Each research article should contain a title, a name of the author, an e-mail, keywords, an abstract (max. 1 500 characters including spaces), a text (max. 45 000 characters including spaces and footnotes) and list of references.

Structure of comments

All comments should contain a title, a name of the author, an e-mail, keywords, a text (max. 18 000 characters) and a list of references.

Structure of book reviews

Each book review should contain a title of the book, a name of the author, an e-mail, a full citation, a text (max. 18 000 characters) and a list of references.

Structure of citations

Citations in accordance with AGPS Style Guide 5th ed. (Harvard standard), examples:

Book, one author: Dahl, R. (2004) *Charlie and the Chocolate Factory*. 6th ed. New York: Knopf.
Book, multiple authors: Daniels, K., Patterson, G. and Dunston, Y. (2014) *The Ultimate Student Teaching Guide.* 2nd ed. Los Angeles: SAGE Publications, pp.145-151.
Article: Battilana, J. and Casciaro, T. (2013) The Network Secrets of Great Change Agents. *Harvard Business Review*, 91(7) pp. 62-68.
Case: *Evans v. Governor of H. M. Prison Brockhill* (1985) [unreported] Court of Appeall (Civil Division), 19 June.
Citation Guide is available from: https://journals.muni.cz/public/journals/36/download/CitationguideMUJLT.pdf

Formatting recommendations

Use of automatic styles, automatic text and bold characters should be omitted.
Use of any special forms of formatting, pictures, graphs, etc. should be consulted.
Only automatic footnotes should be used for notes, citations, etc.
Blank lines should be used only to divide chapters (not paragraphs).
First words of paragraphs should not be indented.
Chapters should be numbered in ordinary way – example: "5.2 Partial Conclusions".

Submissions

Further information available at
https://journals.muni.cz/mujlt/about

LIST OF ARTICLES