Public Governance, Administration and Finances Law Review

in the European Union and Central and Eastern Europe

2.
2019

Public Governance, Administration and Finances Law Review Vol. 4. No. 2. (2019) • 5–15.

10.53116/pgaflr.2019.2.1

Articles

Administrative Liability for Causing Damage to Selected Components of the Environment

Branislav Cepek*

* Branislav Cepek, Associate Professor, PhD, Paneuropean University in Bratislava, Faculty of Law, Institute of Public Law. (e-mail: branislav.cepek@paneurouni.com)

Abstract: The article deals with one of the most important and recent issues of the contemporary law of the Member States and the EU in the field of environment, which is criminal liability for environmental crimes which serves as a tool for promoting environmental protection. Environmental law can be divided into two basic types of environmental liability for damage to the environment and liability for damage. Liability for environmental damage is divided into civil liability for damage as well as liability of the public for ecological damage. A special case is liability for historical damage. The Directive on torts is divided into criminal liability and administrative liability. In this paper, the author focuses on the analysis of the contemporary Czech tort law in the field of biodiversity protection and considers several aspects of this a *de lege ferenda* issue.

Keywords: environmental law; administration; law; liability for damage to the environment

1. Introduction

In connection with the legal-theoretical research into the subject matter of environmental liability, the legal science, before the adoption of Act No. 17/1992 Coll. on Environment, drew attention to a number of specific features of the regime of administrative and legal liability allowing, within the *de lege ferenda* considerations, to "incorporate" the provisions related to compensation, or more precisely, to restoration of environmental loss. Professional legal literature deals mostly with the issue of imposing individual types of sanctions.

In the following article, my intention is to give an analysis of the Slovak legal arrangements of liability in tort in the field of biodiversity protection, further, to compare it partly with the Czech legislation and consider some aspects of this issue *de lege ferenda*. I choose liability in tort in the field of biodiversity protection of the ecosystems because it ranks among one of the most important environmental components, where the most scientific research has been done into, but it is also one of the most sensitive components regarding the change in environment. Biodiversity is, in a broader sense, the diversity of species of

the living organisms (plants, fungi, animals and one celled organisms of the living world); we do not discuss only those species that are generally known.

In situ protection remains the most effective approach towards biodiversity protection. It means protection of the ecosystems and natural habitats, including maintaining and restoring viable species populations in their natural habitat. An important part of *in situ* protection is the management of specially protected areas of national and international importance, ensuring the ecological networks of functional habitats, including the restoration of destroyed habitats and the conservation of species within natural habitats.[1]

In the Slovak environmental law, the general regulation of administrative and legal liability for administrative offences in environmental protection is contained in Act No. 17/1992 Coll. on Environment, namely in the section called "Liability for a breach of obligations while protecting the environment". Provision 28 sets forth the general regulation of sanctioning/punitive liability, i.e. liability in tort. A sanction, at the set amount, can be imposed only on a natural person or legal person that is authorised to engage in business who while doing their activity causes some environmental harm by breaching laws, or fails to take measures that would lead to correction, or fails to warn some competent authority that there is a threat of harm to the environment. Pursuant to Section 2 of this provision, a fine may be imposed only within one year since the day on which the environmental authority ascertained the breach of obligations, but no later than three years since the date on which the breach occurred. However, environmental law does not regulate the jurisdiction of the state sanctioning authorities under the cited provision, and thus the practical application of this provision is practically excluded. However, the need for such a provision is rather arguable, especially in the view of the fact that laws in question contain specific provisions which regulate the breach of obligations in each of the environmental sectors.[2]

2. Protection of Biodiversity under Special Provisions

For the specific actus reus of administrative offences, it is necessary to investigate in special legal regulations, namely in the area of sources of environmental law (especially Act No. 543/2002 Coll. on Nature and Landscape Protection) and further (although now only in the "remnants") in Offences Act.

Offences defined in this Act, can be divided according to the level of complexity of legislation in relation to protection into:

a) *specific offences,* which can be further subdivided into general § 45 and segmental § 35
b) *generally designed,* for example § 46.

In the field of biodiversity protection, it is possible to consider, under the special part of Offences Act, the so-called offences, namely offences in the field of agriculture, hunting and fishing. This is the category of offences against individual environmental components, which can, however, have a significant impact on the protection of biodiversity, especially on the ecosystem and species protection. Finally, residual offences can be applied in order to achieve the protection of biodiversity, namely the offences in the field of environmental protection, and the so-called other offences against order in administration.

The mutual proportion of offences in the field of environmental protection and its individual components regulated by special laws and offences in Offences Act is expressed by the speciality principle.

From the viewpoint of enforcing the principle of liability of a tortfeasor within liability in tort in the area of administrative and legal liability related to the protection of biodiversity, it is necessary to tackle both, individual issues of fact of administrative torts and their definition, sanctions and protective measures and conditions of cessation of liability.

Only a natural person can commit an offence. Article 6 of the Offences Act stipulates that a person who has acted or should have acted on behalf of a legal person is liable for the breach of obligation imposed on that legal person, and in case of an injunction, it is a person who awarded an order for such proceedings.

When we take a closer look at the individual provisions of laws in the area of biodiversity, then we find out that there are no problems with identifying a person who committed an offence.

Liability in tort of natural persons in the conduct of running their business and legal persons is based on the principle of strict liability. The absence of the element of fault differs by liability in tort of natural persons in the conduct of running their business from another liability in tort of natural persons.

In case of legal entities, environmental laws, unlike natural persons, do not distinguish whether they are commercial or non-commercial entities. Consequently, even associations can also, theoretically, commit an administrative offence, in whose articles of associations the protection of natural environment is the main scope of their business activity.[3]

The subjective side of the offence is mandatorily investigated only when it comes to offences, and in case of other administrative offences committed by legal and natural persons who run a business, the element of fault is not investigated. Liability is therefore strict, and the entity cannot be relieved from liability by their reference to contractual agreements or by breach that was caused from the side of their contractual partner.

In terms of environmental protection and in terms of the preventive function of liability modes, it is important to classify administrative offences according to the consequence of unlawful conduct. If the consequence lies in endangerment of protected values and interest, then we speak about the offences of criminal threat, in case the consequence lies directly in the breach of these values, then we speak about breach offences.

In practice, however, we can determine another group of administrative offences of a minor importance. It is unlawful conduct, but it does not reach the level of seriousness of the offence of criminal threat. Although this type of conduct does cause the breach of legal regulations, it is not a type of breach that will pose threats to the environment, but rather it is a breach of obligations related to the organisation of protection of a certain interest, therefore we speak about offences of administrative nature.

For such offences, we could indicate a breach of duty to notice or the duty to report (unless, of course, it is not the duty to report some serious accident or emergency incident), further, a breach of duty to register, a breach of duty to pay fees or other financial deductions or payments, a breach of duty to monitor, and a breach of duty in relation to control authorities. However, the failure to comply with the said duties has no direct impact on threats to the environment.

Issues of the fact of administrative offences appear to a greater or lesser extent in the wording of many legal regulations in the area of biodiversity protection. Their number consequently also depends on the area which is regulated by the relevant legislation. Clearly, the largest number of them is in sections where a great emphasis is placed on monitoring activities, and therefore on keeping a variety of records and fulfilment of the duty of monitoring. A significant number of administrative offences can be also found in the legislation whose legal adjustments stem from the contents of international treaties.

In case of breach offences within the category of administrative offences, the consequence in the form of death of the object of an attack is directly implied. A typical example is killing of birds. Another consequence relates to damage, destruction, deterioration of state and so on.[4]

Some types of conduct are not considered to be unlawful, unless they cause a prohibited consequence defined by law. Interventions against pests, plant diseases and while taking hygiene measures are permitted by separate laws, but this conduct cannot endanger, over an acceptable limit, particularly protected components of nature.

Based on the inspiring ruling of the Czech Supreme Administrative Court, it is possible to document both, the issues of objective liability and the issues of proving the conduct and consequences of an administrative offence in the field of biodiversity protection. The said Court, in its ruling No. A 3 /2003-47, dated on the 24th of February 2005, held that the inadmissible use of organic or industrial fertilisers or any other chemical substantives is sufficient to fulfil the merits of the case of unauthorised interference with natural development of specially protected plant species, under the Nature and Landscape Protection Act; without, at the same time, the necessity of requiring the effect of destroying an individual, and a specially protected plant species. Even in case of another administrative offence, this is liability for unlawful conduct irrespective of fault.

Scientific literature dealing with the categorisation of the issues in the fact of administrative offences recognises, in practice, four types of categories. The most common type is defining the issues of fact by verbal description. The second *unlawful act by unlawful interference with the natural development of specially protected* case is a partial wording in combination with a reference to the provisions governing the duty which a liable person violated. For example, *"a nature conservation authority will impose a fine of up to the amount of € 7,000 on a natural person who commits an offence by damaging or destroying a cave and its part, or who violates other duties".*

The third case occurs when the issues of fact only refer to the relevant provision of the law which is sanctioned. For example, *"a natural person commits an offence if they sell or offer specimens in violation of the relevant provisions of Act No. 543/2002 Coll. on Nature and Landscape Protection".*

The fourth option concerns other (residual) facts. For example, *"a nature conservation authority will impose a fine of up to the amount of € 16,000 on a legal or natural person, if in the conduct of their business they commit an offence by [...] killing birds or keeping birds, except those that may be hunted, or keeping specially protected animals without permission, or if they otherwise unlawfully interfere with their natural development".*

Furthermore, in my view, it is also possible to distinguish cases where an act infringes directly some statutory provision, or it refers to the infringement of a specific

administrative act issued under the law or some directly effective EU regulation. For example, an *"administrative offence is committed by a natural or legal person – an entrepreneur who disposes of an exemplary species directly threatened by extinction in violation of an import license or another valid permit under this Act (Act No. 543/2002 Coll.) or under the regulation concerning trade in endangered species".*

From the principle of *nulla poena sine lege* results the requirement for some legal form of expression of the type and amount of sanction, the conditions and manner of their imposition, as well as considerations for the assessment of the sanction in a particular case. For sanctions to serve their purpose, they must be designed, in terms of their kind and amount, in a way to match the nature and gravity of unlawful conduct, considering the property and other benefits obtained by that unlawful conduct, and so on. Even in the case of sanctions, it is necessary to distinguish sanctions imposed for offences and sanctions imposed for other administrative offences, whereby the type and amount of sanctions is, in particular, in case of administrative offences different than in offences laid down by individual laws. In this respect, it is not possible to omit the general provision of Article 29 of the Act on Environment, under which fines or other measures are imposed for a breach of duties stipulated by these special regulations.[5]

In case of offences, the law in the area of biodiversity protection mostly imposes a fine as a form of sanction. However, under the Offences Act, other forms of sanctions may also be applied in a subsidiary way, which means, for example, giving a caution, or imposing prohibition of an activity and a thing forfeit. In particular, the latter two may be relevant in the field, for example, while regulating the trade in threatened animal and plant species. Exceptionally, in case of offences, in special laws, it is possible to come across another sanction form, different from fines. For example, under the Hunting Act, *"a government authority will impose a fine of up to the amount of € 1,200 on a hunting license holder who commits an offence by violating some hunting rule; it may impose a ban on activity for the period of up to two years; alongside the ban, the hunting license is withdrawn; at the same time it is possible to pronounce a thing forfeit".*

In case of other administrative offences committed by legal persons and natural persons who act as entrepreneurs, these groups of individuals are most likely to be fined, although there are other types of sanctions that can come into consideration, such as a ban on activity or a ban on farming.

Exceptionally, in case of offences, as well as in case of other administrative offences, it is possible to come across a recurrence in the area of biodiversity, which is a repeated breach of the same obligations. Usually, the relevant law combines repetition with a certain time limit. For example, under the Act on Zoological Gardens, *"for an offence or other administrative offence stated in the Section [...] a fine of up to the amount of € 200,000 may be imposed, if that offence has been committed repeatedly within the period of one year after the imposition of the fine on it".*

In the environmental protection legislation, other institutes of sanctioning nature than fines are also entrenched. Although they are often not labelled as sanctions, they undoubtedly are some form of punishment for a recipient, by virtue of their nature. An important thing is that these are the institutes that may also be involved as a result of a breach of an obligation imposed by law, and in this sense, they may be included in

the accountability scheme. An important element is, in most cases, also the public interest, which is also confirmed by the fact that the application of the instrument in question is not only permissible in connection with unlawful conduct, but often also in the absence of substantive conditions for the performance of certain activities or in the actual occurrence of the unlawful state. The confiscation or seizure of a thing does not preclude the simultaneous imposition of a fine.

In the area of biodiversity protection, we can come across the following types/tips:

1. instruments relating to entities – for example, in the form of authorisation or license withdrawal in the event of a serious breach of duties while performing special activities
2. instruments relating to activities of some place of business – usually in the form of bans, revocation, suspension or limitation of operation or refusal of an application
3. instruments relating to a thing – removal or seizure of a thing or a living animal that cannot be disposed of or kept. Typically, in the area of biodiversity protection, it involves a plant or an animal species, living or dead, or a product made from them, in case of unlawfully kept individuals within the category of particularly protected species, and these protective measures are implemented quite often[6]

The majority of the environmental protection laws, including the laws in the area of biodiversity, set deadlines in relation to the application of sanction liability. These are both of the subjective and objective nature. The Nature and Landscape Protection Act provides an exception to this, it regulates only the objective periods of time.

For example, *"a fine, under sections 1 and 2, may be imposed not later than three years from the date on which the unlawful conduct was committed".* It can come across as a failure of a lawmaker, but by looking back at the historical development of the legal adjustment of the Nature and Landscape Protection Act, we can come to a clear conclusion that this is an obvious intention in the stated examples.

The said Act, even before the Act on Regulation of Trade in Endangered Species came into force, contained the subjective period of time. However, after the Act on Regulation of Trade in Endangered Species had been amended, the said period was left out. This was probably due to the effort to facilitate a proceeding and to increase the possibility of imposing a timely fine.

The time limits for the imposition of a fine for committing an administrative offence are subject to preclusion, the passing of which is neither interrupted nor stopped as a matter of principle. The objective time limit is set only in case of offences. Provision 20 of Act No. 372/1990 Coll. on Offences, makes it impossible to deal with an offence if two years have passed since it was committed.

Some offences in the field of nature and landscape protection can also be qualified as criminal offences under the Criminal Code No. 300/2005 Coll., as altered and amended. To be precise, it concerns, in particular Article 300 on "threats and damage to environment", and Article 305 on "violation of plant and animal species protection", which are aimed at protecting the species of wild fauna and wild plants.

The conditions contained in these issues of fact are designed in a way to be consistent with the meaning of this general provision, and applicable to all objects of this crime (in

other words, to the environment as a whole and to all its components), not only to plant and animal life. Articles 300 to 305 have been amended and their purpose is to clarify the provisions of the Criminal Code in question in order to cover all the proceedings required by the Directive, and follow the established system of listed national, European and international sources of environmental law.

The typical feature of crimes against environment is that, apart from some exceptions, all provisions refer to other generally binding legal regulations.

Crimes of threats and environmental damage (Articles 300 and 301) have a "general character" compared to other provisions, which means that in this paper, other offences are in the subsidiarity or specialty relation to them, and a single-action concurrence between the crimes of threat and harm to the environment with these crimes is therefore excluded.

In case of a deliberate form of criminal offences of threat and damage to the environment (Article 300 Section 2), the offender is punishable, if he unlawfully builds a building in a protected area. The offender can be any natural person (general entity) as well as a legal person who is subject to criminal liability. From the point of view of the subjective element of crime, a criminal offence under Article 300 requires deliberate culpability; in other words, specific intent, in case of a criminal offence under Article 301, negligence is required.

Punishability of a crime of threat and a crime of causing harm to the environment under Article 300 may, upon fulfilment of relevant conditions, lapse by applying effective regret (Article 85).

Less serious interventions in the environment may be sanctioned pursuant to Article 45 of Act No. 372/1990 Coll. on Offences as offences, and pursuant to Article 28 of Act No. 17/1992 Coll. on the Environment as administrative offences.

In the year of 2014, in the field of biodiversity protection, Regulation (EC) of the European Parliament and of the Council of the EU No. 1143/2014 of 22 October 2014 on the prevention and regulation of the introduction or planting and the spread of invasive non-native species was adopted. The impacts of the spread and the effect of invasive non-native species on the biodiversity of geographically indigenous species and on natural ecosystems have been evident for a long time from the side of natural sciences – they pose one of the most serious *sources of threats to biodiversity*.

Article 30 Section 2 of the above-mentioned Regulation imposes an obligation on the Member States to lay down penalties for infringements of the provisions of this Regulation, provided that the Member States shall take all necessary measures to enforce these sanctions. The term *"all necessary measures to enforce these sanctions"* means, within the framework of the Slovak national law, the adoption of substantive and procedural standards in the field of liability in tort, including the determination of the powers of administrative or judicial authorities.[7]

However, Article 30 Section 2 of the above-mentioned Regulation does not explicitly determine whether administrative liability or even criminal liability arises. It only indicates that sanctions are to be imposed, it provides their demonstrative calculation in paragraph 3, and it only sets out what their functions should be like; which means that these sanctions should be effective, proportionate and have a deterrent effect. Sanctions under Article 30 should be mainly introduced in cases of a breach of obligations under Articles 7, 8, 9, 10, 16, 17, paragraph 20, 31 and Article 32.

From the point of view of the subjective aspect of the relevant type of unlawful act, it is possible to formulate both a deliberate and negligent act, and an omission to act, except for Article 7 where gross negligence is required. After the adaptation of Article 30 of the Regulation on the prevention and regulation of the introduction or planting and the spread of invasive non-native species within the Slovak national law, in my opinion, in the context of *de lege ferenda* considerations, there are two ways – legal liability will be regulated not only in the area of administrative law, but also in criminal law.

When it comes to the imposition of proper punishment, of course, offences committed by natural persons and other administrative offences committed by legal and natural persons, entrepreneurs who are subject to strict liability – come into consideration. In terms of sanctions, the types of sanctions calculated demonstratively correspond to Article 30 Section 3, in other words fines, further we speak about the seizure of invasive non-native species as well as the immediate suspension or withdrawal of a permit in accordance with Article 8.

When it comes to entrenching administrative punishment in case of offences, two options are in place – it is of course, the legal adjustment of the Offences Act (where the common arrangement for different cases would be an advantage); the second option would be the amendment process of sanctioning provisions in each individual segmental law which regulates this subject matter, for example in the Forest Act, Nature and Landscape Protection Act, Water Act, Hunting Act, etc.).[8]

From the perspective of other administrative offences of legal entities and natural persons who are entrepreneurs, only one option is possible, providing that there is the absence of a code listing other administrative offences, the option is to amend the sanctioning provisions in each individual segmental law that regulates this subject matter.

It is clear from the point of view of determining the relevant state administration authorities that in case of offences either general regulation of the authorities under the Offences Act will come into question, or the relevant control and sanctioning authorities will have to be determined in individual segmental laws. The already existing authorities, particularly the Slovak Inspectorate of the Environment and the state veterinary authorities, are in consideration. In the territory of national parks and protected landscape areas, the respective national park administration authorities could exercise these competences. Local authorities could be omitted because of the high level of expertise in the issue of control and imposition of sanctions and corrective remedies.

The area of criminal law is also considered, without doubts, but there is a question whether the requirement of the above-mentioned EU regulation is criminal liability, or whether it can be deduced. Such a requirement is absent. On the other hand, pursuant to Article 30 Section 2, sanctions that are determined must be effective, proportionate and deterrent. The expression "deterrent" could also mean the introduction of criminal liability.

Similar wordings are commonly found in the case law of the Court of Justice of the European Union, and in other sections of environmental law (CITAS, nature and landscape protection within the NATURA 2000 scheme, protection of the Earth's ozone layer, etc.), where, in the past, the European Union law enabled the introduction of criminal liability concept into the Slovak domestic law.[9]

As long as the Slovak Republic makes a decision to do so, it will be necessary to amend the Criminal Code, in order to complete the *actus reus* of a crime that deals with the most serious violation of the regulation, but only such proceedings that will not be determined as offences or other administrative offences at the same time – because such a duplication would be inadmissible. Sanctions could be then imposed, in particular, for the violation of the following obligations:

- failure to take preventive and regulatory measures
- failure to take measures to restore damaged ecosystems
- failure to make a notification
- breach of a relevant decision
- unlawful possession, or possession of an individual

This occurs, of course, on the condition that there is no duplication with offences or other administrative offences. Criminal offences must be defined in accordance with the *ultra ratio* principle.

The offender would be a natural person. It should be also considered whether it is necessary to establish such a crime also for legal persons. Again, duplication will not be possible, if there is a correctly defined administrative offence of legal entities in the relevant segmental laws.

From the point of view of giving the precise wording to the *actus reus* of crimes set out in the Slovak Criminal Code, it is possible to refer to the violation of a directly effective EU Regulation on the prevention and regulation of the introduction or planting and the spread of invasive non-native species, which is acceptable from the viewpoint of criminal law, for example this is the way how CITAS offences in the Czech Penal Code are dealt with.

In terms of specific sanctions in the area of criminal liability, it can be stated that the sanctions set out in the demonstrative calculation in Article 30 Section 3 on IND, can be also employed in the Criminal Code, and possibly, in the Act on Criminal Liability of Legal Entities. Since it is not an exhaustive calculation, it is possible to consider also introducing other sanctions, for example in the form of a custodial sentence or a ban in the area of environment protection.

In case of determining competent authorities, this subject matter, when it comes to adaptation, is no longer valid, since we speak about the already established criminal justice system.

3. Conclusion

I hold the view that *de lege ferenda* should be more focused on unification of the conditions of administrative punishment in the area of administrative liability for other administrative offences of legal persons and natural persons, who are entrepreneurs in the field of species biodiversity protection. Furthermore, the precise wording of the *actus reus* of

offences and other administrative offences in the area of administrative punishment in case of persecution of threatened species of wild animals (especially when placing poisonous baits), and stating the conditions of liability in tort for the import and transport of invasive non-native species, including their regulation.

Definitions should concern not only amendments made to laws in the area of administrative liability and liability for environmental protection, but also the level of criminal law (Criminal Code and criminal liability of legal entities). The amendment process should be based on both the normative requirements of European legislation in the area of biodiversity protection, and at the same time, it should take into account the needs of the domestic practice.

References

1 Richard B. Primack, Pavel Kindlmann, Jana Jersáková, Úvod do biologie ochrany přírody [Introduction to the biology of nature protection] (Praha, Nakladatelství Portál, s.r. o., 2011).
2 Soňa Košičiarová, *Ekologická ujma a škoda v práve životného prostredia* [Ecological Damage and Damages in Environmental Law], 120 (Bratislava, Vydavatelské oddelenie Právnickej fakulty UK, 1997).
3 Milan Damohorský et al., *Právo životního prostředí, 3. vydání* [Environmental Law, 3rd edition] (Prague, C. H. Beck, 2010).
4 Branislav Cepek et al., *Environmentálne právo. Všeobecná a osobitná časť* [Environmental Law – General and Special Part, 1st edition] (Pilsen, Aleš Čeněk, s.r. o., 2015).
5 Helena Prášková, *Východiska budoucí právní úpravy správního trestání* [Background of the Future Legal Regulation of Administrative Punishment] (Prague, Právní praxe, 1999).
6 Lilla Garayová, Bioethics and Law in the Postmodern Society, 37–45, in *Wissenschaftszeitschrift des Studienzentrums Hohe Warte* conference proceedings (Sonderausgabe 2014 December).
7 Milan Damohorský, Legal Responsibility in Environmental Protection, 34, in *Acta Universitatis Carolinae – Iuridica,* no. 2 (2015).
8 Peter Potasch et al., *Zákon o priestupkoch – Veľký komentár* [Law on Offences – Big Commentary] (Bratislava, Eurokodex, 2016).
9 Lilla Garayová, Sources of EU Law, 59–62, in *Selected Sources of Law – Past and Current Perspectives* (Bratislava, Paneurópska vysoká škola, 2019).

Public Governance, Administration and Finances Law Review Vol. 4. No. 2. (2019) • 16–29.

10.53116/pgaflr.2019.2.2

The Right to Informational Self-Determination in the Context of Selected Judicial Decisions and Practical Background[1]

Andrea Erdősová*

* Andrea Erdősová, JUDr., PhD, Paneuropean University in Bratislava, Faculty of Law, Institute of International Law. (e-mail: andrea.erdosova@paneurouni.com)

Abstract: It is essential to address in particular the comprehensive prevention of breaches of the right to informational self-determination and whether the persons concerned are aware that they "voluntarily agree" to pass on their identity information to third parties. It is alarming nowadays what amount of private data are available at their disposal for companies or private persons regarding other persons and how easy it seems to obtain this data. In today's information age and the era of more advanced use of artificial intelligence, it will be more necessary than in the past to define what the individual intended, what he agreed with, and what he eventually approved as data privacy.

In order to ensure the protection of the individual and his/her privacy, it is therefore necessary to respond to and refine the existing sources of law, especially to establish codes of ethics taking into account the modern technological and social development.

Keywords: ethics; informational self-determination; the right to privacy; personality rights; European Court of Human Rights; findings of the Constitutional Court; case law

1. Introduction

Primarily, the right of the informational self-determination originates in guaranteeing the freedom and dignity of individuals in relation to public authorities. Today, state power is not the only threat to law. Nowadays it seems easy for different subjects to gather without a problem huge amounts of information about individuals, especially for those such as Google, Facebook, Instagram, or Twitter. It might not be satisfactory to just consider how to protect someone effectively from the power handled by public authorities.

In order to ensure the protection of the individual and his/her privacy, it was therefore necessary to respond to and refine the existing legislation in this area, in particular at the European Union law level.[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) is one of the "new" means of protecting the privacy of individuals.[3] In the context of the protection of informational self-determination, the whole regulation is an important instrument for the protection of the right to

privacy, in particular through the so-called *Right to erasure ('right to be forgotten')* in Article 17 of the Regulation, which consists in the rights of the data subject[4] to obtain the deletion of personal data relating to him from the controller[5] without undue delay. The controller is then obliged to delete such personal data without undue delay if one of the enumerated reasons is fulfilled, allowing the data subject to request the deletion of his personal data published on the Internet (with or without his knowledge).

To what extent it is an effective means in the current technological development and possibilities of data and information backup on other media, it seems more than questionable. Therefore, we perceive these means rather than the mechanisms of derangement of one's own information identity, where, particularly in disputes concerning the protection of personality, the court will thus be able to see by consenting, verifying and examining what the individual has agreed to interfere to his/her right to privacy. Last but not least, today, more than in the past, it is also necessary to set general ethical boundaries of permissible interference from the perspective of exploitation of the artificial intelligence.[6]

2. The Meaning of Informational Self-Determination

The term "right to informational self-determination" (informationelles Selbstbestimmungsrecht) originated in the Federal Republic of Germany and its author is the Federal Constitutional Court (Bundesverfassungsgericht), which derived this right from Article 2(1) 12 in conjunction with Article 1(2) of the Constitution of Germany.[7] The term "self-determination" generally means the right to autonomy and independence. The essence of the right to informational self-determination is therefore the right of every individual to control information from his/her privacy so that he/she decides what facts about his/her surroundings will get known, who has them and how they will be used.

The Constitutional Court of the Slovak Republic knows this term, although it is used only very sporadically, i.a. judgment of the Constitutional Court of the Slovak Republic of 29 April 2015, no. PL. ÚS 10/2014-78, where its paragraph 89 defines as follows:

"The case law of foreign constitutional courts also takes a similar approach to privacy. For example, the Federal Constitutional Court of Germany, through the right to informational self-determination guarantees protection not only of the content of the information to be moved, but also protects the external circumstances in which it is carried out; location, time, subscribers, type and mode of communication, because knowing the circumstances of the communication made, in conjunction with other data, may itself indicate the content of the communication itself, and by examining and analysing this data, individual subscriber profiles can be constructed out of the communication.

[e.g. Decision of 27.7.2005, BVerfGE 113, 348 (Vorbeugende Telekommunikationsüberwachung) or 27.2.2008, BVerfGE 120, 274 (Grundrecht auf Computerschutz)]."

The ruling in question was a proposal by a group of Members of the National Council stating that the contested provisions of the Electronic Communications Act impose an obligation on electronic communications providers to keep traffic data, location data and

data of communicating parties from the date of communication for 6 months in the case of Internet connection, e-mail and Internet telephony, and for 12 months for other types of communication.

In the view of the group of deputies, "the introduction of the obligation to retain data pursuant to the above provisions constitutes a noticeable interference with private life, as it is a blanket surveillance of all Slovak citizens, regardless of their integrity and honesty. Every day, every person in Slovakia is obliged to record who he was calling, who he sent text messages and emails, when he did, where he was, what phone or service he used, how long the communication in question took, and many others. By combining this information, we can describe the movement of every citizen in Slovakia who uses a mobile phone or the Internet, predicting their behavior, circle of acquaintances, hobbies, health, sexuality, or other personal data and secrets [...] it is possible to compile the perfect personality, communication and movement profile of an individual, revealing a number of essential characteristics of his identity and behavior, in other words, reveal a substantial part of his privacy."

In its proposal, the group of deputies also points out that "according to the case-law of the ECHR", interference with private life "e-mail and telephone calls (ECtHR judgment in Klaas v. Germany), as well as finding telephone numbers of telephone persons or storing information that the person was calling with a person, all of them have to be considered as keeping the control or check over the mail and its content. It is irrelevant whether the data retained has been used or disclosed in any way (in particular the ECtHR judgment in Copland v. The United Kingdom). Infringement of fundamental rights, and hence private life, means not only immediate intervention (e.g. familiarisation with stored data), but also measures taken by public authorities from which it is foreseeable that they will result in a restriction of fundamental rights and freedoms".

According to the proposers, the contested provisions of the Electronic Communications Act "are in direct contradiction with the principle that fundamental rights and freedoms must be respected in substance and meaning, and restrictions can only be applied to a stated objective (Article 13(4) of the Constitution)". They further state that "the merits of any interference with fundamental rights and freedoms in a democratic and legal state are assessed on the basis of the cumulative fulfilment of three basic criteria, namely the legality, legitimacy and proportionality of such interference (Constitutional Court Findings, file no. I. ÚS 117/07, PL. ÚS 23/06, PL. ÚS 3/09, PL. ÚS 3/00, PL. ÚS 67/07)".

In a part of this petition, the Constitutional Court of the Slovak Republic granted the proposal about the breach of law.

Also i.a. in the decision of the Constitutional Court of the Czech Republic under no. Pl. ÚS 24/10, in which the court assessed the constitutionality of § 97 par. 3 and 4 of Act no. 127/2005 Coll. on electronic communications regulating the obligation of legal or natural persons providing a public communications network or publicly available electronic communications service to store traffic or location data, this court adopted and used the term "informational self-determination" as a doctrine contained in the above-mentioned Federal Constitutional Court decision and informational self-determination as follows:

"The primary function of the right to respect for private life is to provide space for the development and self-realisation of an individual personality. In addition to the traditional definition of privacy in its spatial dimension (protection of the dwelling in the broader sense of the word) and in the context of autonomous existence and public power undisturbed in social relations (marriage, family, society), the right to respect for private life fundamental decision – decided freely by the individual. In other words, the right to privacy also guarantees the right of the individual to decide at his/her own discretion to what extent, in what manner and under what circumstances should the facts and information about his/her personal privacy be made available to other entities. This is an aspect of the right to privacy in the form of the right to informational self-determination; guaranteed by Article 10 paragraph 3 of the Charter."

Pars pro toto two findings of the two constitutional courts serve as an example of the use of a term which, despite its extraordinary timeliness and, so to speak, material significance in disputes concerning the protection of personality and privacy, has still not been frequently used as a terminus technicus. This is peculiar, pointing out that in today's information age and the era of more advanced use of artificial intelligence, it will be more necessary than in the past to define what the individual intended, what he agreed with, and what he eventually approved as data privacy. In our view, this is also a key aspect of shifting the burden of proof to the operators, or creators or sponsors of the algorithms involved in setting up and using a wealth of information and data from our privacy.

However, even the national doctrine of the general courts does not leave the right to informational self-determination unnoticed. According to the order of the Supreme Court of the Slovak Republic (Order of the Supreme Court of the Slovak Republic of 18 February 2010, ref. No. 3 Cdo 137/2008), the right to privacy lies in the right of a natural person to decide independently whether and to what extend should the facts from his private life be made available to others or made public. The violation of the right to privacy is not only the unauthorised acquisition of knowledge about the privacy of a natural person, but also the unauthorised dissemination of this knowledge. The unauthorised interference with the right to privacy may significantly reduce dignity or seriousness in society, but this is not the only right required to demonstrate the seriousness of the harm to a natural person. Consequently, there is no procedural obligation to prove to the injured party that the unlawful interference had the effect of reducing his seriousness and dignity in society.

3. Strasbourg Doctrine

Although the European Court of Human Rights also does not directly and expressis verbis address the issue of self-determination, the basis of its earlier case law can still be used to answer the question of which data, information an individual has authorised or where was his legitimate expectations about the use and spread of these information, to what extent, location, time and for which range of recipients.

Paradigmatic in this context is the case of Max Rufus Mosley, Mosley v. United Kingdom,[8] who is known to the public as ex-president of the International Automobile Federation (FIA).

Briefly, on March 30, 2008, Sunday's newspaper *News of the World* published an article on the front page entitled "F1 chief had perverted Nazi orgies with five prostitutes". Ex-president of the International Automobile Federation was exposed as a secret sadomasochistic sexual pervert. The published text continued by describing the event and adding a few photos taken from a video recorded by one of the sex orgy participants, and the recording was pre-ordered and paid for. In addition, the extract from the record as well as the relevant photographs were accessible on the newspaper's website, where potential candidates could further disseminate them.

In the proceedings against the publisher of the tabloid, the complainant did not in fact object that the sexual sadomasochistic act had not occurred as was clear from the recordings and the text, but openly admitted that he had been professing this kind of sexual practice for years, but denied background act simulation with Nazi content. He alleged that the media had unlawfully interfered with his privacy, on the grounds that his private life was his personal affair and that the newspaper publisher had no relevant evidence, except for the presence of uniforms, a strange German accent in his speech and connotations to his father's fascist past and the direct relation of sexual orgies to Nazi ideology.

He requested that the footage of the video be immediately downloaded from the newspaper website. The applicant was successful in the national proceedings for the protection of his personal rights and was awarded damages of GBP 60,000 and GBP 420,000 with respect to costs. Mosley argued that the State failed to fulfil its positive responsibilities and had ensured a general obligation for publishers or journalists to seek prior consent from the person concerned.

In so doing, the complainant demanded that the ECtHR determine that newspaper publishers be required to notify the person concerned of the planned media coverage three days before publishing information that infringes the privacy of persons. Thus, the ECtHR also assessed the practical impact of the complainant's claim and found that there was no general obligation to pre-notify as such in any of the Member States' legal systems. On the other hand, some Member States require the data subject's consent to the publication of material relating to family life,[9] although in many cases they provide for exceptions to the publication of information relating to "public interest" issues (paragraph 62).

In paragraph 128 of the ECtHR, referring to the national decision, it recalled that any prior consent would not have any effect other than a penalty for not respecting it. A regulatory or civil sanction in the form of a fine would probably be a small incentive to avoid publication without the prior consent of the person concerned. This is all the more necessary to prevent the prohibition of publishing the article in question in the press because the person concerned has not given his consent to its publication. Moreover, as the ECtHR pointed out, these obstacles can also lead to censorship. The threat of criminal sanctions or punitive penalties may have a freezing effect in the field of political reporting and investigative journalism concerning the highly protected values of the Convention.

Information and video footage of Max Mosley were seen by hundreds of recipients and they had the opportunity to spread them further. Therefore, the response to the request to download video footage and prevent access to information was as follows: "The court must always be cautious when considering the real facts and the limits of what can be achieved [...]. However, in order to limit access to information by court order, it must be

remembered that information is so widely and generally accessible on public domains that such a court command would have practically no meaning. In traditional terminology, such a measure would be labelled "brutum fulmen". It is not appropriate for the court to make only blank gestures (paragraphs 34–35)."

For these reasons, the Chamber decided that Article 8 of the Convention had not been infringed in that case. In addition, what can be seen as the scope of the legitimate requirement can be summarised from one of the three decisions in the case of Caroline von Hannover, in concreto Hannover v. Germany, no. 59320/00.[10]

It can be inferred from the judgment in question that, although there is a public demand – in the case of a commercial interest in magazines – for the publication of photographs and articles, in the present case, everyone, even if known to the public, must have a "legitimate expectation" of protecting and respecting their private lives.

The judgment of the ECtHR on the basis of a complaint from the Princess of Monaco, Caroline von Hannover, is not only pointedly defining the so-called personality protection of "relative" (quasi) public persons, but it is also a sort of navigation system in the endless sea of the details of the private life searched from the prominent people. It will serve the press in a number of cases to distinguish between legitimate and well-known processing and further dissemination of information and details from the privacy of "celebrities". As J. Herczeg pointed out: "[...] the readers of the boulevard will not lose their stories, as the media behavior of these persons will also be important for assessing whether or not the intervention is justified. But in other words, one's own behavior will set the limits of legal privacy."[11]

This also applies, mutatis mutandis, to cases of confidentiality of data from the private sphere of a natural person subject to professional secrecy. Legal theory has clarified that "[...] when a patient himself publishes in the press or other mass media his own health condition stating the facts subject to confidentiality by the doctor, or when the patient himself discloses certain facts subject to confidentiality, and so they will exclude them from their personal privacy".[12]

On the other hand, Reid's legal opinion commenting on the ECtHR's judicial practice in this context cannot be overlooked. In its view, the mere fact that an individual is in a public place or that his personal data is publicly accessible to others on public domains does not necessarily preclude the application of Article 8 of the Convention. Like the person's legitimate expectations regarding their protected sphere of privacy, although significant, they are not necessarily the only determining factor in assessing the legitimacy of an intervention.[13] This also applies, mutatis mutandis, to the voluntary disclosure of information or guarantees of its later use.[14]

4. Informational Self-Determination of Minors in the Context of One Case

The situation where there is currently an Internet connection in virtually every home, even in the streets of cities, is making it even more difficult by the lack of general legal knowledge of what data are collected in the Internet environment, how they are used and to

what extent they are kept. The issue is also addressed by relevant psychological concerns, according to which a group of minors approaching adulthood are not even partially aware of the importance of protecting their privacy and informational self-determination and the consequences of its ill-considered sharing with third parties in cyberspace.

In addition, it is very common to find that the parents of minors also violate their right to informational self-determination by sharing their photographs or by publishing them in public places. This question was also addressed by the Supreme Court of the Czech Republic in its order of 12 December 2012, file no. 30 Cdo 3770/2011, which unequivocally ruled that unauthorised interference with the right to informational self-determination of a child could also be carried out by a legal representative, stating: "Protection under Section 11 of the Civil Code also includes images of a minor of "celebrities" who capture his daily and private activities for which there is no public interest, even if his or her legal representative is motivated by an incentive to attract public attention to himself or herself. [...] The appellant's argument that the consent of the legal guardian to the public dissemination of photographs and articles on minors that capture and map the child's privacy precludes the unlawful interference must be rejected. Article 16 of the Convention on the Rights of the Child[15] affords the child protection against arbitrary interference with his or her privacy, without distinction from where they are carried out. In other words, a child has the right to protection from arbitrary interference with his/her privacy, even if carried out by legal representatives (holders of parental responsibility)."

The right to informational self-determination is also related to monitoring the behaviour of individuals, which is no longer a dystopia, but an increasingly current reality, where there are certain algorithms of systems, of which the most familiar is the so-called "cookies". Modern software, however, cannot only read the behaviour and decision-making processes of an individual, but also over time his or her consumer preferences, thoughts, and motivations, giving rise to very interesting and relevant information for data collection. Worse, however, is the risk of interference with the right to privacy, in particular the right to informational self-determination, where the individual does not even know not only what data are collected about him/her, but also where and for what purposes he or she continues to use it. Installations of industrial cameras may also be another way of disrupting the individual's self-determination.

5. Industrial Cameras in a Legislative and Practical Framework

The emergence and existence of the first industrial cameras is associated with monitoring missile test launches in Nazi Germany in 1942. By technical improvement, we now have not only a larger number of camera systems but also an increase in the number of objects monitored by them. These are, for example, security cameras, which follow us when shopping, in underground garages, cameras at the entrance to the pub together with appropriate software, which can identify among the visitors known so-called "troublemakers", furthermore, those that recognise vehicle licence plates, but also camera surveillance through other devices that we accept on a voluntary basis, but eventually become an

undesirable burden. These include laptops, phones, tablets, game consoles, the Internet, video servers and viral videos.

In the United States, there has recently been a debate on the introduction of cameras with face recognition software,[16] which is mainly used by police forces in several countries. Cops are allowed i.a. to take a picture of a person with a mobile phone and immediately identify their identity and eventual criminal record or other personal information from various accessible databases. A very turbulent case of the right to privacy is the so called "Street View", which under this technology was designed in 2007 to monitor populated parts of the world.

It was tracking in about 12 countries collecting emails, passwords, photos and other personal information.[17] Related to this was a system creating a mapping of an increasing number of states through the so-called google maps, which also retrieves images captured by people in public places which allows them to find themselves online. This way, it is also possible to take a look at dwellings and private spaces. This may potentially undermine the right to privacy and, in these circumstances, the unauthorised use of personal data. The biggest commotion was caused by the maps in Italy, where they captured a high-ranking politician coming out of a public house.[18]

In many of the disputes that Google has encountered in connection with this technology, it has been argued that WIFI communication channels have allowed this data to be retrieved, making it publicly available to society. Finally, even in disputes where Google lost, monetary sanctions were negligibly small compared to the company's regularly high profits. In the context of privacy invasions through surveillance, or rather espionage,[19] there has to be mentioned the media-narrated case of Snowden's testimony, according to which there is a secret PRISM anti-terrorism program that allegedly allows the U.S. National Security Agency and the Federal Bureau of Investigation to retrieve texts, photographs or video-mails, chats, social networking, and phone calls around the world.[20]

We have a number of cases of violations of the right to privacy through camera systems, both at home and close to the border. Not long ago, the media resonated the case of a journalist from the Czech Republic, who protected his property against vandals with his own CCTV system, but CCTV did not allow the perpetrators to be detained and accused as evidence in court and acquitted the perpetrators. The damaged journalist was eventually sanctioned by the Office for Personal Data Protection of the Czech Republic for unannounced installation of the camera and unauthorised collection of personal data. On the basis of an analogous case, the Supreme Administrative Court of the Czech Republic even referred a question to the Court of Justice of the European Union.[21]

6. Public Versus Private

Finally, the right to informational self-determination is also a question of what information should be and for what purpose part of the monitoring, even if a person has not directly elected it, but the interest in monitoring has exceeded private interests and is rather perceived in the public good.

In one such case, the Regional Court in Brno upheld the lawsuit against the decision to place the camera on the ground floor of an apartment building at the entrance so as to capture the persons entering and leaving the house, thereby identifying the property better and in the aim to prevent stealing mailboxes. The court has rightfully held that by placing the camera at the entrance to the house against the plaintiff's will, the defendants rightfully infringed his right to privacy as a personality right within the meaning of Section 11 of Act No. 40/1964 Coll. Civil Code, as amended, hereinafter referred to as OZčr, as well as unlawful interference with the applicant's right to protection against unauthorised acquisition and collection of pictorial records pursuant to § 12 para. 1 OZčr.[22]

Since no legal licence has been given for this intervention and the installation of a CCTV system requires the consent of all residents of the apartment building, the court pursuant to § 13 para. 1 OZčr prohibited the acquisition and collection of video recordings and ordered the defendants to dismantle it. However, in this and similar cases, the problem is mainly focused on obtaining monitoring consent, as other cases assess cases in which the subject feels affected by the monitoring and therefore disagrees with the capture of premises owned or exercised by other related rights.

Pursuant to the aforementioned legislation, it would be necessary not only to obtain the consent of all potentially affected persons before installing a CCTV system, but also to place a visible space monitoring sign. If all residents of the dwelling house were to agree in unison, then it would seem difficult to assert that the monitoring affected the rights of visitors or other persons who found themselves in the dwelling without having a legal relationship with it. Assuming, of course, that the monitoring of this space could have anticipated what was clearly indicated. This obligation also creates space for labelling without being linked to an active system, i.e. it is only an assembly of non-functioning dummy devices.

However, they logically do not establish any real violations of law and their importance lies in the territory of purely preventive security measures. If we rely on the case law of the European Court of Human Rights, we find a number of explanations for what is considered a home, even though the concept of home is generally autonomous and according to the text of the European Convention on Human Rights[23] it can only be defined with great difficulty. In principle, it is a space that is a physically defined area where private and family life develops. However impersonal we would consider prima facie, for example, a hotel room, in the case of a homeless person who was paid for accommodation by the local authorities, it became home during his stay.[24]

However, the Court is not concerned with extending the right to home through the right to acquire or own property, but to place protection in respect of home without being able to undermine the right to use it. In particular, the intervention of competent authorities by confiscation, control or secret surveillance is prevented.[25] In Friedl v. Austria case decision, the Commission considered essential that the taking of photographs and the subsequent recording in the investigation file infringed the right to privacy, irrespective of the interests of a private or public nature behind the pictures taken.[26]

The Court has stated on several occasions that the mere fact that an individual is in the public domain or that data about him is widely available on public domains does not

automatically exempt from the application of Article 8 of the Convention. The Court accepts that there are a number of factors which may be considered in assessing whether there has been an infringement of the right to privacy.

The individual's reasonable expectations of possible interference with his or her privacy are certainly essential facts, but not exclusive. The same applies to the information provided by the parties concerned (right to informational self-determination).[27] To the same extent, it applies to e-mails and the Internet used at the workplace which are part of private autonomy, provided that the employee has not been notified by the employer on the possible monitoring of its manifestations.[28]

Finally, persons who are being prosecuted must not be excluded from the protection of privacy.[29] It can therefore be settled in the ECtHR case law that insofar as the purpose of obtaining information is to protect the public interest, whether it is the right to public information or the protection of collective security. Interference with the right to respect for private life are going to be considered less strictly than searching for information and details from private life. For this reason, the control of the exercise of a public function, the task of which is, for example, to maintain security and order in public places, also implies an obligation to suffer the capture of video recordings from the intervention.[30]

At the same time, it is clear from that judgment that the powers of public officials, in particular exercised in public and in contact with the public, may, and should be, directly subject to a control regime, which is an exercise of the right to information. Naturally, questions falling within the scope of the fundamental right to privacy of a natural person are not subject to such a legal regime. It is also necessary to carefully differentiate whether the attacks carried out in the sphere of personality rights were really directed against individuals or against the state authority of which they are representative.

"Given the above-mentioned differences between the State authority and the natural persons of which it is composed, it can be concluded that if an intervention is directed against a particular authority of the State, it cannot be inferred from this that such interference affects the personality rights of the natural persons of which a government body is composed, which does not mean that the authority concerned is also hit by this interference."[31]

The need for obtaining and storing information is generally not disputed as long as it is carried out under the auspices of a police investigation or security guarantee and is clearly based on legitimate objectives and is indispensable in a democratic society.[32] In addition, the necessity and procedural guarantees enjoy a wide margin of appreciation in national security measures.[33]

The question of the violation of the right to privacy in such cases has been answered in the earlier case-decision of the Commission, which in Hilton v. United Kingdom[34] has confirmed that security control per se does not affect private life, except for information pertaining to private life, which is subject to control.

It was a strictly individualised demonstration of the interference that caused direct interference with the right to privacy. However, the case law has evolved to more general assumptions, and thus, through a permanent court in particular, has established that the principle of "reasonable probability" will always be decisive in establishing whether

an individual is a subject of observation (reasonable likelihood). Indeed, it indicates that such measures are applicable to the person concerned or those that belong to the category of persons likely to be monitored. If he/she finds himself/herself in this category, then there is no longer any need to prove whether or not surveillance has or could affect private-sector attributes.[35]

In addition, the Court has established that public information falls within the scope of private life when it is systematically collected and stored in the files of the competent authorities, particularly where it relates to the distant past or is false or capable of significantly undermining a person's good repute.[36]

The perception of the existence of a specific subject is also significantly influenced by the nature of the activity per se, as was the case, for example, with Vanessa Redgrave,[37] who found a wiretapping device which, in her view, was placed by the Government. The suspicion was supported by the fact that the applicant was known both from controversial political cases and by belonging to the revolutionary party, and there existed an interest in tracking her in the past.

Another important criterion taken into account by the Court is the legality of the intervention. In this sense, judicial criteria are based on legality which refer to the presence and content of national legislation available and guarantee that the measures in question are reasonably foreseeable and protected against arbitration.[38] According to doctrine, the question of predictability is meant in terms of general guarantees of predictability of law, but this does not automatically represents that an individual will know in advance i.a. control procedures of special forces, as this could be the threat to the controls relating to national security interests. However, it must be pre-defined, what categories of people will be monitored, within what time limit, by what procedural mechanisms, how data will be further used, how they will be protected when communicating them to third parties, and the conditions under which records can or must be destroyed.[39]

The ECtHR case law focuses in particular on examining the adequacy and effectiveness of safeguards against misuse of information. On the other hand, it is not excluded that the alert in some form will persist later, sometimes despite or without the adoption of rules on the obligation to destroy it. This raises the association to the aforementioned Max Mosley case where the Court was i.a. forced to state that even downloading video footage and preventing official later distribution after the recording appeared on public domains does not prevent its misuse. Despite all this, forcing publishers, journalists to ask for prior approval of the publication leads to nothing and it solely can present nothing or means only an empty gesture.[40]

7. Conclusion

A few of these cases map out circumstances of the use of the institute of the right to informational self-determination, and although we see that it appears sporadically in both national and European Court of Human Rights rulings, we consider this could be one of the criteria for assessing both the rate of participation of a person affected by the rights of personality and the subsequent determination of the amount of non-material harm.

As can be seen from the text followed, informational self-determination is not always a question of delimiting the private sphere, and the autonomy of the individual in this context may be outweighed by the public interest, fulfilling the purpose of the public good, i.a. trying to maintain security, or preventing unrest, or a certain preventive-deterrent effect while maintaining public order.

References

1 This contribution is the result of the project implementation grant by the APVV No. 16-0588.
2 See more i.a. Elena Júdová, Ochrana slabšej strany – porovnanie európskeho a slovenského medzinárodného práva súkromného [Protection of the Weaker Party – Comparison between European and Slovak Private International Law], 17–31, in *Acta Iuridica Olomucensia,* vol. 9, no. 1 (2014).
3 Lilla Garayová, Regulácia voľného pohybu osôb v kontexte protiteroristických opatrení v EÚ [The Regulation of the Free Movement of Persons in the Context of Counter-terrorism Measures], 80–86, *Paneurópske právnické listy,* no. 1 (2018).
4 The expression "data subject" according to Article 4(1) of the regulation states that "personal data" means any information relating to an identified or identifiable natural person ("data subject"), an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
5 "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
6 See the document drafted by a panel of experts at the request of the European Commission (DG Research and Innovation) which aims at raising awareness in the scientific community, and in particular with beneficiaries of EU research and innovation projects. It does not constitute official EU guidance; the document was adopted on November 14, 2018, https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf (accessed 8 August 2019).
7 Ruling of the German Constitutional Court defining informational self-determination, http://sorminiserv.unibe.ch:8080/tools/ainfo.exe?Command=ShowPrintText&Name=bv065001 (accessed 8 August 2019).
8 Mosley v. United Kingdom, judgment of 10 May 2011, no. 48009/08, Complaints valid September 15, 2011.
9 Lilla Garayová, Odhad vplyvu Brexitu na voľný pohyb osôb [The Estimated Impact of Brexit on the Free Movement of Persons and Data], 51–62, in *Voľný pohyb osôb a vnútorný trh Európskej únie: vedecký zborník* (Bratislava, Paneurópska vysoká škola, 2018).
10 Hannover v. Germany, judgment of 24 June, 2004, no. 59320/00.
11 Jiří Herczeg, Případ Caroline von Hannover – zveřejnění fotografií ze soukromí prominentů, 877–880, in *Právní rozhledy,* no. 23 (2004).
12 Karel Knap et al., *Ochrana osobnosti podle občanského práva,* 4th substantially revised and supplemented edition, 24 (Linde Praha, 2004).
13 To this we associate, mutatis mutandis, the case of Friedl v. Austria, judgment of 31 January 1995, no. 15225/89, in which the Court did not find a violation of Article 8 of the Convention, even though the police photographed the complainant, but during a public demonstration and they remained anonymous without mentioning the name of the photographers.
14 Karen Reid, *A Practitioner's Guide to the European Convention on Human Rights,* 3rd edition, 483 (London, Sweet & Maxwell Ltd., 2008).
15 *Convention on the Rights of the Child,* adopted and opened for signature, ratification and accession by General Assembly Resolution 44/25 of 20 November 1989, entry into force 2 September 1990, in accordance with Article 49, www.ohchr.org/en/professionalinterest/pages/crc.aspx (accessed 8 August 2019).
16 *Technológia rozpoznania tváre a GDPR,* 9 March 2011, https://blog.canex.sk/2019/12/19/technologia-rozpoznavania-tvare-a-gdpr/ (accessed 8 August 2019).
17 Judgment of the Federal Supreme Court on Google Street View: Decisions on the processing of personal data, published August 2013, www.edoeb.admin.ch/datenschutz/00683/00690/00694/01109/index.html?lang=en; compare with David Streitfeld, Court Says Privacy Case Can Proceed Vs. Google, 11 September 2013, www.nytimes.com/2013/09/11/technology/court-says-privacy-case-can-proceed-vs-google.html (accessed 8 August 2019).

18 *Pohlad do zákulisia Google StreetView,* 1 November 2012, www.wesolyaniolek.com/pohlad-do-zakulisia-google-streetview/ (accessed 8 August 2019).
19 Lilla Garayová, *Spoločnosť proti terorizmu?* [Torture as a Just Means of Preventing Terrorism?] 360–364 (Plzeň, Aleš Čeněk, 2016).
20 *Super veľký brat? Fakty a mýty o tajnom programe PRISM,* 11 June 2013, https://zpravy.aktualne.cz/zahranici/supervelky-bratr-fakta-a-myty-o-tajnem-programu-prism/r~i:article:782171/ (accessed 8 August 2019).
21 *Nejvyšší správní soud: Nejvyšší správní soud položil předběžnou otázku Soudnímu dvoru Evropské unie* [The Supreme Administrative Court referred the question to the Court of Justice of the European Union for a preliminary ruling], 22 April 2013, www.nssoud.cz/Nejvyssi-spravni-soud-polozil-predbeznou-otazku-Soudnimu-dvoru-Evropskeunie/art/956 (accessed 8 August 2019).
22 See also *Ako GDPR nahliada na používanie kamerových systémov* [How GDPR views the use of camera systems], www.isecure.sk/sk/aktuality/monitorovanie-kamerovym-systemom-z-pohladu-gdpr.html (accessed 22 August 2019).
23 Convention for the Protection of Human Rights and Fundamental Freedoms, podpísaný 4. novembra 1950 v Ríme, hereinafter referred to as "Convention", O'Rourke v. United Kingdom, decision about admissibility 2001, no. 39022/97; see also David John Harris, Michael O'Boyle, Edward Bates, Carla Buckley, *Law of the European Convention on Human Rights,* 2nd edition, 380 (Oxford, Oxford University Press, 2009); Friedl v. Austria, 1995, no. 15225/89, compare with X. v. U.K., 9702/82 or Murray v. U.K., par. 84, 85, concerning data collection, fingerprints and photos by the police, also Chave née Jullien v. France, no. 14461/88, for obtaining and storing medical records or DNAs and Marper v. U.K., 2008, no. 30562/04 and 30566/04; Lupker v. Netherlands, 1992, no. 18385/91; Copland v. U.K., 2007, no. 62617/00, par. 42; Sciacca v. Italy, 2005, no. 50774/99, par. 29.
24 O'Rourke v. U.K., decision on admissibility by 2001, no. 39022/97.
25 David John Harris, Michael O'Boyle, Edward Bates, Carla Buckley, *Law of the European Convention on Human Rights,* 2nd edition, 380 (Oxford, Oxford University Press, 2009).
26 Compare with case X. v. U.K., 9702/82 or Murray v. U.K., par. 84, 85.
27 Lupker v. Netherland, by 7 December 1992, no. 18385/91.
28 Copland v. U.K., by 3 April 2007, no. 62617/00, par. 42.
29 Sciacca v. Italy, by 11 November 2005, no. 50774/99, par. 29.
30 See also the judgment of the Constitutional Court of the Slovak Republic of 5 January 2001, rec. II ÚS 44 / 00-133: "According to the legal opinion of the Constitutional Court, the exercise of his/her statutory duty of service by a public official – an employee of the municipal police – cannot be considered a part of the fundamental right to privacy or a manifestation of personal nature (pursuant to § 11 of the Civil Code) [...] these are diametrically opposed issues of the public and not the private sphere, which cannot in any way be considered a part of their fundamental right to privacy."
31 Judgment of the Supreme Court of the Slovak Republic of 27 March 2001, rec. no. M Cdo 46/2000.
32 Leander v. Sweden, of 26 March 1987, no. 9248/81, par. 49.
33 Ibid. par. 59.
34 Hilton v. U.K., of 6 July 1988, no. 12015/86.
35 Compare with Halford v. U.K. of 25 June 1997, no. 20605/92.
36 Rotaru v. Romania, 4.5.2000, č. sť. 28341/95 ods. 43–44.
37 Redgrave v. U.K., of 1 September 1993, no. 20271/92.
38 Lilla Garayová, Sources of EU Law, 59–62, in Andrea Erdősová, Lilla Garayová, Peter Potásch (eds.), *Selected Sources of Law – Past and Current Perspectives* (Bratislava, Paneurópska vysoká škola, 2019).
39 Karen Reid, *A Practitioner's Guide to the European Convention on Human Rights,* 3rd edition, 563 (London, Sweet & Maxwell Ltd., 2008).
40 Mosley v. U.K., of 10 May 2011, no. 48009/08, par. 34–35.

Public Governance, Administration and Finances Law Review Vol. 4. No. 2. (2019) • 30–51.

10.53116/pgaflr.2019.2.3

Information Security Awareness in Public Administrations at an International Level[1]

Lilla Garayová*

* Lilla Garayová, JUDr., PhD., Paneuropean University in Bratislava, Faculty of Law, Institute of International and European Law. (e-mail: garay.lilla@gmail.com)

Abstract: Privacy and data protection laws have changed significantly over the last two decades. The highly networked and interconnected world we live in today was only a flash on the horizon in the 1990s. The Internet itself was still a whole new innovation for many people. Many businesses have not had a public website yet. Concepts, such as online social media platforms, did not exist – and certainly no one thought about how they should be regulated. Smartphones, wearable technology and artificial intelligence have made huge leaps over the past 20 years – powered by new ways of data acquisition and processing. As a result, courts and regulators have increasingly had to adapt the aging data protection laws to suit a constantly changing world for which they were simply not designed. Government digital agendas worldwide go hand in hand with this fast-paced digital evolution. Information security and awareness should be a crucial part of public administration agendas with the primary goal to protect information of all types and origins.

Keywords: public administration; privacy; data protection; private information

1. Introduction

In the global information economy, personal data has become the driving force of most of today's online activity. Every day, a great deal of information is transmitted, stored and collected worldwide, allowing a tremendous improvement in computing and communication power. In developing countries, online social, economic and financial activities have been facilitated through the use of mobile phones and improved internet connectivity. As more economic and social activities move online, the importance of data protection and privacy is increasingly recognised, not only in the context of international trade. At the same time, the current data protection system is very fragmented and has different global, regional and national regulatory approaches.

In this study we will provide a comprehensive overview of the current situation and an analysis of the development trends of compatibility of data protection policies at international level. We also aim to provide a new and balanced view of privileged data protection issues by considering the views of different stakeholders. The conclusions of this study should contribute to reflection on how to increase international compatibility in data protection and privacy, in particular in relation to public law as well as international trade

and provide *de lege ferenda* proposals that could serve as inspiration for countries planning to introduce new laws or amendments to existing laws.

The protection of personal data belongs to the area of fundamental human rights and freedoms. Personal data is sensitive information that serves to identify a person and can only be processed with his or her consent. Everyone has the right to protection from unauthorised interference in private and family life, as well as protection against unauthorised collection, disclosure or other misuse of personal data. The processing of personal data should be designed to serve humanity. The right to the protection of personal data is not an absolute right; it must be assessed in relation to its function in society and must be balanced with other fundamental rights, in accordance with the principle of proportionality.[2] Rapid technological development and globalisation have brought new challenges in the area of personal data protection. The extent of collection and sharing of personal data has increased considerably. Technology enables private companies and public authorities to use personal data to an unprecedented extent in carrying out their activities. Natural persons are increasingly disclosing their personal data, including on a global scale. Technology has transformed both economic and social life and should further facilitate the free flow of personal data on a global scale and transfer to third countries and international organisations, while guaranteeing a high level of protection of personal data. The economic and social integration resulting from the functioning of the internal market has led to a significant increase in cross-border flows of personal data.

Data protection is directly related to trade in goods and services in the digital economy. Insufficient protection can create negative effects on the market by diminishing consumer confidence, and too strict protection can unduly restrict businesses, resulting in adverse economic effects. Ensuring that laws take into account the global nature and scope of their application and promote compatibility with other frameworks is essential for global trade flows that increasingly rely on the Internet. Many social and cultural standards around the world include respect for privacy. While the basic privacy policies contain many common features across countries, interpretations and applications vary considerably in specific jurisdictions. Some protect privacy as a fundamental right, while others base individual privacy on other constitutional doctrines or delicts. Others still have to accept privacy. Such differences will increasingly affect individuals, businesses and international trade. Internationally compatible data protection regimes are desirable as a way of creating an environment that is more predictable for all stakeholders involved in the information economy and building trust online. New technological developments increase this need. Data protection legislation must carefully address the changing needs and opportunities associated with these changes in order to facilitate potential benefits.

In order to ensure a consistent level of protection of personal data and to avoid differences between the jurisdictions of different States that could hinder the free movement of personal data, it is necessary to adopt rules providing legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and providing individuals in all countries of the world with the same level of legal enforceable rights, ensuring consistent monitoring of the processing of personal data and providing for equivalent sanctions, as well as effective cooperation between the supervisory authorities of

the countries of the world. The proper functioning of the international market requires that the free movement of personal data is not restricted or prohibited for reasons connected with the protection of individuals in the processing of personal data. In order to avoid a serious risk of circumvention, the protection of individuals should be technologically neutral and not dependent on the technological solutions used. The protection of individuals should apply to the processing of personal data by automated means, as well as to manual processing if personal data are stored in or to be stored in the information system.

Efforts to achieve balanced, flexible and compatible data protection regulation have become an urgent global objective. Some countries have strong regulatory mechanisms, while others have outdated legislation or none at all. In order to achieve adequate protection that enables innovation and facilitates trade, it is essential to continue the national, regional and global dialogue of all stakeholders.

2. Key Privacy Concerns in an International Context

Data and privacy concerns are manifested in many different dimensions. Governments – especially those in developing countries that are trying to adopt data protection legislation – have difficulties in modelling their data protection regimes, although most have opted for an approach in line with EU legislation.

Common challenges include:

1. the time needed to adopt legislation
2. the financial costs of implementing and enforcing the data protection regime, and
3. lack of public and private sector knowledge and cooperation between governmental entities regulating in parallel

In some countries, lack of understanding and fear in society can aggravate one or more of the above concerns. Concerned consumers, concerns about the integrity of payment systems, hidden costs, fear of fraud and product quality are often more pronounced in the context of international e-commerce. Building trust in the online environment is crucial, and confidence is reflected in transactions with government and private actors. Studies show that citizens are concerned about how their personal data are collected and used and they also point out that these concerns are growing.[3] The lack of clarity in terms of protection and remedies tends to aggravate these concerns.

The most commonly highlighted concerns are:

1. Too strict protection regimes will disproportionately restrict activities, increase the administrative burden and hamper innovation.
2. Uncertainty and compatibility between schemes increase uncertainty with negative effects on investment.
3. Given the link between cross-border e-commerce and data protection, different regimes will prevent the uptake and dissemination of emerging technological developments, thereby reducing potentially accompanying societal benefits.

Although there are significant differences in data protection laws in different countries around the world, there is a more universal consensus on the fundamental principles of personal data protection, which are considered to be at the core of most national legislation and international regimes. This set of basic principles can serve as a useful starting point for efforts to achieve greater compatibility and harmonisation on a global scale. There is currently no uniform agreed model of data protection legislation. However, compatibility is an established objective of many global and regional initiatives in the area of personal data protection. There are a number of challenges in the development and implementation of data protection legislation. We believe that areas where action is particularly needed are:

- addressing gaps in the legal protection of personal data
- addressing new technologies
- management of cross-border data transfers
- strengthening the enforcement of justice
- determination of authority in the field of personal data protection

The number of national data protection laws has risen sharply in the last decade, but large gaps remain in the legislation of the different countries. Some countries have no legislation in this area, others have partial laws and some laws that are outdated and require amendments. In this study, we would like to provide considerations *de lege ferenda* that can help countries that are developing, revising or amending and supplementing their data protection laws.

For countries that still do not have the relevant legislation, governments should develop laws that should apply to data processed by government and the private sector and remove the exemptions to achieve greater coverage of personal data protection. The core set of principles is found in the vast majority of national data protection legislation as well as in global and regional initiatives. Adopting this core set of policies enhances international compatibility while allowing some flexibility for domestic implementation.

The creation of a single central regulatory authority shall be encouraged, where possible, with a combination of supervisory and complaint functions and powers. In addition, the trend is to extend enforcement powers as well as to increase the extent and scope of fiscal constraints and data protection sanctions. It is critical to address cross-border data transmission issues with specific text and to support one or more mechanisms that businesses can use to facilitate international data flows.

In an increasingly globalised economy, where more and more economic activities are carried out online, it is impossible to remain silent on this issue. A modern approach to addressing this seems to be allowing companies to consider a range of options. National data protection legislation should avoid (or remove) clear barriers to trade and innovation. This may include avoiding or removing data localisation requirements that go beyond the basic options for managing cross-border data transfers. A useful test that has emerged in this area is the requirement that such provisions should not be "disguised restrictions on trade".

It is also increasingly difficult to ignore the need to balance personal data protection and state surveillance requirements. In general, countries should implement measures that set appropriate monitoring limits and conditions.

In order to promote the international compatibility of different legislations, it is important to avoid duplication and fragmentation of regional and international approaches to the protection of personal data. It would be preferable for global and regional organisations to focus on a single consolidating initiative or a smaller number of initiatives that are internationally compatible rather than carrying out multiple initiatives. Where possible, similarities to the basic principles should be used to establish mechanisms for recognition and compatibility between different legal frameworks. Future work to achieve greater compatibility will require the effective involvement of all stakeholders, including the government, the private sector and civil society representatives. Their involvement must go beyond general discussions in order to be formally involved in the process of developing the legal framework. This active involvement will also help to develop measures that promote a higher level of legal certainty and trust among stakeholders, which will increase the overall effectiveness of the legal frameworks.

Most regional and global initiatives do not mention the issue of monitoring initiated by governments. However, we believe that it is essential that national legislation and global and regional initiatives recognise the existence of surveillance issues and try to address them directly. While monitoring issues often have an international or cross-border dimension, the extraterritorial nature of data flows must be addressed separately, as they relate to state sovereignty. The UN Declaration on Digital Rights can serve as a platform to consider the link between data protection and surveillance.[4] The development and promotion of international and regional data protection initiatives should also take into account the compliance burden and the potential for adverse effects on trade, innovation and competition.

Finally, favouring provisions that build consumer confidence in regulatory models will help to expand e-commerce. The most important is the development of effective policies around the world, especially with the advent of the latest technological advances. Countries should endeavour to counterbalance the various legitimate concerns of data protection stakeholders, while cautiously avoiding solutions that unduly restrict trade. Rebalancing can have serious consequences for the protection of fundamental rights as well as for international trade and development.

Efforts for a balanced, flexible and compatible legal regulation of personal data protection have become an urgent goal worldwide. Some countries have strong regulatory mechanisms, while others have outdated legislation or none at all. In order to achieve adequate protection that enables innovation and facilitates trade, it is essential to pursue a multi-stakeholder national, regional and global dialogue.

3. Increasing Importance of Personal Data Protection

Data protection laws date back to the 1970s, reflecting concerns about the development of computer and communication technologies and their ability to remotely process large volumes of data. In the global information economy, personal data has become the driving force of most of today's online activity.

Every day, a huge amount of information is transmitted, stored and collected around the world as a result of the huge improvement in computing and communication power. In developing countries, online social, economic and financial activities have been facilitated through mobile phones and better internet access. The cross-border nature of the Internet, as well as the speed and volume of communications itself, cause cyber security problems, such as those related to the identification, investigation, jurisdiction, criminalisation and prosecution of those who commit security and privacy violations. In this environment, information security is a problem for governments, businesses and consumers. Protecting data and privacy rights online is a major and increasingly pressing challenge for policy makers. The scrutiny of and access to information obtained through online activities concerns legislators whose task is to protect their citizens from unauthorised interference and harm.

From a commercial point of view, the transmission of data to and from developing countries may be hampered by the lack of domestic legal protection, which may result in missed business opportunities. Adequate legal instruments to ensure data protection and privacy are still lacking in most developing countries. The scope of the definition of personal data varies (wide or narrow) depending on the jurisdiction, and privacy laws vary considerably between countries and regions.

While many national, regional and international initiatives have pursued distinctly different regulatory approaches, there is a considerable degree of harmonisation of the underlying principles that underpin them. The common principles include the need to have a legitimate reason for any processing activity obtained either by consent or by some other justification. Obligations regarding the quality of the processed personal data are another fundamental principle that requires data to be accurate, complete and updated. Compliance with this principle should be mutually beneficial to both the processing entity and the processor. The role of data security is essential. Whether physical, logical or organisational, security measures should protect against intentional misuse as well as accidental loss or destruction of data. As with data quality issues, the needs of the individual data subjects and the data processing entity – and in principle society as a whole – should be combined in implementing adequate data security. Although there is a broad agreement on fundamental principles, there is no consensus on how best to apply them.

Some data protection regimes apply equally to everyone who processes personal data. Other regimes apply different rules to specific sectors (e.g. health, education), types of processing entities (e.g. public authorities) or data categories (e.g. children's data). In such jurisdictions, some sectors are not subject to regulatory controls at all. A distinction may also be made between regimes which operate primarily through enforcement actions brought by individuals or their representative groups and regimes that confer enforcement powers on a specialised supervisory authority, which continuously monitors the behaviour of those processing personal data. Some modes work by combining both approaches. Data protection is seen as an important area of law, policy development and regulation. It combines elements of human rights and consumer protection, and in many international agreements and individual jurisdictions, the protection of personal data is even considered a fundamental right. At the same time, many stakeholders see data protection regulation

as a legal framework that facilitates the development of new technologies and innovations and promotes international trade and development. Data protection regulation is currently a very topical issue, as evidenced by a number of recent events:

- In 2015, the United Nations appointed a Special Rapporteur on the right to privacy.
- The European Union has adopted a new general data protection regulation, Regulation (EU) 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. This Regulation is an essential step towards strengthening the fundamental rights of citizens of the digital age and facilitating entrepreneurship by simplifying the rules for companies in the digital single market. At the same time, the unified legislation will put an end to the current fragmentation and costly administrative burden.
- Data protection has been included in several international trade agreements.
- Data protection regulation has been considered in several lawsuits with a high degree of professionalism on national surveillance issues.
- Many countries are drafting new data protection laws or reviewing existing legislation.
- The European Union and the United States have renegotiated a long-term cross-border data protection agreement (the former EU–U.S. Safe Harbor framework, now called Privacy Shield), one of the few alternatives for transmission of data outside the EU and therefore its existence is very important.
- Several global and regional organisations have issued (or are preparing) multilateral agreements and/or guidelines on the protection of personal data.

4. Key Challenges in Drafting Data Protection Laws

While many of the global and regional initiatives discussed in this publication are aimed at increasing interoperability between personal data protection regimes, the key problem is that huge gaps remain in the scope of data protection legislation. These gaps fall into three main categories:

1. Countries without personal data protection legislation

The number of countries with data protection legislation has risen sharply in recent years, currently reaching a total of 107 countries that have comprehensive data protection laws, or at least partial data protection legislation. However, this still leaves almost 30% of countries in the world without applicable privacy laws.[5] Personal data in these countries receive a low level of protection, thus reducing legal certainty and confidence in a wide range of business activities. These countries may also be cut off from international business opportunities, as many business transactions require cross-border data transmission, subject to minimum legal requirements. These requirements are difficult (but not always impossible) to meet in the absence of basic data protection legislation. At least 35 countries are currently drafting data protection laws to address this gap. However, the development and

implementation of data protection laws is a time-consuming and complicated process. The United Nations surveys of government officials in 48 African, Asian and Latin American and Caribbean countries highlight the need for awareness-raising and knowledge among lawmakers and courts in order to formulate and effectively enforce informed data protection policies and laws.

2. Countries with legislation containing large gaps and exemptions

Many national data protection laws contain significant gaps and exemptions. For example, some laws exclude small businesses (such as Australia and Canada) or small data sets (such as Japan excludes data sets with less than 5,000 records) from the privacy laws. Other exceptions in some laws apply to:

- types of data subjects (e.g. only children's data and no employee data)
- data sensitivity (e.g. only to sensitive data such as health or financial records)
- data sources (e.g. limited to online or offline data collection)
- sectoral data (e.g. private and public sector exceptions or laws that are limited to specific sectors such as health and credit)

The exceptions are so numerous and so complex that the entire textbook could only be written with a list of exceptions and loopholes in the privacy laws. These exceptions are generally common in North America, Asia and the Pacific, but less typical in Europe, South America and Africa, where data protection legislation tends to provide comprehensive coverage. Exceptions create several legal problems. They require a wide range of stakeholders (business partners, consumers and regulators) to comprehensively identify and categorise data. They severely limit countries' ability to meet the "adequacy test" for cross-border credit transfers and can also lead to complex complaints and disputes.

3. Countries where companies are allowed to exclude certain services or practices from the scope

The third type of gap is less common but has been steadily growing in recent years. Some national laws and regional initiatives allow individual companies to determine the "scope" of the data protection they offer to consumers. There are two ways to do this:

First, a company can join a data protection regime (for example, the EU–U.S. Safe Harbor framework/EU–U.S. Privacy Shield or cross-border privacy rules), but their membership is limited to specific activities. The scope is usually published in the online register. Typical limitations restrict coverage to online or offline data collection, consumer or employee data, or other general categories. However, some scope constraints exclude whole countries from the protection offered by large multinationals.

Second, a company may exclude certain activities from protection by including exceptions in its privacy policy. Organisations are increasingly excluding specific services such as mobile apps, cloud services and software. These exclusions often apply to dispute resolution

when a company uses a third-party dispute resolution provider, so these exclusions can be quite significant for consumers. In practice, the second type of exclusion may not be entirely legitimate if a complaint is lodged with the regulator concerned. Regulators have a wide range of powers in this area. In the United States of America, the Federal Trade Commission (FTC) may take steps for "unfair" behaviour, which may limit the use of such exceptions. Such specific exclusions are a relatively new phenomenon in international data protection regulation and their state (and future) is uncertain. Overall, however, it is difficult to promote global interoperability, while these three types of "gaps" in coverage remain.

5. Cross-border Data Transfers

Overall, it is generally recognised that there should be legislation on cross-border data transfers, but there is a wide range of approaches to this issue and there is no single global model to manage it yet. At a national level, some countries have no restrictions on the transfer of personal data to foreign jurisdictions (such as the United States of America). Most countries have some restrictions in place, usually accompanied by a long list of exceptions. Typical exceptions fall into two broad categories.

1. One-off exceptions – On a global scale, there seems to be a broad consensus on one-off "exceptional circumstances" that allow cross-border data transmission. A recent report by the International Center for Policy Management states that the following exceptions have already become common:[6]

a) the transfer is necessary for the performance of the contract between the data subject and the operator or between the operator and the third party and is concluded at the request of the data subject; or is in the interest of the data subject
b) transmission for the purposes of legal proceedings or for the purpose of obtaining legal advice or for the establishment, exercise or protection of legal rights
c) the transfer is necessary to protect the vital interests of the data subject

2. Ongoing exceptions – The use of ongoing exceptions is less consistent. The following list demonstrates the wide range of approaches available, but there is no consistency or global consensus in their use.

a) The "reasonableness" approach (sometimes known as the white list) assesses whether the entire jurisdiction of destination provides a sufficient level of protection for the transfer of personal data. This approach is used by different countries, including members of the European Union, Israel, Japan and Switzerland.
b) The "binding rules" approach assesses whether a particular company has put in place processes and independent control mechanisms that provide a sufficient degree of protection for the transfer of personal data (usually across a group of companies). This approach is used in a system of binding EU business rules. Some individual jurisdictions also have the potential to recognise these types of binding rules, notably Australia and Japan.

c) The "model contracts" approach assesses whether the specific wording in the contracts provides a sufficient degree of protection for the transfer of personal data. So far, this approach has only been used in the EU.
d) The "consent" approach examines whether individual consumers can agree to transfer their data abroad. This approach is used in the EU and some other jurisdictions but is subject to additional conditions regarding the nature of consent. Consent may be difficult to prove and does not constitute an effective guarantee of protection.

Not surprisingly, many countries have decided to adopt a combination of several approaches to managing cross-border data transfers, as there is no single mechanism that stands out as completely positive. As a result, the law on cross-border data transfers is fragmented and inconsistent.

The problems associated with cross-border data transfer are to some extent addressed through international trade agreements. One recent example of the agreement is the Trans Pacific Partnership Agreement (TPP), which covers 12 countries. TPP addresses the issue of balancing data protection with special regard to trade. In particular, it imposes restrictions on the scope of the Data Protection Regulation which signatories may lay down in their national legislation and is partly based on Article XIV of the WTO General Agreement on Trade in Services. Article XIV allows for restrictions on cross-border transfers if they meet four requirements:

1. the law must "achieve a legitimate public policy objective" – this seems to be a very direct requirement
2. the law must not be "applied in a manner which would constitute a means of arbitrary or unjustified discrimination"
3. the law must not be a "disguised restriction on trade"
4. the law must not "impose restrictions on the transmission of information beyond what is necessary to achieve the objective"[7]

It seems that this four-part test could provide a potential basis for a global standard to determine whether a restriction went "too far". These criteria have a good chance of removing "hidden trade restrictions" and have the potential to increase interoperability and harmonisation beyond the signatories to the agreement.

Overall, the possibilities for managing cross-border data transfers are diverse and varied. Most countries adopt a combination of the above measures and give businesses considerable leeway in managing their own cross-border transfers. This is largely due to the recognition of the reality of modern data-processing systems as well as the current volumes of cross-border transfers that occur at any given moment.

6. Strengthening Powers and Determining Jurisdiction

Currently, we can see a trend towards strengthening enforcement and sanctioning powers in the area of personal data protection. This is a response to a number of high-profile cases

where existing regulatory powers have proven to be disproportionate in view of the widespread impact and scale of privacy breaches. Strengthening enforcement has been a major issue in amending and updating laws (especially in Australia, the EU, China and Japan). The United States is considered a leader in this area. Although there are many loopholes and inconsistencies in the U.S. legislation, the country has had good experience of using extensive sanctions to prevent neglect of privacy. The imposition of large sanctions is considered important for:

- the target company (as a clear signal to senior management and employees to reform their practices)
- the consumers concerned (as a form of compensation for the damage they have suffered), and
- also as a wider deterrent to the whole industry

Jurisdiction is an extremely important issue in all areas of law, in particular in the areas of cybercrime, tax law and intellectual property law. Data protection regulation has become a very important issue, partly because of the extensive flow of data across borders, partly because of the lack of a single global data protection agreement (and the consequent fragmentation of regulation). In the absence of an international agreement, determining jurisdiction is very difficult.

The issue of determining jurisdiction has long been a source of debate and legal reform. The U.S. Child Online Privacy Protection Act (COPPA) extends to foreign service providers who direct their activities to U.S. children or consciously collect information from U.S. children. A recent law reform in Japan resulted in a new request (which came into force in 2017) stating that if a data controller outside Japan collects personal information concerning Japanese citizens, then that foreign controller will be required to meet the requirements listed in the Japanese law.

Regulation (EU) 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data contains an extraterritoriality clause (Article 3) stating:

1. This Regulation shall apply to the processing of personal data in the context of the activity of the controller or processor in the Union, whether or not processing is carried out in the Union.

2. This Regulation shall apply to the processing of personal data of data subjects who are situated in the Union by an operator or intermediary not established in the Union, the processing activities being related to:

a) the offering of goods or services to those data subjects in the Union, whether or not payment is made to the data subject, or
b) monitoring their behaviour within the Union[8]

These reforms are part of a trend towards national data protection regulations that seek to capture any activity that targets local people, regardless of the actual location of the company.

Privacy requirements may limit the possibilities for innovation or create an unrealistic burden on compliance businesses (especially for smaller businesses). Some examples of data protection requirements that have the potential to burden businesses are as follows:

1. Registration requirements

In a small number of jurisdictions (mostly in Europe), data controllers are required to register their operations and sometimes their individual datasets with the local data protection authority. This requirement relates to the historical introduction of data protection regimes at a time when data processing was considered a key risk to privacy. Over time, some data protection authorities considered the registration procedure to be a useful form of general regulation and supervision. In many developing countries, the registration process has also become an important source of revenue. In jurisdictions where data protection relies on membership of a specific system (such as the EU–U.S. Privacy Shield), membership in these systems requires a combination of payments to a central system operator (such as the U.S. Department of Commerce) plus payments to service providers dispute resolution (such as the American Arbitration Association) and payments for third-party certification services (such as TRUSTe). Most fees in these systems must be paid annually. For businesses, registration requirements can be a significant financial burden. Some processes are time-consuming and bureaucratic, and many require fees, whether one-time or annual. Registration requirements may also hamper the ability of businesses to create a single, comprehensive system of data protection processes that could be used in all jurisdictions.

2. Requirements for the appointment of Data Protection Officers

A common requirement in national legislation is that each undertaking appoints a specific Data Protection Officer (the specific name varies slightly in each national law). This does not represent a significant burden in most large organisations if such appointments are common, but it may be a burden for smaller businesses.

3. Requirements for the establishment of data centres

In a few rare cases, data protection laws require businesses to set up either data centres or offices at a specific location. These requirements are a significant obstacle for all businesses but are particularly challenging for smaller businesses and new entrants. Overall, they can effectively reduce opportunities for smaller, newer businesses and negatively affect interoperability. Smaller businesses play an important role in managing innovation and competition, yet they face difficulties in jurisdictions with high compliance burdens. However, the interests of businesses (including small ones) are not completely neglected in global, regional and national personal data protection initiatives. Most global and regional initiatives include a warning of linguistic complexity, excessive burdens on privacy requirements.

7. Global Developments and Trends in the Field of Personal Data Protection

Privacy is not the subject of a single comprehensive global agreement or contract. Rather, it is included in a number of international and regional instruments, each covering a particular group of countries. These global and regional initiatives differ in scope and application – many are simply voluntary guidelines. This chapter discusses major global initiatives, plus the strengths and constraints of each system. In short, we would like to focus on major initiatives with an almost global reach: the UN, the Council of Europe, the OECD and IDPC. Each of these initiatives has its strengths and weaknesses.

1. UN

The United Nations has long promoted the right to privacy through human rights treaties, in particular through Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights. In the period of 2013–2015, the UN strengthened its role in the field of privacy by means of two highly profiled measures. The first was the publication of the Digital Rights Declaration. The second was the appointment of a UN Special Rapporteur on the right to privacy.

Declaration on the right to privacy in the digital age – In December 2013, the UN General Assembly adopted Resolution 68/167,[9] expressing its deep concern about the negative impact that monitoring and interception of communications may have on human rights. The General Assembly confirmed that the rights held by citizens offline must also be protected online and urged all states to respect and protect the right to privacy in digital communications. The General Assembly also called on all States to review their procedures and legislation regarding communications monitoring, interception and collection of personal data and underlined the need for States to ensure the full and effective implementation of their obligations under international human rights law.[10]

The resolution notes that international human rights law provides a universal framework under which any interference in individual rights, including the right to privacy, must be assessed. The International Covenant on Civil and Political Rights, which has so far been ratified by 167 states, states that no one shall be subjected to arbitrary interference in private life, family, home or correspondence, nor to attacks on their honour and reputation.[11] It further states that everyone has the right to the protection of the law against such interference or attacks. Other international human rights instruments also contain similar provisions. Although the right to privacy under international human rights law is not absolute, any case of interference must be subject to a thorough and critical assessment of its necessity, legitimacy and proportionality. The resolution was followed by a detailed report published in 2014: Study by the High Commissioner for Human Rights on the right to privacy in the digital age (A/HRC/27/37).[12] The report concludes that practices in many countries have revealed a lack of adequate national legislation, weak procedural guarantees and ineffective supervision, which together contributed to a lack of responsibility for arbitrary or unlawful interference with the right to privacy.

UN Special Rapporteur on the Right to Privacy – The Special Rapporteur is an independent expert appointed by the UN Human Rights Council to examine and report on specific issues. In July 2015, the Human Rights Council appointed Professor Joseph Cannataci of Malta as the first ever UN Special Rapporteur on the right to privacy. Pursuant to Resolution 28/16 of the Human Rights Council, the Special Rapporteur shall:

a) collect relevant information, including information on international and national frameworks, national practices and experiences; study trends, developments and challenges regarding the right to privacy and make recommendations to ensure its support and protection, including in the context of challenges arising from new technologies
b) seek, receive and respond to information from States, the United Nations and its agencies, programs and funds, regional human rights mechanisms, national human rights institutions, civil society organisations, the private sector, including business entities
c) remove possible obstacles to the enforcement and protection of the right to privacy, identify, exchange and enforce principles and best practices at national, regional and international level and, in this context, submit proposals and recommendations to the Human Rights Council, including in the light of these facts and in particular to the particular challenges of the digital age
d) participate in and contribute to relevant international conferences and events in order to promote a systematic and coherent approach to mandate issues
e) raise awareness of the importance of promoting and protecting the right to privacy, addressing the specific challenges of the digital age as well as providing information to individuals whose privacy has been violated, ensuring access to effective remedies, in accordance with international human rights obligations
f) report on alleged violations of the right to privacy wherever they occur, as set out in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights, including the challenges arising from new technologies, and alert the Council and the UN High Commissioner for Human Rights on situations of particular concern
g) submit an annual report to the Human Rights Council and the General Assembly

In March 2016, the UN Special Rapporteur prepared his first report on the right to privacy, which was presented to the Human Rights Council (A/HRC/31/64). The report describes his vision of the mandate and provides an overview of the state of privacy in early 2016 and a work plan for the first three years of the mandate. In order to facilitate the process of further elaborating the dimensions of the right to privacy and its relation to other human rights, the Special Rapporteur has developed a Framework Action Plan.

The strengths of UN initiatives include universal respect and global coverage, a long history of promoting and protecting human rights; and recognition of privacy as a fundamental right. One of the limitations of UN initiatives is, in particular, that the current provisions are too theoretical for day-to-day operations – the right to privacy must be translated into a detailed set of principles. Another problem is that the UN is facing some significant constraints in terms of resources, whether material or personnel.

2. The Council of Europe

The right to the protection of the private sphere of the individual from interference by other entities, in particular the State, was for the first time enshrined in Article 12 of the UN Universal Declaration of Human Rights in 1948 and referred to respect for private and family life. The Universal Declaration of Human Rights has influenced the development of other human rights instruments in Europe. The Council of Europe was established after World War II with the intention of bringing together European states in the promotion of the rule of law, democracy, human rights and social development. To this end, the Council of Europe approved the European Convention on Human Rights in 1950, which entered into force in 1953. Member States have an international obligation to comply with the ECHR provisions. All Member States of the Council of Europe have incorporated the ECHR into or have entered into force in their national legislation and must therefore comply with the provisions of this Convention.

The right to the protection of personal data forms part of the rights protected under Article 8 of the ECHR, which guarantees the right to respect for private and family life, dwelling and correspondence and lays down the conditions for the admissibility of restrictions on that right. In its case law, the ECHR has considered many data protection cases, including, inter alia, interception of communications,[13] various forms of surveillance[14] and protection against the retention of personal data by public authorities.[15] Article 8 of the ECHR not only requires States to refrain from taking any action that might undermine this right enshrined in the Convention, but in certain circumstances imposes a positive obligation to actively ensure effective respect for private and family life.

Council of Europe Convention No. 108 – The emergence of information technology in the 1960s has made it increasingly urgent to adopt detailed rules on the protection of individuals by protecting their personal data. In the mid-1970s, the Committee of Ministers of the Council of Europe adopted several resolutions on the protection of personal data referring to Article 8 of the ECHR. In 1981, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) was prepared for signature. Convention 108 was the only legally binding international data protection document. At present, Convention 108 is the most important binding international agreement on the protection of personal data. Although this Convention was established in the Council of Europe, its membership is open to each country, and several non-European countries have already signed the Convention.

All member states of the Council of Europe have ratified the Convention and implemented data protection laws that comply with the Convention (the last one was Turkey, where ratification took place in 2016). Uruguay was the first non-European country to become a Party to the Convention in 2013. Currently, the Convention has been ratified by 9 non-European countries (Argentina, Burkina Faso, Cape Verde, Mauritius, Morocco, Mexico, Senegal, Uruguay and Tunisia). The Convention differs from many other global initiatives in that it is binding on signatories. Data in the private and public sectors, such as the processing of personal data in the judiciary or law enforcement authorities, protects the individual from abuse that could accompany the collection and processing of personal data, while regulating the cross-border flow of personal data.

With regard to the collection and processing of personal data, the principles laid down in the Convention related in particular to fair and lawful collection and automated processing of data which are stored for specified legitimate purposes and are not used for purposes incompatible with those purposes or absolutely necessary. These principles also regulate the quality of the data, in particular its adequacy and relevance, as well as the fact that the data must not be redundant (proportionality) and must be accurate. In addition to providing safeguards for the collection and processing of personal data, the Convention regulates (where there are no adequate legal safeguards) the processing of so-called "personal data", i.e. sensitive data such as race, political attitudes, health, religious beliefs, sexual life, or criminal record data. The Convention also enshrines the right of an individual to know about the retention of data concerning him and to be able to correct such data as necessary. Restricting the rights set out in the Convention is only possible in cases of overriding interests, such as national security or defence.

Among the strengths of the Council of Europe Convention 108 include comprehensive coverage, the existence of broad acceptance of the principles contained in the Convention, the possibility of any country to join, cooperation under the open procedure. The great advantage is the binding nature of the agreement, which leads to effective harmonisation; and that the Convention has strong support of other initiatives (e.g. endorsed by the International Data Protection Commissioner as the best available global model). The limitations of the Council of Europe Convention include, in particular, its Eurocentric nature (although currently extending rapidly to non-European countries). Overall, Convention 108 is the most promising international development in an area where each initiative faces enormous challenges.

3. OECD

Member States of the Organization for Economic Co-operation and Development (OECD) have developed the OECD Guidelines on the protection of privacy and cross-border flows of personal data in consultation with a broad stakeholder group. With the introduction of information technology in various areas of economic and social life, and with the increasing importance and potential of automated data processing, the Organization for Economic Co-operation and Development decided in 1980 to issue guidance on international privacy policy and the cross-border flow of personal data. The rapid and ubiquitous development of information and communication technologies and infrastructures, characterised by a phenomenon such as the Internet, has accelerated developments towards a global information society. The OECD has therefore focused on how this guidance could best be applied in the 21st century to help ensure respect for privacy and the protection of electronically accessible personal data.

The guideline on privacy and the cross-border flow of personal data was adopted as a recommendation of the OECD Council in support of the three principles that are binding on OECD member states: open democracy, respect for human rights and the free market economy. It entered into force on 23 September 1980. The Privacy Guidelines

constitute an international consensus on the general approach to collecting and managing personal information.

The principles set out in the Privacy Guidelines are comprehensible, flexible to apply and formulated sufficiently broadly to be adapted to technological changes. The principles include all media for automated processing of individual data (from local computers to networks with complex national and international branches), all types of personal data processing (from human resources to compiling customer profiles) and all data categories (from transient data to fixed data, from the most mundane to the most sensitive). The principles are applicable both nationally and internationally. They have gradually been incorporated into a large number of national regulatory or self-regulatory instruments and are still frequently used in both the public and private sectors. The Guidelines can be governed by any country, not just OECD members.

The OECD itself has 34 members, of which 32 have already implemented comprehensive data protection laws prior to the adoption of the Guidelines. At the end of March 2016, the Turkish Parliament approved a draft data protection law aimed at aligning the Turkish regime with the EU regime, leaving the U.S. as the only exception (the U.S. is more likely to use the sectoral approach to data protection). However, the real impact of the OECD Guidelines is its impact on the content of privacy laws around the world – far beyond the OECD membership. The Guideline contains eight privacy principles, which are those contained in most national privacy laws.

The strengths of the OECD Guidelines on Privacy include a long and respected history, generally accepted basic principles, a focus on striking a balance between data flows and data protection; wide support for diverse groups. The limitations of the OECD Guidelines on privacy include the absence of the principle of proportionality (or minimisation of data), the non-binding nature of the guidelines and focus on developed countries (although in practice the basic principles are largely applicable).

4. Initiatives of the International Data Protection Commissioners

The latest data protection initiative, which has an almost global impact, is the work of international data protection authorities. Their main role is to regulate national data protection legislation, but since their work involves more international disputes, they have begun to engage in a global privacy debate. There are three main initiatives:

1. annual meeting and conference
2. a system of cooperation on international and cross-border complaints, and
3. a statement of global privacy principles

For our purposes, the third initiative is of the utmost importance. At their meeting in 2005, the International Data Protection Commissioners issued a statement entitled: *The Protection of Personal Data and Privacy in a Globalised World: A Universal Right Respecting Diversities* (also known as the Montreux Declaration).[16] The Declaration called for the development of an international data protection convention and is one of the most important efforts to harmonise data protection laws worldwide. In particular, the Declaration states: Data

Protection and Privacy Commissioners express their desire to strengthen the international recognition of the universal nature of these principles. They agree to cooperate, in particular, with governments by international and transnational organisations in drawing up a universal convention on the protection of individuals with regard to the processing of personal data. To this end, the Commissioners called for:

a) the UN to develop a legally binding instrument that clearly lays down detailed data protection and privacy rights
b) any government in the world to promote the adoption of legal instruments for data protection and privacy in accordance with the fundamental principles of data protection and to extend them to its mutual relations, and
c) the Council of Europe, in accordance with Article 23 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), invites non-member States of the Council of Europe which already have data protection enshrined in domestic law to accede to

The strengths of the International Data Protection Commissioners' initiatives include significant global impact, real world experience, insight into current issues and emphasis on the Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) as a global platform (instead of proposing something brand new). Restrictions on the initiatives of the Commissioners for International Data Protection include the lack of formal structure or follow-up and the non-binding nature of the declaration.

8. Conclusion

On the previous pages, we aimed to emphasise the importance of data protection management in the context of international trade and in the context of different global, regional and national approaches to data protection regulation. We recognise that there are various legitimate concerns regarding data protection and privacy – from consumers (civil society), businesses and governments. The challenge for data protection and privacy laws is therefore to balance these various concerns and interests, ideally in a way that does not unnecessarily restrict trade and innovation.

It is also essential to find solutions that are internationally compatible to facilitate cross-border online trade. As we have mentioned in this study, the current system is not satisfactory and, given the growing economic and social activity on the Internet and the introduction of new technologies, there is an urgent need to address the situation. Against this background, we evaluated the current situation and tried to find possible paths towards a system that provides an appropriate balance between data protection and data streams.

Key conclusions are: There is a recognised set of basic data protection principles. With a remarkable degree of harmonisation and coherence around the core principles of data protection in key international and regional agreements and guidelines, different implementation procedures exist. Although there are significant differences in the details

of data protection laws around the world, we can find greater agreement at the core of most national laws and international regimes.

These common basic principles are: openness, limitation of data collection, purpose specification, limitation of use, security data quality, transparency and accountability. This set of basic principles is a useful starting point for efforts for interoperability and legislative harmonisation. Countries that have not yet introduced laws, or countries that are updating or reforming their laws, should seek to incorporate these basic principles into their new (or amended) legislation. While the coherence of the principles may not guarantee full mutual recognition, it can significantly contribute to the compatibility of different policies.

In some other legal areas, international and regional organisations have come together to support a single initiative to achieve compatibility and harmonisation. For example, in the case of cybercrime, there is broad support for the development and extension of the 2001 Council of Europe Convention on Cybercrime, which now has 54 signatories, including many European countries, Australia, Canada, Japan and the USA. The Convention has led to the harmonisation of cybercrime legislation in many other countries, beyond the signatory members, as the basic provisions are often reflected in the national legislation of several States. On the contrary, there is no single global agreement on data protection. There are many regional and international initiatives in this area, some of which are in competition with each other. Although there are different approaches, there are quite a number of common views on the basic principles and broad agreement on the issues to be addressed. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe Convention No 108) is the agreement with the widest support and greatest potential for compatibility. The Convention may be signed by any country; already has a large number of supporters; it is based on generally agreed principles; has the support of key stakeholders (in particular civil society and regulators); and its binding nature would increase compatibility and interoperability. However, the Convention must attract key support in North America and Asia and the Pacific.

Regardless of which instrument will form the basis of cohesion, convergence of regimes may already occur. One example is the European Union. The European Union intends to make progress not only towards internal but also external cooperation: the EU is actively engaged in international data protection cooperation through various international fora, including the OECD and the Council of Europe (and intends to become a party to the revised Council of Europe Convention on Data Protection 108). The EU participates in a dialogue on privacy and data protection with regional organisations, in particular APEC.

Achieving the wrong balance between data protection and data flows can have serious consequences for the protection of fundamental rights as well as for international trade and development. In most cases, data protection initiatives have been developed in an open and transparent way, with opportunities for entry from different stakeholders' perspectives. For example, the Council of Europe Convention 108 contains a forum where all Member State governments, regulators, private sector stakeholders and civil society representatives can gather information and share information on the promotion and improvement of the

Convention. However, there are examples of initiatives that were developed without the opinion of external stakeholders. For example, international trade agreements are often considered to be developed through clandestine negotiations, which clearly limit the opportunities to hear the voice of the consumer – civil society.

Another key point for countries without a legal framework in the field of personal data protection is the establishment of an effective regulatory structure. The benefits of a single central regulator, in particular for international trade opportunities and for consumers in general, are considerable. While there are differences in the regulatory structure of the legislation, the creation of a single central regulatory authority seems to be strongly encouraged, where possible. Several countries have moved from a complex regulatory structure of several agencies to a simpler structure of national agencies (e.g. Japan has moved from 30 regulators to one central regulator). This is not always possible due to the federal nature of jurisdiction (e.g. Canada, Germany and India). However, the benefits of a single regulator, especially as regards international trade opportunities, are huge. Foreign companies then have to deal with only one focal point and a single regulator can achieve consistency by issuing a single set of guidelines or standards. Consumers will also be made much easier to deal with complaints and questions if there is a single regulatory body and at the same time, a single consistent set of decisions of the national regulatory authority will have a greater impact than a diverse set of decisions from several regulatory authorities. It is important that the regulator also has the role of complaint manager. Most regulators combine a general supervisory function with this specific task, with some exceptions. For example, the FTC in the United States of America is a strategic regulator (it may not respond to individual complaints), while dispute resolution in the United States is partly governed by private litigation and third-party providers. The Republic of Korea has formally divided the regulatory and complaints agenda between the two agencies.

Developing and implementing data protection laws is a complex and costly process that often requires a careful balance between data protection and data flows. Redressing the balance can have serious consequences for the protection of fundamental rights or for international trade and development. Future efforts to achieve greater compatibility will require the effective involvement of all stakeholders, including representatives of the private sector and civil society. This involvement must go beyond general discussions (conferences, seminars, etc.) to engage in the formal policy development process. Developing global and regional data protection initiatives also requires the involvement of developing countries in the debate. Too often, the debate is dominated by the interests of developed countries. Developed countries have the most advanced data protection laws and have the most experience in enforcing them but improving cooperation with developing countries is increasingly encouraged. The world is at the forefront of a transformational technological revolution, fuelled by the economic and social benefits of access to data. Emerging markets are competing with time to capture these benefits but are left out of the innovation dialogue that largely takes place among developed markets.

Global privacy laws are at a crossroads. So far, these laws have mostly focused on the rights of individuals. In general, the aim was to ensure the protection of individuals' private lives and to prevent their governments and businesses from being unfairly violated. However, interesting new pages are emerging in discussions on the future direction of

policy in this area. On the one hand, there is strong business pressure to allow a free flow of data, which is an essential part of a world in which economic growth is increasingly digital. On the other hand, individuals generally do not like the feeling that they are being spied on or that their data is beyond their control. The overall approach to this issue in the EU and some other jurisdictions is currently being resolved for the foreseeable future, but legislators in jurisdictions in which privacy is emerging are facing challenges.

The main question is where there should be the right balance between the right to privacy and the ability of companies to monetise individual data. On the one hand, there is an indication that the right to privacy is absolute and inviolable (in fact, it is referred to as a fundamental right in the EU). The supporters of this view consider that the right to the privacy of the individual is paramount – and it is not difficult to understand why this argument is attractive. Major privacy breaches and security failures are getting headlines with alarming regularity and show that many businesses are not investing as much in digital security as they should. In fact, even if proper and responsible investments have been made, it is often impossible for any company to ensure that no third-party attacker gets well into its systems.

Efforts to achieve balanced, flexible and compatible data protection regulation have become an urgent global objective. Some countries have strong regulatory mechanisms, while others have outdated legislation or none at all. In order to achieve adequate protection that enables innovation and facilitates trade, it is essential to continue the national, regional and global dialogue of all stakeholders.

The need for new legislation is fast approaching due to the unstoppable technological revolution. New technologies, including machine learning, artificial intelligence and fintech, offer countless benefits in terms of data analysis and quick and accurate decision-making in tasks that can take a lot longer. However, the testing and development of these technologies often relies on access to large data sets to achieve meaningful results.

Developers are faced with difficult decisions to move their operations to jurisdictions that place less restrictions on data handling for testing purposes. Once the products are functional, many companies find that if they choose to offer their services in jurisdictions with very strict privacy laws, they have to face a high regulatory barrier.

Some companies have taken the view that the costs of meeting these strict privacy obligations are too high to be justified until the product is well established. As a result, users in jurisdictions with strict privacy laws are increasingly finding that the latest technologies are not available in those jurisdictions. It is therefore important that all jurisdictions ensure the implementation of data protection laws in a way that does not hinder creativity and technological development. If they fail to do so, they risk their citizens becoming second-class passengers on the digital journey.

References

1 This work was supported by the Slovak Research and Development Agency under the contract No. APVV-16-0521.
2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
3 Data protection regulations and international data flows; United Nations Publication; UNCTAD/WEB/DTL/STICT/2016/1/iPub United Nations, 2016 Switzerland.
4 *The Age of Digital Interdependence,* Report of the UN Secretary-General's High-level Panel on Digital Cooperation, www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf (accessed 11 August 2019).
5 *Summary of Adoption of E-Commerce Legislation Worldwide,* Global Cyberlaw Tracker, http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Global-Legislation.aspx (accessed 11 August 2019).
6 Centre for Information Policy Leadership (CIPL), Cross-Border Transfer Mechanisms, www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_indonesia_ministry_of_comm_and_it_draft_regulation_august_20_2015.pdf (accessed 08 November 2019).
7 WTO General Agreement on Trade in Services, www.wto.org/english/tratop_e/serv_e/gatsintr_e.htm (accessed 08 November 2019).
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).
9 The right to privacy in the digital age: resolution / adopted by the General Assembly, A/RES/68/167, https://digitallibrary.un.org/record/764407/?ln=en (accessed 08 November 2019).
10 United Nations, Resolution adopted by the General Assembly on 18 December 2013, 68/167. The right to privacy in the digital age, www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167 (accessed 08 November 2019).
11 *The International Covenant on Civil and Political Rights,* https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf (accessed 08 November 2019).
12 United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age* (an Overview), www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx (accessed 08 November 2019).
13 Copland v. The United Kingdom European Court of Human Rights [2007] C/62617/00, European Court of Human Rights.
14 Klass and others v. Federal Republic of Germany, Judgment, Merits, App. no. 5029/71 (A/28), (1979-80) 2 EHRR 214, IHRL 19 (ECHR 1978).
15 S and Marper v. United Kingdom, ECHR [2007] EHCR 110, 30562/04.
16 The International Data Protection and Privacy Commissioners, Montreux Declaration – *The Protection of Personal Data and Privacy in a Globalised World: A Universal Right Respecting Diversities,* 2005, https://edps.europa.eu/sites/edp/files/publication/05-09-16_montreux_declaration_en.pdf (accessed 08 November 2019).

Public Governance, Administration and Finances Law Review Vol. 4. No. 2. (2019) • 52–64.

10.53116/pgaflr.2019.2.4

Blockchain Technology – Current Status, Challenges and Perspectives in Tax and Customs Law[1]

Ladislav Hrabčák,* Monika Stojáková**

* Ladislav Hrabčák, Mgr., Internal PhD student of Pavol Jozef Šafárik University in Košice, Faculty of Law, Department of Financial Law, Tax Law and Economy. (e-mail: ladislav.hrabcak@student.upjs.sk)

** Monika Stojáková, JUDr., Internal PhD student of Pavol Jozef Šafárik University in Košice, Faculty of Law, Department of Financial Law, Tax Law and Economy. (e-mail: monika.stojakova@student.upjs.sk)

Abstract: One of the hallmarks of the 21st century society is rapid technological progress. It must be addressed by national legal systems, which is another theme discussed in this article. Blockchain technology is one of the most current issues, not only in information technology, but also in law. This paper aims to assess the current legal situation and to reflect on the challenges and perspectives that are undoubtedly related to Blockchain, as it focuses on tax and customs law. Whether Blockchain is capable of contributing to more efficient tax and customs collection is a fundamental hypothesis that we will attempt to confirm or refute.

Keywords: Blockchain; tax law; customs law; taxes; customs

1. Introduction

The Blockchain technology was birthed in 2008, when a person under the pseudonym Satoshi Nakamoto[2] introduced an alternative payment system in the document called *Bitcoin: A Peer-to-Peer Electronic Cash System.* The idea of the Bitcoin's author and developer was initially not embraced by society. The change occurred only at the turn of 2017 and 2018 with a rapid increase in the value of cryptocurrencies, although it could be perceived more as the motivation of most entities to engage in speculative buying and selling virtual currencies[3] to appreciate their money rather than to show interest in the technology itself.

It is an issue which has been unexplored, and unregulated by legislation. National parliaments have adopted certain legislations with substantial delay, and only due to the increasing value of cryptocurrencies, since it became a prospect of taxation. The concept of "virtual currency" has been applied in Slovak law since January 1, 2018, when the legislature began taxing income linked to cryptocurrency operations.

We can see that the legal systems of the individual states limit their scope mostly to regulating one specific way of using Blockchain, namely cryptocurrencies (in particular their taxation), which relate to their cautious approach to modern technologies, and their lack of readiness to use it potentially in the public sector. It is the positive way of using Blockchain we have set out to highlight in the following text of this paper, which aims to assess the

current legal status of the technology and to reflect on the challenges and perspectives that are undoubtedly related to Blockchain, as it focuses on tax and customs law.

2. Technological and Legal Aspects of Distributed Ledger, Blockchain and Smart Contracts

2.1. Distributed Ledger Technology (DLT)

Before we elucidate the Blockchain technology, we must first briefly attend to the "distributed ledger technology" (hereinafter: DLT), since Blockchain represents the most renowned DLT. It is a concept that is broader than the concept of Blockchain. This term is so specific that there is no equivalent denotation for it in the Slovak language without raising certain reservations.

With some measure of generalisation and imprecision, DLT can be defined as a technology, which allows computers in various locations to propose and verify transactions, as well as update the records in the network in a synchronised fashion.[4]

On the whole, DLT represents a way, which enables chronologically arranged information to propagate throughout the entire network. Its defining attribute revolves around information that is cryptographically locked and retroactive changes that are not possible. Another significant aspect is storing information in a decentralised way.

The above is of course also valid for the Blockchain technology with features which make it unique in relation to the DLTs. The most significant difference between the two lies in storing information about potential transactions in Blockchain into blocks that gradually interconnect. It is a quality which every DLT need not have. The following section of the article is dedicated to Blockchain.

2.2. Blockchain technology

Some authors consider *Blockchain* to be both a technology as well as a strategy, which the states can use to provide services in a transparent, effective and decentralised fashion.[5] We can agree with this opinion and immediately list examples of multiple states which have already adopted the use of the Blockchain technology in the public sector.[6]

We are going to attempt to elucidate the concept of Blockchain in several remarks. The previously presented information makes it apparent that Blockchain is a specific type of a distributed network, in which the exchange transactions are gradually classified into blocks that are mutually interconnected and invariably recorded within the network.[7]

Technically speaking, there are 3 types of computers involved in Blockchain as follows:

1. nodes – which preserve the entire Blockchain and perceive all transactions, including their histories

2. miners – who verify the authenticity of the executed transactions via the dedicated technology, and
3. clients

To get a better grasp of how the technology works, Figure 1 models a transaction in Blockchain.

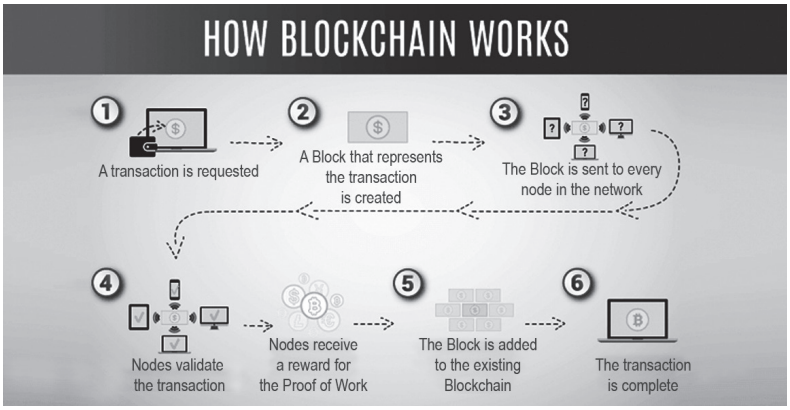

Figure 1.

Source: www.zignuts.com/blogs/how-blockchain-architecture-works-basic-understanding-of-blockchain-and-its-architecture/[8]

Blockchain is a legally unregulated technology, which can be attested by the example of the Slovak Republic. In theory, Blockchain is usually compared to a general ledger, database, or a computer program. It is however questionable, whether this technology meets the attributes of at least some of the listed concepts, which have found its place in the legal order of the Slovak Republic.

Most often, Blockchain tends to be likened to a general ledger, namely to an *accounting journal.*[9] Although in Act no. 431/2002 Coll. on Accounting as amended,[10] there is no legal definition of these concepts, it is possible to perceive the likeness in the way accounting is done in the accounting journal. The individual accounting entries are arranged chronologically, which proves accounting of all accounting cases in the accounting period (Act No. 431/2002, s. 12 (1) Coll. on Accounting, as amended).[11] To some extent this comparison can be accepted with one exception. Our reservation is rooted in the fact that Blockchain allows for virtually endless chaining of new and new blocks and is not confined to a limited period such as the accounting period for an accounting journal.[12] In contrast to an accounting journal, information recorded in Blockchain is virtually immutable, which is an advantage to states.

Another concept which Blockchain is compared to is a *database.* Pursuant to s. 130 (1) of Act no. 185/2015 Coll. on Copyright as amended[13] (hereinafter: Copyright Act), a database is: *"...a collection of mutually independent works, data, or other mutually independent materials which are systematically or methodically arranged and individually*

accessible by electronic or other means regardless of the form of its expression." It is clear from this definition that it serves a specific piece of legislation, but by generalising it, it is also possible to arrive at certain characteristics that can subsequently be confronted with the properties of Blockchain technology. The content of the database, as it follows from the respective definition, does not necessarily have to include only copyrighted works, but also other elements that are not copyrighted works or are even excluded from copyright protection.[14] Blockchain also shares this property since different types of data can be stored within this "database".[15] Since the element of creativity is absent in the arrangement of the data in question, it can be ruled out that Blockchain carries the attributes of an author database. However, we might wonder whether Blockchain is a so-called unauthorised database where a substantial contribution of an entity to the acquisition, verification or presentation of the database content is important.[16] This question can also be answered in the negative. Blockchain technology is an open source,[17] which means it is available to virtually anyone. Based on the above, Blockchain cannot be a database in the sense of the Copyright Act.

Blockchain technology does not carry the features of a *computer program* either. Here, too, the provisions of the Copyright Act are useful. A computer program *"...is a set of commands and instructions expressed in any form, which is used directly or indirectly in a computer or similar technical device..."* Also significant here is the conclusion of the referenced provision: *"...if it is a result of the author's intellectual activity (Act No. 185/2015, s. 87 (1). Coll. on Copyright as amended").*[18] This condition is absent in this case. There are also information technology reservations in relation to this comparison but we will not discuss these in detail.

We can see that Blockchain technology is somewhat in a vacuum in the legal conditions of the Slovak Republic, much like in most countries. Due to its peculiarities, it cannot be compared to any of the presented concepts, even if it is closest to an accounting journal.

This technology is in principle considered safe because thousands of independent miners[19] participate in the network to verify individual transactions (see above), and therefore its use in the public sector can be considered. It connects to the following characteristic features of Blockchain:

1. availability – it is a non-patented technology, allowing for a wider range of application
2. decentralisation and security – data control is transferred from centralised institutions to individuals
3. transparency – information is easily traceable and retrospective change is not possible
4. distribution – P2P[20] systems hinge on the fact that all information is sent to all active nodes in the network which ensures fast and automatic availability of information to users

States will first have to deal with the issue whether the state's local Blockchain can be as secure as the one used for cryptocurrencies and whether it is global in nature. In principle, it is essentially far easier to compromise Blockchain that exists within a single state than the worldwide Blockchain. Another question raised revolves around ways to strengthen

the position of the state, as the use of this technology weakens it,[21] while the possibility of avoiding foreign influence remains an equally important issue if a person or a group of persons gained control over the absolute majority of the miners' network, in which they could then arbitrarily falsify transactions without being revealed. These are only some of the pitfalls associated with this modern achievement.

2.3. Smart contracts

Smart contracts serve as an example of Blockchain's use that is not limited to cryptocurrency. Generally, smart contracts are agreements in the form of computer programs. The basic objective of smart contracts is to eliminate the need for an intermediary and at the same time to contribute to simplifying the execution of online transactions between anonymous participants.

As far as the definition of smart contracts is concerned, they can be defined as agreements between parties, which are stored as computer codes recorded in Blockchain that ensures independent and automatic execution when pre-agreed conditions are fulfilled.[22] This definition yields certain defining features, which are:

1. terms of contract in source code – use of programming language in contrast to standard contracts using a common language[23]
2. storing source code on the Blockchain platform – this platform ensures durability and non-reversibility of a smart contract[24]
3. independence – the will of the parties is required initially, but it is no longer needed after the conclusion of the smart contract
4. self-execution, after fulfilment of predetermined conditions, is related to the previous quality and therefore smart contracts are described by some authors as executors of themselves[25]

We could undoubtedly include its unregulated nature as another defining feature, since this is an issue that the legal norms in the legal systems of states do not consider.

It is also important to deal with the question of whether smart contracts can be regarded as contracts in the true sense of the word. There is no consensus among law theorists on this issue. Many have reservations in relation to the designation of smart contracts as "smart", as they are merely executors of what is contained in the source code.[26]

We are going to point out to the example of the Slovak law to elucidate whether smart contracts are contracts in the proper sense of the word. *"The contractual relationship is a legal relationship that gives the creditor the right to performance (receivable) from the debtor and the debtor becomes obliged to fulfil the obligation (Act No. 40/1964, s. 488 Coll. of the Civil Code as amended)".*[27] It is a very broad definition of a contractual relationship, but more important to us is that the smart contract is certainly a legal fact that gives rise to a legal relationship between the contracting parties. In accordance with that provision, therefore, the obligation is subject to certain performance. The will of the contracting parties is required initially, but it is subsequently no longer necessary, and therefore the debtor is essentially unable to avoid the fulfilment of his obligation. The essential fact here,

however, is that the contracting parties show their willingness to be bound by it which makes the views in theory, whether legal obligations in the true sense of the word arise here, unfounded.[28]

It is questionable whether a smart contract can be regarded as a comprehensive contract or an agreement on the way of its performance which will form a part of a comprehensive contract.[29] Regardless, we agree that in the event of damage, it is possible to file a claim in court, and also, that if one of the parties is a consumer, the consumer protection regulation applies.[30]

Their use in practice could follow this course:

1. the contracting parties set the terms and conditions
2. the terms and conditions must then be written in computer code
3. the code is stored in Blockchain and cannot be changed from now on
4. the conditions are fulfilled, the contract will execute itself

In comparison with traditional contracts, smart contracts are characterised by the following aspects:

1. they are completely digital
2. they are "self-executing" in nature, and
3. the code itself defines the obligations of the contracting parties

Smart contracts are a very interesting idea, but they have not yet had much success in practice. However, it is more than likely that future is bright for smart contracts, which is why the legislators will have to deal with this issue. The use of Blockchain and smart contracts is possible also in tax and customs law, which we are going to point out further on.

3. A New Tool for more Efficient Tax and Customs Collection?

Several authors have already pointed out in their publications that Blockchain can also be used in the public sector.[31] This can be explored in several directions, but we will, because of the limited scope of the paper, consider its use in the following situations.

3.1. Use of Blockchain to eliminate tax and customs fraud

Value added tax (hereinafter: VAT), as a general indirect consumer tax,[32] is a traditional part of the tax systems of the EU Member States. While it is true that this tax involves certain issues, it is the most profitable tax ever.[33] On the other hand, VAT evasion climbed across the EU in 2016 to € 147.1 billion,[34] which is in fact an alarming figure. This situation can also be attributed to cross-border intra-EU trade as it is exempt from VAT in the current legal situation. Although this exemption is planned to be abolished in the context of the upcoming reform of the EU VAT system, Blockchain technology is also a promising tool (especially in the future) in eliminating VAT evasion.

Here, we will try to briefly explain what the MTIC fraud entails (from *Missing trader intra-community fraud*), and how it could be countered by using this modern tool. In general, MTIC fraud is an abuse of the VAT system in cross-border trade. Figure 2 models how such fraud could work.

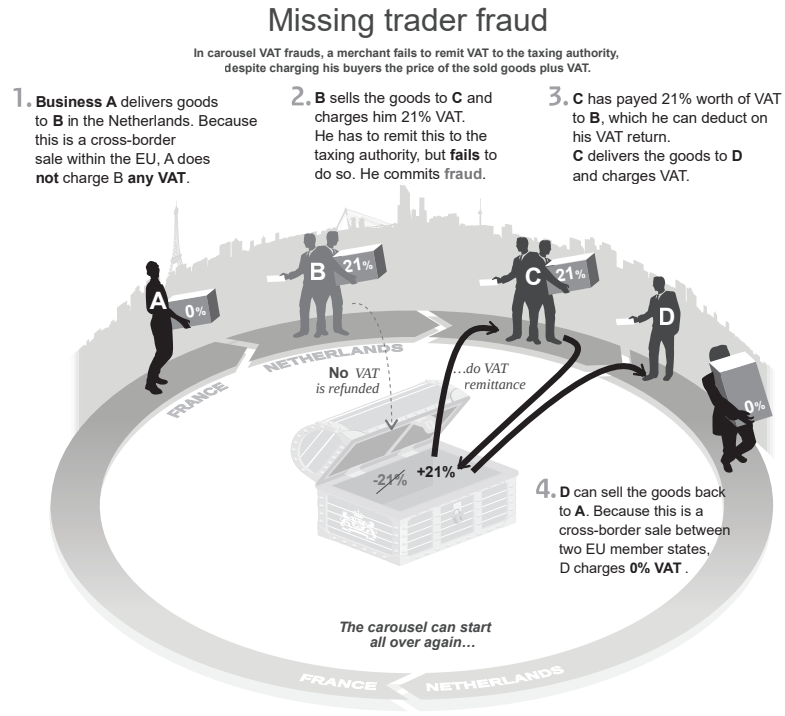

Figure 2.

Source: https://en.wikipedia.org/wiki/Missing_trader_fraud#/media/File:Carrouselfraude.svg[35]

Person A from one member state delivered goods to person B in another member state. This trade will not be subject to VAT as it qualifies for a VAT exemption. Subsequently, person B sold the goods with applied VAT to person C from another member state. Person B, however, did remit the VAT to the tax authority, thereby committing fraud, but person C deducted it on their VAT return. Then, person C delivered the goods to person D, who sold it back to person A. Such a chain can be repeated practically indefinitely. In theory, this situation is commonly referred to as carousel fraud, or carousel chain.[36]

According to some estimates, applying the potential of Blockchain technology could reduce VAT evasion by EUR 50–60 billion per year.[37] It could be possible by using a multilateral smart contract to which the seller, the buyer, the competent tax authority, and the banks of the seller and the buyer would be parties. It is the buyer's bank that will have a significant role in this multilateral relationship, since it will "redistribute" the buyer's payment by transferring VAT to the tax authority's account and the purchase price, less

VAT, to the seller's account. In this way, it would be possible to eliminate the risk of error by taxpayers, and, also to reduce the extent of fraudulent action. Such an automated process would also be advantageous because the information about the entire transaction would be recorded in Blockchain, in an immutable and continuous manner.

From a legal point of view, the nature of the legal relationship arising from a multilateral smart contract is also an interesting issue. Here we get to a specific situation where the state is also represented by a particular tax authority. It becomes permeated by public law elements and the legal relationship becomes hybrid.

In contrast to the current situation, final VAT clearance would no longer lie with the taxpayers.[38] Based on this principle, each company's VAT input and output balance would be kept by the tax authorities, and its new information updates would be continuously recorded in Blockchain. Technically, entrepreneurs will need to be linked to a "transaction register".

As it is a modern technology, there are some unanswered questions, or pitfalls. One is the amount of data that would be recorded. It is questionable whether Blockchain is able to function smoothly even under an extreme load and overload of business transactions. It is also questionable how to protect this confidential data from various hacker attacks, as practice has shown us that even these are not out of the question.

If the EU member states are interested in putting this technology into practice, it will also be very difficult to deal with the user interface, taking into account the number of member states and the number of entities operating in their territory. This system must also take into account the modification of existing registers in the individual countries, or whether eIDAS must be compatible[39] to be applicable under the current legal situation.

In addition to tax law, the concept of Blockchain has not gone unnoticed also in customs administration. Meanwhile, it is clear, that information technology is taking on an increasingly important role in modern customs administration, but the priorities, expectations, experience, capacities and resources of individual customs administrations vary widely. Customs administrations fight fraud by demanding a high degree of accounting and reporting accuracy to support indirect taxation and customs declarations. The so-called "blocking technology" is also a step forward for customs in the 21st century, as it offers several opportunities for it, from collecting accurate data to automatically detecting customs evasion and fraud, as well as collecting customs. Where block chains allow sensitive or valuable data to be transmitted with accuracy and trust, it is no wonder that they are becoming increasingly common in everyday business processes.

The customs procedure takes place in certain phases – from the start of a customs procedure, through the identification of the documents for the decision, to the issuance of the substantive decision.[40] It is very important in the customs procedure to prove the veracity, credibility and completeness of all the documents required for the goods. The time and cost of clearing goods for import or export entails a significant financial burden on trade because of the number of permits necessary to import or export goods. These are various permits, licenses, phytosanitary certificates, and others that are required for health, human, animal or plant safety. The so-called "arbitrator" in border trade is the customs administration whose task is to ensure that all such authorisations are duly obtained, valid and the goods legally declared and that all regulatory requirements are met. In customs

administration, the documents, which describe or should describe the nature of the goods, and whether the goods comply with the required standards, play an important part. What if all steps in the supply chain from origin to destination were contained in Blockchain?!

Customs block chains would allow for comprehensive management of product life cycle data by providing a common platform where manufacturers, laboratories, logistics operators, regulators and consumers can fully access all related information such as demonstration, testing, certification and licensing. Blockchain technology would ensure that the electronic certificate is appropriately and properly issued and subsequently digitally signed by a valid regulatory/issuing agency. At the same time, the certificate would be protected from any risk of modification, misuse or tampering with its content. Consequently, it would only have to be verified whether there is any discrepancy between the data submitted by traders and the data that has been updated repeatedly in the public ledger. Depending on the unchangeable and trustworthy data that the customs authorities might have in the private sector network, they could distinguish between illegitimate and legitimate trade as much as possible without relying on their traditional risk management technique.

Blockchain technology is based on cryptographic evidence instead of trust, allowing parties to trade directly with each other without the need for a trusted third party. The truthfulness and reliability of the information contained in the documents is essential, but it is difficult to achieve certainty, as the necessary information is often provided by third parties and can be obtained from different systems. Errors can lead to penalties, loss of opportunities and costly delays in cross-border goods transport. One of the advantages of Blockchain technology is that there is *no intermediary* which means that decentralised ledgers reduce the need for trust based on third-party transaction verification, i.e. intermediaries, from transactions. The speed, accuracy and transparency of Blockchain could help alleviate this burden for taxpayers by reducing the risk of fraud. Traders are often obliged to provide additional information, documents (e.g. on the origin of goods), or documents which enable them to benefit from concessions or reductions in customs duties (e.g. through a free trade agreement). However, if these items were kept automatically in the block chain and the customs authorities had access to the chain, they could verify with complete accuracy the origin and nature of the goods at each stage of the chain. In short, the documentation and communication required for the transport of goods between continents would be largely automated and, at that, done with accuracy, security and reduced time and costs associated with these tasks. The launch of Blockchain would also significantly reduce the costs associated with documenting each step of customs authorities, the logistics process, transparency in terms of shipment delivery and the transfer of funds.[41]

Blockchain is a step forward in customs and trade that want more efficiency in their business. More specifically, the technology will help to ensure the customs security of legitimate trade, while also calling on customs and commercial authorities to simplify their tasks (often called "bureaucracy") that have been required to comply. Undoubtedly, Blockchain technology is a huge leap for customs in the 21st century.

3.2. Blockchain technology and real estate registration for tax purposes

Local taxes, including real estate tax, can be considered a relatively new but stable instrument in our tax system, even though their existence was already foreseen by the Slovak National Assembly Act no. 369/1990 Coll. on Municipal Establishment, as amended,[42] but most of all, Article 59(1) of the Constitution of the Slovak Republic[43] no. 460/1992 Coll., as amended.[44] Local taxes are taxes that citizens pay to their municipality to finance a wide range of public goods. However, with regard to local taxes, all citizens' taxes must be manually registered through private entities, logged in a database where the information is collected by the tax officials of the municipality. The citizens paying these taxes then "pass" through the banks to make the payment. All these methods are centralised and they are not automated.

Blockchain enables a decentralised and distributed system that allows you to track paid taxes, streamlines, and automates the process itself, and brings confidence to the system. The Real Estate Cadastre is a formal system that provides identification and location of real estate and records of the past, as well as current data relating to the respective piece of real estate. Many public services rely on data stored in the Real Estate Cadastre (hereinafter: REC). The main issues which the REC systems still face in many countries relate to the accuracy of the data stored in the REC and the effectiveness of the REC systems. Although all data stored in this information system should be credible and correct, this is not the case – inaccuracies or errors are usually the result of errors that occurred in the digitisation process. The Land Register provides answers to questions about who owns certain property and what legal document establishes the title. Cadastre is an official record of real estate data in a particular area, which is also significant for tax purposes.

Blockchain used for property records could be potentially applicable via smart contracts. In fact, smart contracts are written and stored in Blockchain (see above). Because they are stored in Blockchain, they are also immutable, so it should not be possible for anyone to have access to smart contract data stored in Blockchain technology. The simplest example could be that as soon as there is a change of ownership registered in the Land Register, the other involved institutions should be automatically informed of the change. For example, the tax administrator in whose district the property is located, could be automatically informed, but also, for example, utility companies that are entitled to be informed of a change in billing information from a certain date to another natural or legal person.[45]

At present, it is not unusual for computer programs to evaluate images. We also see the potential of Blockchain technology in synergy with other databases, by linking them together to automatically compare the real estate data recorded in Blockchain with the data obtained from satellite imagery. This could prevent (even by the verification of facts by local investigation) both illegal construction and the related tax evasion on real estate tax.

4. Conclusion

This paper aimed to confirm or refute the basic hypothesis – whether Blockchain technology is capable of contributing to more efficient tax and customs collection. Based on what we have presented here, we must conclude that the hypothesis has been confirmed.

Undoubtedly, Blockchain is an instrument (among others, also in the fight against tax and customs evasion) that the governments of individual member states can count on in the future. However, as things stand, there are a number of issues (both legal and technical), such as:

- protection of confidential data from hacking attacks
- respect for modifications in the existing registers and lists for tax purposes in the individual Member States
- eIADAS compatibility, and others

These must first be answered to make use of Blockchain in the public sector and to assist the states.

While lack of legal regulation makes this technology attractive to many, it is necessary for both national parliaments and the European Parliament to address this issue and establish minimum standards to create a legal framework for the use of Blockchain technology in the public sector.

It will also be difficult to find a suitable model, or Blockchain "public" architecture, which could be put into practice, not only at the European or national level, but also at the level of municipalities and cities. This need has already been identified by the European Parliament and, to this end, it has asked the European Commission, as well as the relevant working groups, in its Resolution of 24 November 2016 on towards a definitive VAT system and combating VAT fraud [2016/2033 (INI)],[46] to address the issue of "digital technologies", which should contribute to "filling" the VAT gap.

Only the future will show how the regulatory challenges of the EU and the member states will be dealt with and whether we can use modern technologies to our advantage or they will engulf us.

References

1 This paper was created as a partial output of the project solution vvgs-2019-1068 "Blockchain Technology as a Factor Affecting the Current Form of Law" and VEGA 1/0846/17: "Implementation of the Initiatives of the EU Institutions in Direct and Indirect Taxation and Their Legal Budgetary Implications".
2 Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System,* 2008, https://bitcoin.org/bitcoin.pdf (accessed 25 August 2019).
3 The concepts of "virtual currency" and "cryptocurrency" are not identical, but are used interchangeably for the purposes of this paper.
4 David Allessie, Maciej Sobolewski, Lorenzino Vaccari, *Blockchain for Digital Government,* Publications Office of the European Union (Luxemburg, 2019). https://doi.org/10.2760/942739
5 Zdenka Poláková, Peter Rakovský, Blockchain technológie – regulačné výzvy a príležitosti [Blockchain Technologies – Regulatory Challenges and Opportunities], 82 et seq., in *Zborník z medzinárodnej vedeckej konferencie Bratislavské právnické fórum 2018* [Collection of Papers from the International Academic Conference Bratislava Legal Forum 2018] (Bratislava, Univerzita Komenského v Bratislave, 2018).
6 The Scandinavian countries are pioneers here, while Estonia is definitely an interesting example of modern technology application within parameters similar to the Slovak Republic.
7 David Allessie, Maciej Sobolewski, Lorenzino Vaccari, *Blockchain for Digital Government,* Publications Office of the European Union (Luxemburg, 2019). https://doi.org/10.2760/942739
8 *How blockchain architecture works? Basic Understanding of Blockchain and its Architecture,* www.zignuts.com/blogs/how-blockchain-architecture-works-basic-understanding-of-blockchain-and-its-architecture/ (accessed 25 August 2019).
9 Zdenka Poláková, Peter Rakovský, Blockchain technológie – regulačné výzvy a príležitosti [Blockchain Technologies – Regulatory Challenges and Opportunities], 82 et seq., in *Zborník z medzinárodnej vedeckej konferencie Bratislavské právnické fórum 2018* [Collection of Papers from the International Academic Conference Bratislava Legal Forum 2018] (Bratislava, Univerzita Komenského v Bratislave, 2018).
10 Act no. 431/2002 Coll. on Accounting, as amended.
11 Ibid.
12 Of course, by this we do not mean an inability to check the individual transactions in another accounting period, as taxpayers are required to keep their accounting records for the period prescribed by law, but we wanted to point to the content of Blockchain and the accounting journal.
13 Act no. 185/2015 Coll. on Copyright, as amended.
14 Peter Vojčík et al., *Právo duševného vlastníctva* [Intellectual Property Law] (Plzeň, Aleš Čeněk, 2014).
15 Ladislav Hrabčák, Výzvy pre daňové právo v podobe Blockchain technológie [Challenges for Tax Law in the Form of Blockchain Technology] in *Zborník príspevkov zo 6. ročníka Jarnej internacionalizovanej školy doktorandov UPJŠ 2019* [Proceedings of the 6th Spring Internationalized School of PhD Students UPJŠ 2019] (Košice, ŠafárikPress, 2019).
16 Peter Vojčík et al., *Právo duševného vlastníctva* [Intellectual Property Law] (Plzeň, Aleš Čeněk, 2014).
17 The "open source" designation generally means that it is a computer software with so-called open source code.
18 Act no. 185/2015 Coll. on Copyright, as amended.
19 Of course, it also depends how consensus is achieved in the relevant network. This is typical of the Proof of Work method. See Ladislav Hrabčák, Výzvy pre daňové právo v podobe Blockchain technológie [Challenges for Tax Law in the Form of Blockchain Technology], 60, in *Zborník príspevkov zo 6. ročníka Jarnej internacionalizovanej školy doktorandov UPJŠ 2019* [Proceedings of the 6th Spring Internationalized School of PhD Students UPJŠ 2019] (Košice, ŠafárikPress, 2019).
20 Peer-to-peer phrase, which originates in English, refers to a decentralised communication model.
21 The weakened position of the state lies in the fact that Blockchain is decentralised in nature and as such is somewhat elusive to the state's full control.

22 Alexander Savelyev, *Contract Law 2.0: «Smart» Contracts as the Beginning of the End of Classic Contract Law* (Moscow, National Research University Higher School of Economics, 2016). https://doi.org/10.2139/ssrn.2885241
23 In judicial practice, this could cause considerable complications due to the lack of knowledge of the programming language by judges.
24 Theoretically, changes could be made by concluding a new smart contract (but without affecting the original contract) or if this option was directly incorporated in the source code.
25 Adam Zábranský, *Úvod do práva smart kontraktů – část 1* [Introduction to the Law of Smart Contracts – Part 1], www.epravo.cz/top/clanky/uvod-do-prava-smart-kontraktu-cast-1-109049.html (accessed 10 August 2019).
26 Stephen McJohn, Ian McJohn, *The Commercial Law of Bitcoin and Blockchain Transactions* (2016).
27 Act no. 40/1964 Coll. the Civil Code, as amended.
28 Alexander Savelyev, *Contract Law 2.0: «Smart» Contracts as the Beginning of the End of Classic Contract Law* (Moscow, National Research University Higher School of Economics, 2016). https://doi.org/10.2139/ssrn.2885241
29 Some academics regard smart contracts as a form of self-help. See Max Raskin, *The Law of Smart Contracts* (Georgetown Technology Review, 2017).
30 Adam Zábranský, *Základní právní aspekty smart kontraktů – část 2* [Basic Legal Aspects of Smart Contracts – Part 2], www.epravo.cz/top/clanky/zakladni-pravni-aspekty-smart-kontraktu-cast-2-109050.html (accessed 10 August 2019).
31 Zdenka Poláková, Peter Rakovský, Blockchain technológie – regulačné výzvy a príležitosti [Blockchain Technologies – Regulatory Challenges and Opportunities], 82 et seq., in *Zborník z medzinárodnej vedeckej konferencie Bratislavské právnické fórum 2018* [Collection of Papers from the International Academic Conference Bratislava Legal Forum 2018] (Bratislava, Univerzita Komenského v Bratislave, 2018).
32 Vladimír Babčák, *Daňové právo na Slovensku* [Tax Law in Slovakia] (Bratislava, Epos, 2015).
33 Miroslav Štrkolec, *Zabezpečovacie inštitúty pri správe daní* [Tax Administration Security Institutions] (Košice, Equilibria, 2017).
34 Grzegorz Poniatowski et al., *Study and Reports on the VAT Gap in the EU-28 Member States: 2018 Final Report TAXUD/2015/CC/131,* https://ec.europa.eu/taxation_customs/sites/taxation/files/vat-gap-full-report-2019_en.pdf (accessed 13 August 2019). https://doi.org/10.2139/ssrn.3272816
35 *Missing Trader Fraud,* https://en.wikipedia.org/wiki/Missing_trader_fraud#/media/File:Carrouselfraude.svg (accessed 13 August 2019).
36 Peter Šamko, *Daňové podvodné konania a ich dokazovanie* [Tax Fraud and Evidence] (Bratislava, Wolters Kluwer, 2015).
37 David Allessie, Maciej Sobolewski, Lorenzino Vaccari, *Blockchain for Digital Government,* Publications Office of the European Union (Luxemburg, 2019).
38 Ibid.
39 Petra Krupičková, Smart contract – revoluce v smluvním právu 21. století? [Smart Contract – Revolution in 21st Century Contract Law?], 26, in *Revue pro právo a technologie* [Revue for Law and Technology] (Brno, Masarykova univerzita v Brne, 2017). https://doi.org/10.5817/RPT2017-1-2
40 Karin Prievozníková, *Colné právo* [Customs Law] (Žilina, Knižné centrum, 2008).
41 Monika Stojáková, Eliminácia daňových a colných únikov vplyvom moderných technológií [Elimination of Tax and Customs Evasion due to Available Modern Technologies], 272–285, in *Vplyv moderných technológií na právo* [Effect of Modern Technologies on Law] (Košice, UPJŠ, 2019).
42 Slovak National Assembly Act no. 369/1990 Coll. on Municipal Establishment, as amended.
43 Constitution of the Slovak Republic no. 460/1990 Coll., as amended.
44 Vladimír Babčák, *Daňové právo na Slovensku* [Tax Law in Slovakia] (Bratislava, Epos, 2015).
45 Miroslav Stefanović et al., Blockchain and Land Administration: Possible Applications and Limitations, in *Proceedings of the 5th International Scientific Conference on Contemporary Issues in Economics, Business and Management EBM 2018* (Kragujevac, Faculty of Economics, University of Kragujevac, 2018).
46 European Parliament resolution of 24 November 2016 on towards a definitive VAT system and combating VAT fraud [2016/2033 (INI)].

Public Governance, Administration and Finances Law Review Vol. 4. No. 2. (2019) • 65–77.

10.53116/pgaflr.2019.2.5

Application Possibilities of Blockchain in Accounting

Péter Bálint Király*

* Dr. Péter Bálint Király, Internal PhD student of the Széchenyi István University in Győr, Faculty of Law, Department of Administrative and Financial Law. (e-mail: kiralypeterbalint@gmail.com)

Abstract: In recent decades technology has advanced rapidly, and inventions that have made our lives easier have emerged. Among the many life changing inventions, Blockchain facilitates our financial activities, for example banking, commerce and accounting, because it eliminates the need for a third party, thus saving us time and money. With its help, we can manage and record asset movements, contracts and their fulfilment, as well as other data by cryptographic methods. In the following article, firstly I will describe the concept and operation of Blockchain and the advantages of using it in the field of accounting. After that I will introduce the accounting principles, based on the Hungarian Accounting Act. Finally, I will address the legal questions raised by applying the accounting principles to Blockchain when they are used in the process of accounting.

Keywords: Blockchain; tax law; accounting

1. Introduction

In recent decades, technology has advanced rapidly, and inventions that have made our lives easier have emerged. In the following, I address the issue of Blockchain regulation, examining the legal challenges generated by technological innovation, including its impact on the current accounting regulation. Blockchain is already considered by many to be the most important invention of the 21st century and is compared to the Internet in terms of importance. Blockchain is essentially a decentralised or distributed ledger that, due to cryptographic procedures, is capable of authenticating transactions, without the need for an intermediary. Blockchain allows us to trust third parties we do not know and therefore do not have enough information about them. In the past, in order for this trust to exist, we needed an intermediary trusted by both parties to ensure that the other was not deceived. For example, we needed financial institutions in order to prove that we have the amount of money or collateral needed for a particular transaction. Blockchain systems eliminate the need for a third party, thus saving us time and money, while allowing everyone to access and supervise transactions carried out through Blockchain.[1]

Blockchain allows transactions to be made anonymously. Applying it can bring many benefits in different areas of life. The purpose of its creation was to eliminate the failures of the traditional financial intermediary system, and to provide a faster, cheaper and more secure way of conducting financial transactions. With its help, we can manage and record asset movements, contracts and their fulfilment, as well as other data by cryptographic

methods. In addition, it can ensure the transparency of transactions, verify the origin of goods, provide authorities with real-time, reliable and credible data, enable continuous collection of taxes immediately after a transaction without human intervention, etc. Its potential for use is endless and the recent emergence of Blockchain-based innovations has significantly accelerated, necessitating an examination of how Blockchain and other related technologies can be integrated into the current regulatory environment.

2. The Operation of Blockchain

In order to present the legal challenges, the concept and operation of Blockchain must first be described.

Blockchain is a distributed ledger or decentralised database that is publicly accessible and, through cryptographic procedures, authentically and unalterably captures recorded data (e.g. transactions) without any intermediary, in a merely peer-to-peer way.[2]

Blockchain is an implementation of Distributed Ledger Technologies (DLTs).

The Distributed Ledger Technology is a database based on a technology that enables the content to be simultaneously accessed, modified and authenticated by authorised personnel and, upon agreement, to be copied, shared and synchronised between participants, regardless of geographic boundaries. The essence of a centralised software system is that there is a central node (central computer) and all other nodes (computers) are connected to the central node, but these other nodes are not directly connected to each other. In contrast, in a distributed/decentralised system, like a blockchain, nodes (computers) are connected to each other without any central node among them. That is, the nodes communicate directly with each other, and not through a central node.

Blockchain is essentially a so-called peer-to-peer protocol, which means that it is a computer network whose users (or rather their computers functioning as nodes) communicate directly with one another without a central node (computer). P2P systems are distributed software systems that consist of nodes (computers) and thus make their computing resources (e.g. processing speed, storage, information distribution) directly accessible to others. When connected to a P2P network, users' computers become equal nodes in the system in terms of their roles and privileges. Although users are different in terms of available resources, all nodes in the system have the same functional capabilities and the same responsibility. As a result, all users' computers are both service providers and consumers.[3]

The above properties mean that anyone can join Blockchain, and once connected, initiate transactions directly to each other, anonymously. Transactions are also authenticated by users through their computer capacity made available to Blockchain. During this process Blockchain wraps the information about the transactions in so-called blocks, and then these blocks are added to the Blockchain that serves as the ledger. An essential element of this process is the so-called consensus mechanism, which is needed to get computers to agree on Blockchain updates so that all computers will then have the same Blockchain data content.[4]

How does it work? I would like to illustrate the operation of Blockchain through the example of the Bitcoin–Blockchain Proof of Work consensus mechanism. The data about transactions are gathered into blocks every 10 minutes. Then the transactions included in the new block are authenticated by the nodes (e.g. they confirm that the buyer actually had the needed amount of cryptocurrency available for the transaction).[5] Thereafter, the transaction data set of the new block is supplemented by the so-called "header" of the previous block. This header actually works like a personal number. Each block has a unique header through which it can be identified. This means that each block refers to the preceding block and consequently the chain of transactions can be traced back to the original block containing its first transactions. Once the header of the previous block is added to the new block, the data contained therein begins to be encrypted by solving a cryptographic puzzle.[6] (Cryptography was originally equivalent to encryption, but today it has become a stand-alone mathematical-informatics science, which is about protecting information by transforming and transmitting information, text and messages in a way that only those can understand, to whom the message was intended.) All the blockchain-running computers (the so-called miners) compete on which one can solve this cryptographic puzzle the fastest, because the first one to solve receives Bitcoin (or other cryptocurrency in case of other Blockchain systems) for their work. The new block is then added to the blockchain and shared on all computers in the system.[7]

When a sufficient amount of computer power is provided, Blockchain is able to record transactions reliably, as the entire Blockchain is constantly updated and shared among network members. That means that every single moment any participating computer can verify every transaction that has been recorded.[8] Recorded transactions are virtually immutable once added to the Blockchain. This is because the complete Blockchain is present on all computers and each block refers to the preceding block. This means that if a hacker wants to change a transaction, they need to change not only the block that contains that transaction, but also the next one, and then the next one, and so on, since all blocks contain the header of the previous block. In addition, these changes would have to be made on more than half of the nodes of the Blockchain, since more than half of the computers are needed to reach consensus about transactions.[9]

3. Advantages of the Blockchain Technology in Accounting

The essence of accounting and auditing is to create mutual trust and to provide protection for investors. That is why the requirement of double-entry accounting has been introduced, which ensures the accuracy of the recorded data. As business companies grew and evolved, they increasingly needed external financial resources. However, investors only provided capital to a business company if they saw that their investment was paying off. The easiest way to check this was if the company in which they were investing disclosed information about their activities. Due to the information asymmetry between the company and the investor, the company can easily manipulate the data. This is why there is a need for external auditing of accounts, which can reduce information asymmetry and increase trust

and thus the value of the company. Of course, conducting an external audit to detect accounting errors and fraud is also in the interest of the business, since the decision of potential investors is greatly influenced by whether they can rely on the information disclosed by the business. Because external auditing is done by people, it is not perfect either: it reduces the risk of errors and fraud, but it cannot detect all.[10]

The digitisation of accounting activities may provide a solution to this. However, this is made more difficult by the complex set of legal requirements which require, among other things, the authenticity of the recorded data. The purpose of the accounting rules is to prevent the possibility of forgery and the recording of false or misleading information. This is ensured by, among other things, various regular checks, extensive documentation of data, double-entry bookkeeping, etc., all of which are labour-intensive and costly activities and difficult to automate. At least that was the case until Blockchain appeared.[11]

As is clear from its concept, Blockchain is a technology that functions as a general ledger for transferring ownership and recording accurate financial information. The focus of the accounting profession's activities is to record, measure and communicate financial information, property rights and obligations, and to analyse that information. Based on this data, accounting professionals plan the best allocation of financial resources. For accountants, using Blockchain can greatly improve efficiency by reducing the cost of maintaining and reconciling ledgers, and reliably recording transaction chains and ownership of assets.

Applying Blockchain can help accountants' work by making the resources, rights and obligations of companies more transparent. In addition, it saves time for accountants, as transactions need not be recorded by accountants, as Blockchain will do it.[12] Blockchain technology can also facilitate compliance with legal requirements, for example by assisting in double-entry bookkeeping, and the authenticity of recorded data no longer has to be verified by an external actor (auditor), as the Blockchain itself provides this.[13] In addition, with the help of Blockchain, all of these activities are performed by the program itself without the need for an intermediary, in a transparent, secure, reliable and tamper-proof manner.[14] The focus of the accountants' activities is thus expected to shift from data accounting to planning and the evaluation of Blockchain data. Blockchain is not able to answer all the questions that arise during the activities of a company. For example, you can credibly prove who owns an asset, but its value, condition, method of accounting, and placement in each category of financial statement still need to be determined by experts.[15]

4. Accounting Principles

Below I present the accounting principles required by Act C of 2000 on Accounting (hereinafter: Sztv.).

The basic principle of the Sztv. is the *principle of going concern,* which means that drawing up the financial report and the accounting records shall be based on the assumption of the economic entity's capacity to sustain operations in the foreseeable future and on its ability to continue its activity, and the termination of or a considerable reduction, for any reason, in the operation is not expected.[16] It assumes that the business is created to operate profitably in the long run. The other principles must also be interpreted in this light.

According to the *true and fair view principle,* assets shown in the books and contained in the financial report shall be such that they can be found and verified as in fact being in existence, tenable and verifiable. The measurement of such assets shall be carried out in accordance with the valuation principles prescribed in the Sztv., as well as with the relevant valuation procedures.[17]

Based on the *principle of completeness,* economic entities shall keep accounts of all economic events, the effect of which on the assets and liabilities, as well as on profits, are to be shown in the financial report, including the economic events which pertain to the financial year in question that became known after the balance sheet date but before the date of closing, as well as the ones generated by the economic events of the financial year ending on the balance sheet date, that had not yet taken place prior to the balance sheet date but became known prior to the closing date of the balance sheet.[18]

According to the *principle of prudence,* no profit shall be recognised where the financial realisation of the revenues and certain items of income are uncertain. When determining the profit or loss for the year, foreseeable liabilities and potential losses shall be taken into account and shall be covered by provisions, even if such liabilities or losses become apparent only between the date of the balance sheet and the date on which it is drawn up. Depreciation impairment losses shall be accounted for, regardless of whether the income statement for the year shows a profit or a loss.[19]

The *principle of matching* means that when determining the profit or loss for a certain period of time, the revenues recognised for a given period of activities and the costs (expenditures) directly associated to such revenues shall be taken into account, regardless of the financial settlement. The revenues and costs shall relate to the period in which they were incurred for economic purposes.[20]

Based on the *principle of accruals,* the consequences of economic events concerning two or more financial years shall be recognised under the revenues and costs of the period in question in the proportion in which they are incurred between the underlying period and the accounting period.[21] For example, if a business leases an office for 3 years and receives a 3-year lease in advance, it may not account for the full 3-year rent for the year it was issued, but only show 1/3 of that year.

According to the *principle of grossing up* with the exceptions laid down in the Sztv., revenues and costs (expenditures), and receivables and liabilities may not be set off against one another.[22] This means that liabilities, receivables and revenues should be recorded separately, because if these could be offset, the data would no longer give a credible picture of the company.

The *principle of substance over form* means that in the financial report and in the relevant accounting records, economic events and transactions shall be shown and accounted reflecting their economic substance and in accordance with the basic principles and relevant provisions of the Sztv.[23] This means that in accounting, not the legal content is primary, but the economic. However, when recording economic events and transactions, the principles of the Sztv. and the relevant regulations must be followed. (For example, in the case of a finance lease, the leased asset must be shown to the lessee, even though the legal ownership of the asset is with the lessor. Because the lessee possesses the asset in the economic sense of the asset as if it were the owner, it will order the lessee to account for it.)

According to the *principle of valuation on an item by item basis,* assets and liabilities shall be entered and evaluated item by item in the course of bookkeeping and preparing the report. That is, each item must be separately identified and recorded as specified in the accounting policy of the company.[24]

The *principle of materiality* means that for the purposes of the financial report, information is material if its omission or misstatement could influence – within reason – the economic decisions of users taken on the basis of the financial report. The materiality of individual items shall be assessed in the context of other similar items. It is the entity's responsibility to determine in its accounting policies exactly which information is material to that particular entity.[25]

Based on the *principle of cost–benefit,* the usefulness (utility) of any information published in the financial report (balance sheet, profit and loss account, notes on the accounts) shall be commensurate with the costs of producing that information.[26]

According to the *principle of consistency,* in respect of content and formal requirements, and of the financial report and the underlying accounting records, constancy and comparability shall be provided for.[27] Compliance with this requirement is facilitated by the models annexed to the Sztv. and the EU Directives.

The *principle of clarity* means that the accounting records and the financial report shall be prepared in a concise, comprehensible form in accordance with the Sztv.[28]

Based on the *principle of continuity,* the opening data of a financial year shall be identical to the corresponding closing data of the previous financial year. In consecutive years the valuation of assets and liabilities, and the assessment of profit of loss may be altered only in accordance with the relevant provisions of the Sztv.[29] If the valuation principles applied in the process of drawing up the balance sheet for the previous year have been changed, the factors causing the change, and the quantified effect thereof shall be detailed in the notes on the accounts.[30]

5. The Application of the Accounting Principles on Blockchain

In the previous chapters, the operation of the Blockchain technology, its conceptual basis, the advantages of its application in the field of accounting, and the accounting principles have been described. Blockchain, while it automates bookkeeping, creates the necessary trust between the parties without resorting to intermediaries and saves us time and money, but does not solve all the problems. Indeed, from a legal point of view, many issues need to be addressed. In the following, I will address the application challenges of Accounting Principles on Blockchain.

In my opinion, among the accounting principles described above, there are those that are not influenced by whether a particular company uses Blockchain or traditional tools for accounting.

The *principle of going concern* is also relevant in case of Blockchain, since accounting must continue to be based on the fact that the enterprise is engaged in business indefinitely and thus can continue to operate in the foreseeable future.

The *principle of substance over form* is also an inescapable principle. It requires that in the financial report and in the relevant accounting records, economic events and transactions shall be shown and accounted reflecting their economic substance and that the principles and relevant requirements of the Sztv. should be followed. In my view, adhering to this principle is only a matter of programming.

The same is true of the *principle of completeness,* since the accounting technology does not change the fact that an enterprise is required to account for all economic events that have an impact on its assets and liabilities and on the profit or loss for the current year. Because economic events are recorded in real time, the economic events which pertain to the financial year in question that became known after the balance sheet date but before the date of closing are definitely recorded. However, it should be noted that, with proper programming, the technology can be used not only to look at periodic balance sheets and profit and loss statements, but also to take a look at the current financial position of the enterprise at any time.

However, there are also some principles that are easier to comply with by the use of Blockchain.

The *principle of clarity* requires that the accounting records and the financial report be clear and understandable. Blockchain makes it easier to produce various statements and statistics that help you understand the financial position and activity of a particular enterprise.

According to the *principle of prudence,* it is forbidden to recognise a profit if the revenue, the financial realisation of the income is uncertain. The essence of Blockchain is to verify that a financial transaction has actually taken place, so applying it excludes the recognition of a profit for which the financial realisation of revenue is uncertain.

The obligations set out in the *principles of matching and continuity* – that last year's closing data should be consistent with next year's opening data, and that revenues and expenses should relate to the period in which they are economically incurred – can also be easily met, as Blockchain records the chain of economic events that have already taken place. It must be noted that, if the Blockchain data capture methods change as a result of changes in the legal environment or accounting policies, then, in accordance with the principle of continuity, its quantified effects must be disclosed separately.

Compliance with the *principle of grossing up* is not a problem either, as the individual transactions in the Blockchain are recorded separately. In this respect, states must ensure that the participants in the transactions do not make an agreement outside the Blockchain, and not just transfer the amount determined as a result of the set-off. The same applies to the *principle of valuation on an item by item basis,* as Blockchain is able to record individual items separately in a way specified in the accounting policy.

In accordance with the *principle of materiality,* only material financial events need to be recorded in the financial reports. With the help of Blockchain, not only the material but all economic events can be recorded. However, it is debatable whether we really want all the data to be included in the report, as it is important to maintain transparency. Nonetheless, the technology allows us to authentically record and store a large amount of data and to produce reports and statistics on different subjects that meet the needs of the user.

According to the *principle of cost–benefit,* the usefulness of the information disclosed should be proportionate to the cost of producing the information. In my view, Blockchain can widen the scope of information to be provided, as it can produce more information at a lower cost about companies. All of this can be beneficial to investors, as companies become more transparent.

However, compliance with the *principle of accruals* may be problematic because transaction data are immediately recorded in the Blockchain and there is no possibility to recognise economic events concerning two or more financial years under the revenues and costs of the period in question in the proportion in which they are incurred between the underlying period and the accounting period. Of course, this is really only a matter of programming, but it should be reconsidered whether this principle should be applied to companies using Blockchain. Similarly, consideration should be given to whether the principles associated with a specific time period are relevant to a system that provides data at any time, for any time period, and whether changes in the financial state of the company in question can be tracked in real time.

Based on the *principle of consistency,* enterprises shall provide the consistency and comparability of their accounting records and financial reports. In connection to this, the issue of interoperability arises. Currently, individual states have begun to develop their Blockchain on their own, which are governed by their own laws. This can cause problems for companies involved in international trade or with subsidiaries. These must apply the Blockchain of each state in which they operate in order to comply with the regulations of each state. It would therefore be advisable to set up an international Blockchain that complies with international accounting standards. This, of course, first and foremost requires the creation of a fully unified international system of requirements. Alternatively, we may create a method that can easily convert data from one national Blockchain to another.

The biggest challenge, in my opinion, is to comply with the *true and fair view principle.* It can be problematic that the integrity of the recorded data can be assured only if more than half of the computer capacity connected to the system is owned by the state (or at least by a person or body whose good faith is beyond doubt). Blockchain, as explained above, is a distributed ledger that we can trust because all the computers in the network have the registered data, and it is theoretically impossible to change the data set because in order to do so one needs to hack all computers (or at least more than half them). In case of Blockchain, we do not have to rely on a specific person or institution (as it is not a specific person or institution doing the registration tasks), but on the system itself, on the code of the program. Blockchain is thus potentially suitable for replacing intermediaries in different fields.

The disadvantage of Blockchain systems is that Blockchain can only guarantee the integrity of the input data, but not the authenticity of the input data. So, even if we can make sure that no one has tampered with the input, we still cannot use Blockchain to ensure that the input is accurate.[31] The Blockchain network authenticates the different facts and data with the agreement of the individual nodes, but it can just as easily happen that there is an agreement between the members of the network regarding a fact or data that is not true. From this point of view, Blockchain can also be "hacked" not in the traditional

sense, not by altering the data stored in the Blockchain, but by including false information in the block.[32]

It should also be noted, however, that this problem also arises with the accounting methods currently used, since accountants may enter incorrect or even false data in the ledger. As explained above, that is the reason why the institution of audit was introduced. At this point, the problem arises that, if the data recorded on the Blockchain is also audited by an outsider institute (i.e. auditor), then we have essentially brought back a centralised element into the Blockchain system, which is otherwise based on the principle of decentralisation. Although legally it is completely acceptable, because it is one of the most important goals of accounting principles to ensure the accuracy of the data. However, Blockchain is created precisely for the purpose of directly capturing the necessary data in a system without the involvement of an intermediary (in this case, an auditor, and, moreover, the state), whereby the program itself creates trust between the parties. Subsequent state control over the data registered thus goes against the very essence of Blockchain, the introduction of which would certainly face considerable opposition amongst the Blockchain enthusiasts.[33]

6. Further Challenges: Immutability of the Recorded Data

The essence of the right to forget is that everyone should have the right to request the deletion of their data if its use does not comply with data protection rules.[34] Furthermore, there may be cases where the law states that after a certain period of time stored data must be deleted from the register. In addition, data is uploaded to the system by people and people make mistakes, so we cannot rule out incorrect data entry, which may also need correction. What happens if I enter data incorrectly? How can the data be erased or corrected in a system that relies on the fact that the input data cannot be deleted or modified later? The data once added to the Blockchain cannot be changed or deleted, or at least a so-called hard fork is required to do so.[35] Hard fork is used when the Blockchain protocol is modified in such a way, that a previously created block becomes invalid. This can virtually delete previously recorded data in the event of an error. Of course, this also requires the consent of the majority of the nodes.[36]

This raises another problem: what happens when, despite a legal provision or a judicial or regulatory decision, developers cannot delete data stored in the Blockchain due to a lack of consensus? What happens, for example, if a central bank's decision in the interest of inflation cannot be enforced on the Blockchain because users are voting against it? And what happens if users will not collect the tax that the state intends to collect on the Blockchain? In this case, the members are risking of acting illegally. The consequences of invalidity and nullity could be applied as civil law consequences. That is, they create a chain of virtually void contracts on the Blockchain by not modifying the Blockchain protocol in line with changes in legislation. In practice, this will motivate the community to vote in favour of the amendment, as a chain reaction would also jeopardise the validity of their contract. But who can say that a transaction or Blockchain as a whole is illegal? In case of a DAO, it is practically the community, not a court of justice. (The development of smart

contracts itself has the effect that instead of the court, the program itself says that a party has behaved in an unlawful manner.) But what happens when users abuse their power to vote for a hard fork, though no illegal activity occurred, but they do have an interest in overwriting previous transactions?

A related problem is whether the Blockchain and the code as the law principle are almighty. In principle, all contracts can be rewritten into smart contracts that are self-executing, meaning you do not have to go to court in case of a legal debate. In case of an interest on late payments, this works easily: if the buyer does not pay until the 31st of July, the purchase price paid by the buyer will be automatically increased by the amount of the interest on late payments. But what happens, for example, in case of an accident? A smart contract cannot tell who is responsible for the damage. That is, if, for example, we turn an insurance contract into a smart contract, then who tells the smart contract that the insured person actually caused the damage, and so the insurance amount is due. How can a cooperation obligation be coded? It cannot be written in bits because certain legal concepts are so complex that they cannot be simplified into logical (yes or no; if... then... because if not...) relationships. How could a code be a law if the legislators themselves or the lawyers drafting the contract are not able to incorporate all life situations and their legal solution into law or contracts? Why do we think programmers can do this? (Of course, this is only true as long as we do not have artificial intelligence capable of analogy and thus able to interpret complex concepts from the previous case law, such as equity.)[37]

This leads us to the conclusion that there is still a need for an external body (courts or authorities) with appropriate authority, control, oversight and rights to decide that a transaction, a combination of transactions and the operation of the Blockchain itself is unlawful or not. This decision must also be enforceable in such a way that the unlawful act cannot be lawfully continued, that is, it cannot legitimise the block that needs to be modified in the system (e.g. by continuing the Blockchain based on an illegal transaction, like in the case of Ethereum). From this point of view, it would be advisable for both courts and authorities to operate in a Blockchain, and when a decision is made, it would be included in the system.

So, in the end, we reintroduced the state as the third party. Of course, the problem here (which is not primarily legal, but more technological in nature) is how the state, a centralised power, can enter into a decentralised system in which the basic principle is the lack of intermediary institutions and independence from any central power? How can the benefits of a decentralised organisation be secured in a way that, if necessary, the state intervenes in the Blockchain? After all, allowing the state at any time to interfere with the operating principles of the Blockchain or the data recorded therein immediately raises the risk of abuse and corruption.

7. Conclusion

Blockchain can bring about changes that make life much easier for us. For this reason, we can safely consider it the most important invention since the advent of the Internet. In my paper I introduced the operation and conceptual foundations of Blockchain. I thought it

necessary to explain it because, in my opinion, only by understanding its operating mechanism can we identify the points of legal concern and ask the relevant questions. As stated above, Blockchain is essentially a decentralised or shared ledger that, due to cryptographic procedures, is capable of authenticating transactions, without the need for an intermediary or body.

All in all, Blockchain allows us to rely on third parties that we do not know and about whom we do not have information affecting our risk-taking, even without recourse to intermediaries. Due to all these features, Blockchain can fundamentally change the field of accounting as they save businesses time and money while providing the state and investors with reliable data about businesses and their operations, all this in real time. As explained above, Blockchain is fundamentally consistent with accounting principles, but we must also see that it does not solve all the problems and, in fact, raises a number of issues from a legal point of view. Among these are the challenges related to the authenticity and immutability of the recorded data, interoperability, business secrets and jurisdiction.

The issues raised cannot be left unanswered, and their solution is even more needed, as the technologies described above are used more and more widely. Just think about the fact that even the largest audit firms have already begun to develop their own Blockchain because they do not want to lag behind in innovation competition.[38] The process initiated by Blockchain is irreversible. The question therefore is, first and foremost, how lawmakers respond to the phenomenon. In this respect, I believe that the most important thing is to find an internationally coherent solution, since Blockchain is a cross-border innovation providing a service across the world via the Internet. Uniform regulation could ensure that the economic potential of Blockchain can be exploited more smoothly. However, legislators should also make sure that the regulations they introduce do not hinder innovation, but support, where possible, the development of Blockchain and related technologies.

References

1 Joseph J. Bambara, Paul R. Allen, *Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions,* 15 (New York, McGraw-Hill Education, 2018).
2 Primavera De Filippi, Aaron Wright, *Blockchain and the Law: The Rule of Code,* 13–14 (London, Harvard University Press, 2018). DOI: https://doi.org/10.2307/j.ctv2867sp
3 Daniel Drescher, *Blockchain Basics – A Non-technical Introduction in 25 Steps,* 23 (New York, Apress, 2017). DOI: https://doi.org/10.1007/978-1-4842-2604-9
4 David Schwartz, Noah Youngs, Arthur Britto, *The Ripple Protocol Consensus Algorithm* (2014).
5 Mayukh Mukhopadhyay, *Ethereum Smart Contract Development – Build Blockchain-based Decentralized Applications Using Solidity,* 15–18 (Birmingham, Packt Publishing, 2018).
6 Drescher, *supra n.* 3, at 23. https://doi.org/10.1007/978-1-4842-2604-9
7 Don Tapscott, Alex Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business and the World,* 28–32 (London, Portfolio Penguin, 2016).
8 Hossein Kakavand, Nicolette Kost De Sevres, Bart Chilton, *The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies,* 4–5 (2016). https://doi.org/10.2139/ssrn.2849251
9 Sarah Wurfel, Blockchain is unhackable but these are 5 possible vulnerabilities of "the new Internet", in *Blockchain Crypto Journal,* December 1 (2018).
10 Ting Yu, Stanley Lin, Qingliang Tang, Blockchain: The Introduction and Its Application in Financial Accounting, in *The Journal of Corporate Accounting & Finance,* vol. 29, no. 4 (2018). DOI: https://doi.org/10.1002/jcaf.22365
11 Deloitte, *Blockchain Technology. A game-changer in accounting?* www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Blockchain_A%20game-changer%20in%20accounting.pdf (accessed 18 August 2019).
12 ICAEW, *Blockchain and the future of accountancy,* www.icaew.com/technical/technology/blockchain/blockchain-articles/blockchain-and-the-accounting-perspective (accessed 18 August 2019).
13 Deloitte, *supra n.* 11.
14 Yu, Lin, Tang, *supra n.* 10. https://doi.org/10.1002/jcaf.22365
15 ICAEW, *supra n.* 12.
16 Sztv. 15 § (1).
17 Sztv. 15 § (3).
18 Sztv. 15 § (2).
19 Sztv. 15 § (8).
20 Sztv. 15 § (7).
21 Sztv. 16 § (2).
22 Sztv. 15 § (9).
23 Sztv. 16 § (3).
24 Sztv. 16 § (1).
25 Sztv. 16 § (4).
26 Sztv. 16 § (5).
27 Sztv. 15 § (5).
28 Sztv. 15 § (4).
29 Sztv. 15 § (6).
30 Sztv. 46 § (2).
31 Péter Bálint Király, A blokklánc-technológia nemzetközi kereskedelmi jogi összefüggései, 27, in *Külgazdaság,* vol. 63, no. 3–4 (2019).
32 Mike Bullock, *Blockchain in Plain English* (2017).
33 Király, *supra n.* 31, at 27.
34 Robert Kirk Walker, The Right to be Forgotten, 272, in *Hastings Law Journal,* vol. 64, no. 1 (2012). http://dx.doi.org/10.2139/ssrn.2017967
35 Bambara, Allen, *supra n.* 1, at 79–80.

36 Philipp Hacker, Corporate Governance for Complex Cryptocurrencies? A Framework for Stability and Decision Making in Blockchain-Based Organizations (November 22, 2017), 140–166, in Philipp Hacker, Ioannis Lianos, Georgios Dimitropoulos, Stefan Eich (eds.), *Regulating Blockchain. Techno-Social and Legal Challenges* (Oxford, Oxford University Press, 2019). DOI: https://doi.org/10.2139/ssrn.2998830

37 Josias N. Dewey, Shawn S. Amuial, Jeffrey R. Seul, *The Blockchain: A Guide for Legal and Business Professionals,* 49–50 (Danvers, MA., Thomson Reuters, 2016).

38 Stephen O'Neal, *Big Four and Blockchain: Are Auditing Giants Adopting Yet?* (2019).

Public Governance, Administration and Finances Law Review Vol. 4. No. 2. (2019) • 78–85.

10.53116/pgaflr.2019.2.6

Budget Allocation of Taxes to Territorial Budgets

Ivana Pařízková*

* JUDr. Ivana Pařízková, PhD, Department of Financial Law and Economics, Faculty of Law, Masaryk University, the Czech Republic. The author specialises in Financial Law, Budget Law and Tax Law. (e-mail: ivana.parizkova@law.muni.cz)

Abstract: The contribution deals with the financing of territorial self-governing units in the Czech Republic. The economic basis of local governance is still the most important and the most complicated issue of local governance. Local governances need economic independence for filling their tasks. The aim of this paper is to describe the importance of budget allocation of taxes (BAT) for municipal and regional budgets in the Czech Republic and, on the basis of description and critical analysis or comparison and synthesis of acquired knowledge, to confirm or disprove the hypothesis that partial amendments to the Act on Budget Allocation of Revenue of Certain Taxes to territorial budgets damage municipalities and regions or, on the contrary, strengthen their permanent financial basis. Description, analysis and synthesis are used as a method for writing this article.

Keywords: budget allocation; public sector; territorial self-governing unit; the budget; the Czech Republic

1. Introduction

The issue of territorial budgets is a topic that is not satisfactorily addressed by law and, as a result, it is often very thorny and debatable, although there are amendments to the law every year or new laws are created. As an example, we can mention Act No. 23/2017 Coll. on the Rules of Budgetary Responsibility, as amended. However, problems still arise as to how much entitlement can be granted to these self-government institutions and how many levels the self-government should have. In order for these self-government units to carry out their tasks and to avoid the disproportionate interference of the state in their activities, these self-government units must necessarily have economic independence, i.e. they must have their own assets and their own funds (resources). This is the so-called economic basis of a municipality and a region, within which the municipality and the region operate independently, under the conditions stipulated by special regulations.[1] The Act on Municipalities and the Act on Regions define the conditions of the economy only in a framework. They generally refer to the property of municipalities and regions, establish the right of municipalities and regions to manage, based on a contractual principle, also with the property of other entities, and impose on municipalities and regions the obligation to manage according to the budget.[2]

Budget allocation of taxes in the Czech Republic or tax allocation as stated in specialised literature determines to which budget the relevant tax or part thereof flows. Tax revenue and, therefore, budget allocation of taxes play a decisive role in terms of revenue of municipal and regional budgets and have a significant impact on their financial stability and autonomy. It is also true that this revenue is not in any way assigned.

Specialised literature often discusses whether budget allocation of taxes is a subsidy or transfer, and what can be considered transfers and subsidies.

In order to be able to answer what is the budget allocation of taxes, first of all, we need to make a brief description of the concept of transfer and subsidy.[3]

Generally speaking, a transfer means transferring capital and, in terms of economics, is considered to be a government payment to other entities for which the government does not receive consideration in the form of production factor services owned by the entities. Transfer payments include, for example, payments of old age and disability pensions, child allowances, maternity allowance or unemployment benefits. Transfer payments in this model are independent of the size of the total pension. A subsidy in economics means a financial donation or a financial reimbursement similar to the donation by the state or territorial self-government unit to the relevant entity, in order to reduce the price of a particular property the provision of which is in the "public interest". For our needs, it is important that the concept of subsidy is defined by budget rules providing that a subsidy means funds of the state budget, state financial assets or the National Fund provided to legal or natural persons for the intended purpose and, at the same time, the law stipulates that the subsidy or refundable financial assistance is not a legal claim unless a specific regulation stipulates otherwise.

Budget allocation of taxes is not a typical subsidy since funds from the collection of taxes are reallocated by determining a specific share for a territorial self-government unit based on a mathematical formula according to established criteria. The state has decided to leave some means of tax revenue to entities other than the state, even though they are derived from it to a certain extent. It is a manifestation of fiscal decentralisation, when decentralisation ensuring the degree of financial self-sufficiency of territorial self-government units takes place in addition to decentralisation of the performance of public administration (powers and activities). Budget allocation of taxes, often abbreviated to BAT, does not constitute direct financial flows between the state budget and territorial budgets, since the collection of the statutory and allocated taxes is immediately divided into precise shares. Reallocation takes place immediately after a selection phase, i.e. before the volume of selected funds becomes part of a specific public budget. Budget allocation is certainly a crucial element in defining the links between the state and territorial self-governments in general. The discussion is conducted in the sense of what is considered separate tax revenue and when it is a transfer.[4]

Most confusion is caused by taxes or the share of their revenue. Two situations can be distinguished. If the competent territorial self-government unit can affect the level of taxation by means of certain structural elements of tax such as tax rates or adjusting the tax base of the tax imposed, such revenue is considered to be a separate tax revenue of that territorial self-government unit. However, if a territorial self-government unit has no influence on the structural elements of a tax and this influence is realised only by the central

government, then the reallocation or allocation of selected revenues is made according to the established criteria.[5] In this case, such allocation, i.e. the distribution of tax revenue, can be designated as a transfer.[6] If we accept the tax revenue differentiation thus set, the tax revenue from real estate intended for municipalities will remain the only tax revenue in the true sense of the word for a territorial self-government unit in the Czech Republic. Other so-called tax revenues are already based on the setting of the budget allocation of taxes where the recipient, region and municipality will receive only the determined proportion of tax revenue according to the rules laid down by the law.[7]

The most important law determining the autonomous revenues of territorial self-government units is Act No. 243/2000 Coll. on Budget Allocation of Revenue of Certain Taxes to Territorial Self-Government Units and to Certain State Funds (the Act on Budget Allocation of Taxes), as amended, which is to ensure their fiscal sufficiency. The existing act allocates tax revenue in such a way that the state budget and territorial self-government budgets are balanced and their fiscal volume develops relatively in agreement. This requirement is achieved by an extended portfolio of shared taxes, which in practice means that the share of municipalities and regions is secured both on progressive taxes and regressive taxes.[8]

Given that tax revenues represent about half of the total revenues in municipalities and regions, it is appropriate to perceive changes in their development since 1993, i.e. since the establishment of the independent Czech Republic and the adoption of a new tax system, and also to see the causes of the necessary changes in budget allocation of taxes to municipalities and regions in particular periods.[9]

2. The Concept of Budget Allocation, Shared and Assigned Taxes

Budget allocation generally means either legally defined types of taxes that flow directly to the budgets of municipalities and regions or the statutory share of municipal and regional budgets in the national tax revenue. The issue of budget allocation of taxes is closely related to fiscal decentralisation, which accompanies the general organisational principle in public administration, namely the decentralisation of powers and activities. It is a necessary condition for mutually autonomous decision-making of individual levels of management. Depending on the degree of fiscal decentralisation, we can also assess the applied model of fiscal federalism in the given budget system. The most common, combined model sets own revenues for each level of management and government level, and budget allocation of taxes plays an irreplaceable role in this matter. It is used to determine the extent of financial autonomy of these individual government levels, especially regional and local self-governments.[10]

From a theoretical point of view, the combined model can be divided into:

- a combined model of fiscal federalism with predominant centralising elements in which most of the revenue is concentrated in the central budget from which subsidies are provided to other segments of the public budget system
- a combined model of fiscal federalism with predominant decentralising elements, where the importance of territorial self-governments is strengthened particularly through the determination of a larger part of separate revenue and thus greater self-sufficiency[11]

These divisions are already somewhat redundant in terms of public finances because finding a boundary between the two combined models will be rather complicated. It is sufficient for our needs to realise that in the combined model of fiscal federalism, there is a partial decentralisation of public revenues at lower levels of government, the intensity of which varies greatly in individual cases. There is no uniform view of theoreticians and economists as well as political representation in this matter, where the degree of self-sufficiency is often an ideological argument of supporters of one or the other prevailing tendency.[12]

Some authors describe situations where lower government levels have the direct authority to collect and impose taxes and bear responsibility for expenditures as fiscal decentralisation. By contrast, a mere reallocation by allocating centrally collected taxes to lower levels is called administrative decentralisation.[13]

For example, Michal Radvan holds a similar view, pointing to occasional changes in the economic autonomy of municipalities, so that municipalities can decide not only on local self-government expenditure but also on revenue by influencing the amount of tax revenue. In his opinion, municipalities are not able to correct the amount of tax revenue, except for local taxes and real estate taxes. According to him, everything has been set by the legislator in a fixed manner.[14]

On the other hand, it is not appropriate to narrow the issue of fiscal decentralisation to only the fiscal competence of territorial self-government units, i.e. the issue of local taxes. A manifestation of fiscal decentralisation is also the budget allocation of taxes, even though it is a decentralisation stipulated by law according to well-defined criteria. The specified shares of the allocated tax revenue were not determined by the legislator arbitrarily. It is a continuous development of the level of financial autonomy after the restoration of territorial self-government in our territory after 1990. Own revenues gradually began to form the dominant part of the total revenues, especially for municipalities. Already in the 1990s, authors summarised the tendencies of the territorial budget regime as compared to the previous state to the following points:

- strengthening the financial self-sufficiency of territorial budgets and reducing their dependence on subsidies from the state budget
- attenuating the claim-related requirements of municipalities
- achieving greater autonomy and responsibility of local governments in the budget regime

However, we can speak of these as partial changes that are the result of processes taking place within the public administration and, on the basis of these arguments, we can divide the fiscal decentralisation into:

- fiscal decentralisation carried out by tax sharing, when the legislator sets out shares in tax revenues to be allocated to specific segments of the budget system and their components
- fiscal decentralisation carried out by assigning taxes, when the entire tax revenue is transferred, i.e. assigned, to specific segments of the budget system and their components

From the above, we can conclude that fiscal decentralisation can take place through tax assignment or tax sharing, depending on the budget allocation, to which public fund the tax revenue flows to and in what amount. Budget allocation is one of the tax structural elements because it determines where the tax revenue flows and which budget reports it in its revenue.[15]

Depending on whether only a single public budget is a recipient of tax revenue or the revenue is split between more segments in the budget system, we distinguish between *shared* and *assigned taxes*.

Assigned taxes are the revenue of the relevant tax which flows exclusively into the budget of municipalities and regions. These taxes currently include:

- real estate tax (the entire revenue goes to the municipality budget)
- corporation tax (where the taxpayer is a municipality or region, with the exception of a withholding tax at a special rate)

Shared taxes are taxes the revenue of which is divided into several segments of the public budget system by percentage, i.e. precise shares are set either according to a mathematical formula that takes account of certain reallocation criteria or depending on the place of tax origin, i.e. where the tax is collected. This means that only the share of the national tax revenue goes to the municipal and regional budgets. These taxes currently include:

- value added tax
- personal income tax (advances on this tax)
- corporation tax (except if the taxpayer is a municipality or a region)[16]

3. Legal Framework and BAT Relevance

The fact that the income of territorial self-government unit budgets includes, among other things, tax revenues and their shares according to a special law is regulated at the most general level by Act No. 250/2000 Coll. on Budgetary Rules for Territorial Budgets, as amended. Consequently, the tax allocation of taxes is regulated by Act No. 243/2000 Coll. on Budget Allocation of Revenue of Certain Taxes to Territorial Self-Government Units and to Certain State Funds (the Act on Budget Allocation of Taxes), as amended. This act, comprising only eight articles, identifies two major issues:

- which tax revenues are transferred by the state to the territorial self-government units completely, or a share of tax revenues to territorial self-governments is determined
- establishing criteria and a method for calculating the share of each individual municipality and individual region

It is hard to imagine its practical application by simply reading the text of the act. In fact, formulations verbally express a mathematical conversion, the expression of which is rather complicated for obvious reasons. In order to understand the Act on Budget Allocation of Taxes, a detailed analysis of individual provisions is required, using many materials containing, among other things, data on the performance of individual territorial self-

government units in the time series. It should be noted that budget allocation is always a matter with disputes over the way taxes are reallocated within the budget system and that there is a very frequent debate on the fairness of the system set up. At the same time, we can state that tax allocation, including reallocation of taxes, can be described as a legal and economic and political issue the opinion on which is not uniform.[17]

The most important facts about budget allocation of taxes are as follows:

- Tax revenues constitute a major part of municipal budget revenues (roughly 55–60%).
- Tax revenues of municipalities are not assigned.
- Municipal authorities decide on the use of tax revenues.
- Tax revenues of municipalities are the basis of both economic and financial independence of municipalities from the state.

4. Possibilities for Changes to the Budget Allocation of Taxes Acceptable *De Lege Ferenda*

One of the objectives is to summarise the findings based on long-term monitoring of the issue and to reflect on some of the related aspects. Allocation of taxes is undoubtedly a matter of political nature. Specialists in the field generally enter the discussion only based on set model analyses. Even the specialists do not have a uniform opinion on the reallocation of shared taxes.[18]

The debate on the topic of budget allocation of taxes is definitely not over by adopting the latest amendment. It is assumed that this will be a solution for a year or two, followed by the incorporation of a budget allocation institute as a structural element into individual tax laws.

As far as the current system is concerned, it could be adjusted in the following way to better match the real needs of municipalities with the real costs of municipalities related to the delegated and autonomous authority of public administration:

- establishing a criterion of the built-up area of a municipality
- reducing the weight of the municipality's assessment criterion (or completely abolishing it) and the need to adjust the weight of other criteria (creating a balanced system of criterion weight that would correspond to the amount of costs associated with the given criteria)
- reducing the weight of population criterion at the expense of other criteria
- including the share of consumption and environmental tax revenue in BAT
- setting a single percentage for determining the share of municipal budgets in shared taxes to reflect the inclusion of other taxes[19]

From the point of view of the budget allocation of taxes for regions, the funding of education still seems to be the most current adjustment. At this point, there are two solutions that can be considered:

- the first option would be to increase the total share of regions in shared taxes, with the region continuing to reallocate that part of the funds that would represent the direct costs of education according to the stipulated schedule and, at the same time,

to increase the total share of municipalities in shared taxes to the extent of the current subsidy provided from the state budget in the aggregate subsidy relationship for the partial reimbursement of operating expenses
- the second option would involve increasing the total share of municipalities and regions in shared taxes for the new percentage to include the direct costs of education by the founder, as well as subsidies for partial reimbursement of operating expenses in the case of municipalities[20]

The first option appears to be a compromise where the advantages prevail. It would strengthen the economic impact of territorial self-governments on the educational organisations they establish. On the other hand, the concern about the municipal self-government having too much influence on rewarding teachers, especially in preschool and elementary schools, would be eliminated.[21]

5. Conclusion

Tax revenues are among the most important and largest sources of funds for municipalities and regions. Without tax revenues, municipalities and regions could hardly finance their operations and other public administration activities. Therefore, it is important to set up a BAT system to meet real needs, to be stable and not to favour a particular group of municipalities or regions over others.

In spite of the great criticism of the current BAT system introduced in 2008, we must recognise that this system has brought much needed stability into the funding of municipal systems and that it has removed unfair differences in revenues of cities and municipalities of relatively the same size. Financing of municipalities was linked to decisive tax revenues, which ensured their continuous growth. Yet the municipal budgets, especially of small municipalities, are not enough to cover all the costs associated with public administration. Therefore, it is necessary to keep developing the current system and to introduce criteria that would be able to reflect the real costs that municipalities have in the public administration.[22]

It is clear from the above text that the development of the budget allocation of taxes and their significance for municipal and regional budgets in the Czech Republic is positive, given that the budgeted revenues can be quite easily estimated for each municipality and region. This property of the current BAT is crucial because municipalities and regions have the possibility to estimate revenues and to adjust costs to avoid large indebtedness. The partial amendments to the Act on Budget Allocation of Taxes introducing various criteria for the reallocation of taxes strengthen municipalities and regions as they ensure their permanent financial basis, and it can be concluded from the above that the hypothesis stated in the introduction has been confirmed.

References

1 Milan Bakeš, Marie Karfíková, Petr Kotáb, Hana Marková et al. Finanční právo. 5. upravené vydání [Financial Law, 5th revised edition], 548 (Praha, C. H. Beck, 2009).
2 Ivana Pařízková, *Finance územní samosprávy* [Finances of Territorial Self-Government], 238 (Brno, Masarykova univerzita, 2008).
3 Martin Netolický, *Vztahy mezi články rozpočtové soustavy* [Relationships between Budget System Segments], 104 (Brno, Tribun EU, 2010).
4 Netolický, *supra n.* 3, at 102.
5 Ibid. 105.
6 Romana Provazníková, *Financování měst, obcí a regionů* [Financing of Cities, Municipalities and Regions], 86 (Praha, Grada Publishing, 2007).
7 Act No. 243/2000 Coll. on Budget Allocation of Revenue of Certain Taxes to Territorial Self-Government Units and to Certain State Funds (the Act on Budget Allocation of Taxes), as amended.
8 Petr Mrkývka et al. *Finanční právo a finanční správa,* 1. díl [Financial Law and Tax Administration, Part 1], 397 (Brno, Masarykova univerzita, 2004).
9 Romana Provazníková, *Financování měst, obcí a regionů.* 3. aktualizované a rozšířené vydání [Financing of Cities, Municipalities and Regions, 3rd updated and extended edition], 109 (Praha, Grada Publishing, 2015).
10 Netolický, *supra n.* 3, at 107.
11 Jitka Peková, Jaroslav Pilný, Marek Jetmar, *Veřejná správa a finance veřejného sektoru.* 2. přepracované vydání [Public Administration and Public Sector Finances, 2nd revised edition], 172–173 (Praha, ASPI, 2005).
12 Netolický, *supra n.* 3, at 107.
13 Provazníková, *supra n.* 6, at 40.
14 Martin Netolický, *Vztahy mezi články rozpočtové soustavy* [Relations between the Cells of the Budget System], 107 (Brno, Tribun EU, 2010); Michal Radvan, Ekonomická autonomie obcí v České republice [Economic Autonomy of Municipalities in the Czech Republic], 137–147, in *Interakce ekonomie, managementu a práva při rozvoji regionů* [Interactions of Economy, Management and Law in Development of Regions] (Brno, Vydavatelství MU, 2006).
15 Michal Radvan, *Finanční právo a finanční správa. Berní právo* [Financial Law and Tax Administration. Tax Law], 33–36 (Brno, Doplněk a Masarykova univerzita, 2008).
16 Mrkývka, *supra n.* 8, at 397.
17 Netolický, *supra n.* 3, 109.
18 Ibid. 178.
19 Cf. Ibid. 178.
20 Ibid. 180.
21 Ibid.
22 Provazníková, *supra n.* 9, at 131.

Public Governance, Administration and Finances Law Review Vol. 4. No. 2. (2019) • 86–94.

10.53116/pgaflr.2019.2.7

The Efficiency of Tax Collection in the Czech Republic

Eva Tomášková*

* Ing. Eva Tomášková PhD, Assistant Professor of National Economics and Public Finance, Department of Financial Law, Faculty of Law, Masaryk University, the Czech Republic. (e-mail: eva.tomaskova@law.muni.cz)

Abstract: This paper deals with the efficiency of tax collection in the Czech Republic. The first part of this paper describes theoretical approaches to efficiency of taxes. Considering the aim of the article, there are no mathematical models of efficiency presented. The second part introduces efficiency from the point of view of law. The next part involves the application of efficiency of tax collection, especially how to measure efficiency and the main barriers for its establishment in the Czech Republic. The last part of the paper offers the summing up of gained knowledge. The aim of this paper is to detect if the current approach to tax collection contributes to higher efficiency.

Keywords: qualitative efficiency; quantitative efficiency; tax collection; tax evasions; tax rate

1. Introduction

Total tax income and the increasing of total tax income is one of the most important issues in tax law. Politicians, lawyers and economists try to find the best way for solving this issue. This process can be characterised as a never ending story, it is still underway. All interested persons offer new solutions and then they come back to the older ways; they get inspired from the situation in other countries and they establish new taxes, then, after a time, they repeal these new taxes. These ways are changing according to the political orientation of the presenter or changing economic conditions. For this reason, the tax system is still changing and it is possible to see different tax systems in every country. Therefore, it is possible to characterise tax systems as constantly changing.

There are some requirements for tax systems. These requirements can be divided into some groups. First are general rules, which are democracy, legality, legitimacy and priority of EU law and international law. Second are rules connected with the fiscal part of financial law. There are many specific rules concerning purpose, schedules, effectiveness, efficiency, etc.[1] Effectiveness and efficiency of taxes are still popular topics. There are many views on the implementation of effectiveness and efficiency, however, it is very difficult to apply these approaches in practice. Economists deal with the question how to use resources in the most efficient way to satisfy the needs of consumers. Lawyers are trying to find the most efficient way of tax processes. Politicians are comparing the efficiency of individual public goods.

This paper describes the efficiency of tax collection in the Czech Republic. The aim of this paper is to detect whether the current approach to tax collection contributes to higher efficiency. The following hypothesis is stated: *"The current approach to tax collection applied in the Czech Republic contributes to higher efficiency."* Compilation, comparison, analysis and synthesis are the methods used in this contribution.

2. The History of Attitude towards Efficiency of Taxes

The term "efficiency" is based on the notion of Pareto optimality. It is a situation when there is no possibility to improve the welfare of an individual without making the welfare of at least another individual worse. The question is how to obtain optimal allocation and efficiency.[2]

However, the first written remark about efficiency of taxes is older and it is connected to Adam Smith. Smith wrote down the economic principles for taxation in his book.[3] In his book, he named four maxims on taxation:

- Taxes have to be as equal as possible – every subject ought to contribute to the public budgets in the closest proportion to his or her abilities; that means in proportion to the revenue which he or she respectively earns under the protection of the state.
- Taxes have to be most certain – the amount of tax which each individual is to pay, has to be certain, clear and understandable to the contributor and for all other persons.
- Taxes have to be levied in the most convenient way and in the most convenient time for the contributor.
- Taxes have to be, as much as possible, the least burdensome to the citizens. According to Leijon: *"Every tax ought to be constructed in a way that it both takes out and to keep out as little as possible of the pocket of the people, apart from what it brings into the public treasury of the state."*[4]

Several later authors agree with the approach of Smith and add more characteristics to this approach. One of the other views on efficiency relates to transaction costs. The efficiency is influenced by transaction costs. According to Coase, economic efficiency is shown in externalities, which are connected to economic allocation or outcome. Externalities create transaction costs (these costs are connected to any economic trade when participating in the market).[5] Coase's theorem is based on Pareto optimality. According to Coase, a completely competitive market is without transaction costs and for this reason, it is the most efficient and brings a mutually beneficial outcome.

Musgrave and Musgrave define efficiency at production, efficiency at consumers and interaction between production and consumption. Production efficiency can be described by an example of two consumers and two products: if one production permits 10 units of X and 7 units of Y and another production permits 10 units of X and 5 units of Y the first method of production is preferred. Efficiency of a business is based on preferences of

consumers and shows us the basic principles of good exchange. The marginal rate between the two goods (X and Y) must be the same for consumer A and B. "The lowest rate at which A and B are willing to trade the last unit of X for an additional unit of Y should be the same for both actors."[6] If A is willing to trade 1 unit of X for 4 units of Y and B is willing to give 5 units of Y in order to get 1 unit of X, "they will exchange and a negotiation will occur as both parties gain by exchanging".[7] The third condition is realised at the most efficient tax system. "The marginal rate for substitution of X for Y in consumption should be the same as the marginal rate of transformation in production that is how many extra units of X can be produced if one unit of Y is produced. If the marginal rate for consumption is 3 X for 2 Y but the marginal rate for production is 3 X for 2 Y it will be desirable to increase the output X and reduce Y until the ratio is equalised."[8]

Niskanen deals with efficiency in the public sector and stresses that a better competitive enviroment and an increasing controlling and sanctioning system improve total efficiency. The last two instruments can be applied in the tax system as well.[9]

According to Taghavinezhadian, tax efficiency is most often marked as the tax effort. The success of tax efficiency includes three points. The first is the ratio of the collected taxes and allocated taxes. If the ratio equals one, the current tax system is efficient; the tax system is able to collect the taxes in the estimated level mentioned in the national budget. If the ratio is less than one or more than one, the tax system is not efficient because it gains higher income of taxes than it needs and the welfare of consumers is lower (consumers could not use the money for their own purposes) or the budget estimation has been based on unrealistic facts. The second index includes percentage changes at the collected tax in the current year and percentage changes at the collected tax in the previous year. If this index is lower than one, efficiency of the tax system decreased. If the index is one, the tax system is on the same level with the situation in the previous year. If the index is more than one, efficiency of the tax system has been increased in comparison with the situation in the previous year. Third is the relative tax rate and tax effort.[10]

The current changing environment brings other requirements for taxes, e.g. Salanié adds two further characteristics of taxes. The first is that taxes have to change with the economic environment; they have to be automatic stabilisers. The second one sets that taxes should be clear.[11]

Efficiency should be applied at allocation and distribution. Public finance tries to gain financial means to public budgets with the lowest costs and spend these financial means effectively on solving the public sector tasks.

According to Schäfer and Ott, efficiency does not involve the consideration of moral rights; it might be unjust and it does not fulfil the principles of justice and fairness. Efficiency is influenced by administrative and bureaucratic processes, the political decision-making process and bargaining situations. Raskolnikov notices that inefficiency can only lead to distortive taxes.[12]

The analysis of the above-mentioned knowledge shows that the most important characteristic for efficiency is consumer welfare. Consumer welfare is based on low tax rates and low costs related to redistribution of tax income. Some economic models were established for measuring tax efficiency. Considering the aim of the article, these models are not presented in this paper.

3. Efficiency of Public Administration

Efficiency is defined in § 2 of Act no. 320/2001 Coll. on Financial Control in Public Administration and on the Amendment to some Acts (Act on Financial Control). According to this, "effective management shall mean such a use of public means for ensuring the given tasks with as little as possible provision of those means while maintaining the corresponding quality of the tasks fulfilled".

According to Mrkývka, Pařízková, Radvan et al., efficiency is evaluated through internal control system. This control system shall be independent. Internal control system involves procedures fundamental for the timely providing of information to all relevant levels of management and the elimination of shortcomings, and shall create conditions for all exercise of public administration (see § 25 of the Act on Financial Control). Control systems are necessary for the realisation of internal audit. According to § 28 of Act. No. 320/2004 Coll. on Act on Financial Control, internal audit is characterised as the evaluation of operations and internal control system of the public administration unit. It involves:

"a) the legal regulations, the measures adopted and the procedures defined are adhered to the activities of the public administration body
b) the risks relating to the activity of a public administration body are recognized on time and corresponding measures for their elimination or mitigation are adopted
c) the managing controls provided to the Chief Executive of a public administration body are reliable and timely organizational, together with the financial and other information
d) operational and financial criteria
e) the introduced internal control system is sufficiently efficient, reacts to the changes in economic, legal, operational and other conditions
f) the results achieved during the fulfilment of decisive tasks of the public administration body sufficiently ensure that the approved intentions and targets of the body shall be met" (§ 28)

Internal audit involves financial audits, audit of systems and audit of execution. The aim of a financial audit is the analysis of data from accounting, financial data or data from other statements. The aim of an audit of systems is to evaluate the systems of income provision of the public administration body. Execution audits are based on the examination of effectiveness and usefulness of operations, reasonability and efficiency of the internal control system, etc.

The term "efficiency" is often mentioned in this act. Efficiency is mentioned in 21 cases and inefficiency is mentioned in 3 cases. Efficiency is often connected to management or financial control.

4. Qualitative Efficiency

Efficiency can be divided into two groups – qualitative and quantitative. The qualitative one is based on time analysis. Thus, the number of operations that are performed at

a specified time is analysed.[13] This time limit is often used for larger investment projects. Qualitative efficiency determines how the subject handles time. If we apply this qualitative efficiency to taxes, then it is necessary to first define the time required for all processes. Efficiency gains are related to internal tax collection processes. While it is possible to specify activities according to the necessary time, it is difficult to unify them for all activities as taxpayers and economic conditions differ. Increasing of qualitative efficiency is based on the internal processes of tax collection. It is possible to specify time for some activities; however, it is difficult to uniform time for all activities, since the taxpayers and conditions differ. Qualitative efficiency is suitable as one part of internal audit of tax offices. However, information about the number of operations realised in defined time is not published. For this reason, it is very difficult to realise an analysis of qualitative efficiency.

One possibility is to set the number of financial controls per year for every tax office and analyse if the tax offices realise the assigned numbers of financial controls. However, it is difficult to define time for all activities and internal processes. Nevertheless, it is possible to compare tax offices using their performance of finance control. The time necessary for finance control is based on many variables, e.g. the size of the taxable person, complexity of productions, the number of tax office workers etc. The public often evaluates the efficiency of tax offices according to the number or periodicity of financial controls. The last decade shows that the financial controls differ in different territories of the Czech Republic. Different tax offices performed the financial controls in intervals from 11 to 206 years between the years 2005–2013. Table 1 shows the periodicity of financial controls in the selected territories of the Czech Republic.

Table 1.
Periodicity of financial controls in the selected territories of the Czech Republic

Tax office	Periodicity of financial control in 2014 (in year)	Tax office	Average periodicity of financial control in 2005–2013 (in year)
Náchod	298	Praha 2	206
Praha 2	284	Praha 6	161
Praha 6	277	Praha 4	150
Praha 4	272	Praha 3	146
Praha 1	269	Praha 1	132
Praha 5	225	Praha-Modřany	128
Praha 9	182	Praha 10	124
Chrudim	175	Praha 5	121
Praha-Modřany	171	Praha 9	110
Louny	165	Praha 7	107

Source: Daňové ráje a pekla v Česku. Nový žebříček finančních úřadů [Tax Paradise and Hell in the Czech Republic. New Ranking of Tax Administrators][14]

The situation was caused by a differing number of companies in different localities. Many companies chose one of the tax offices in some districts of the capital city for the low level

of likelihood of financial control. The General Financial Directorate has not published the average periodicity of financial control for the last years. Since January 1, 2015, all tax offices can perform financial control in all territories in the Czech Republic. It is possible to suppose that companies, which want to avoid paying taxes, will leave the market or start to pay the taxes. For this reason, it is possible to state that qualitative efficiency (improving internal processes of tax collection) is increasing. Likewise, the second factor for measuring qualitative efficiency can be the time necessary for preparation, filing and paying the taxes. According to Doing Business (Doing Business evaluates business regulations and their enforcement in 190 countries and in selected cities), time to prepare, file and pay the corporate income tax, value added or sales tax, and labour tax (including social contributions) is one of the key elements for analysing business regulation environments. It is obvious that the time spent to this preparation, filing and paying of taxes could be utilised in business more effectively. Estonia is leader in this factor. Businesspersons in Estonia need for these activities only 50 hours per year. Businesspersons in the Czech Republic need 5 times more time for filing their tax obligations (248 hours per year in 2018). Businesspersons in Poland need more time than businesspersons in the Czech Republic (260 hours per year). The situation in the countries neighbouring the Czech Republic is better. Businesspersons spend 218 hours per year performing all their tax obligations in Germany, 131 hours per year in Austria and 192 hour per year in the Slovak Republic. These data were valid in 2018.[15]

In sum, it is difficult to establish qualitative efficiency because we need to know the time needed for any related activity and internal process. There are some activities where it is possible to establish a time bound, but there are many other activities where it is impossible and generalisation is absurd.

5. Quantitative Efficiency

Quantitative efficiency is based on comparing real inputs and the maximum of outputs, e.g. if it is possible to gain one hundred of outputs and we gained only seventy, efficiency is 70%.

It is difficult to know the maximum outputs (tax revenue). The Laffer curve shows one of its reasons; it shows the dependency of the total tax revenue on tax rate. Table 2 shows the total tax revenue including social contributions in % GDP during the last years.

Table 2.
Total tax rate and contribution rate as % of GDP in the Czech Republic

Year	2003	2004	2005	2006	2007	2008	2009
Total tax rate	34	35	34	34	35	33	32
Year	2010	2011	2012	2013	2014	2015	2016
Total tax rate	33	34	34	35	34	34	35

Source: Total tax revenue by country, 1995–2016 (% of GDP)[16]

Receipts from taxes and social contributions in % GDP create more than one third of the total economic production in the Czech Republic. Poland has very similar total tax share (it is about 33–34% in the last years), the Slovak Republic shows about 31–32% of total share and both German-speaking countries has a higher total share (Germany about 40% and Austria about 43% of total share). However, it is difficult to find optimal tax shares because the environment is still changing and the optimal position is changing as well.

The development of the total tax rate shows that the highest tax share in the Czech Republic was in the1990s. The level of the total share rate was 47% in 1993. The total tax share has not significantly changed in the last fifteen years. Tax incomes are increasing although we reduce the total tax income by inflation and GDP growth.

Correia, Economides et al. notice that the increasing of tax income can be realised by increasing the progressivity of the tax system.[17] It is impossible to gain more tax revenue by increasing the tax rate because people rather choose tax avoidance or tax evasion and a very high tax rate does not motivate people to activities, which are subject to tax. Ramsey offers one solution. He suggested an optimal tax rate – to have higher tax rates while taxing less elastic goods and to have lower tax rates while taxing goods that are more elastic. This rule is difficult to apply in practice; however, the total tax income would increase.

Likewise, maximum outputs at the current level of tax rate can be measured as real incomes of taxes plus incomes of tax evasion. It is impossible to add tax avoidance because it is not conveniently measurable. At first, it is necessary to detect tax evasion. Probably, there are some tax evasions that cannot be detected.

The government stresses that it wants to eliminate tax evasions and increase total tax incomes. The government has three possibilities for the elimination of tax evasions. First, to decrease the tax rate (low tax rate does not motivate people for tax evasions; the level of profit from tax evasion is not so high). Second, to impose more sanctions for tax evasions (high sanctions can be a reason why people change their minds and do not commit tax evasions). Third, to increase the periodicity of financial control. That is the most preferable method of the Government of the Czech Republic.

Tax evasions are still very high. Tax evasions[18] can reach thousands of millions CZK per year. For this reason, from 2016, the government established a system of electronic records of sales. This system of electronic records is aimed at cash sales of goods and services and has to provide prompt communication between the company and the Financial Administration of the Czech Republic. It was supposed that electronic records of sales would increase the total tax income with about 18 billions of CZK in 2018. However, the total expenditures connected with the implementation of electronic records of sales are not published.

Table 3.
Total tax income in the last years

Year	2010	2011	2012	2013
Total tax income in bill. CZK	548,432.3	561,388.1	583,746.5	610,756.9
Year	2014	2015	2016	2017
Total tax income in bill. CZK	639,199.5	670,395.8	732,197.2	786,636.4

Source: Finanční správa [Tax Administration][19]

Table 3 shows that the total tax income in the last years is increasing. However, it is obvious that the main reason is economic development and not electronic records of sales (total tax income was 606,896 bill. CZK in 2008 – before the economic crisis). Eurostat has the same attitude – total tax incomes of value added tax is based on economic development and the impact of electronic records of sales is very small. Moreover, some experts notice that electronic records of sales have a negative impact on the business of micro companies (because electronic records of sales bring extra costs) and do not impede tax evasions.

To summarise, the application of quantitative efficiency is difficult, as well because we need to know the maximum output for the calculation. There are some possibilities how to estimate the maximum output. Unfortunately, these numbers are only estimates with a certain probability. That is the main obstacle for the calculation of quantitative efficiency.

6. Conclusion

This paper deals with the efficiency of tax collection. The theoretical part includes the main notions from the perspective of economy and law. It is obvious that many politicians, economists and lawyers try to solve this issue. They made some recommendations for a better tax system and tax collection. However, there is no comprehensive solution that can be used in all tax systems. This is due to specific tax systems in each country, specific history, specific attitude of taxpayers to paying taxes, specific economic conditions, etc.

The efficiency of public administration is defined in Act no. 320/2001 Coll. on Financial Control. According to the Act on Financial Control, efficiency is mentioned in relation to management and financial control. This sense of efficiency is close to economic attitudes.

Economic theory divides efficiency into qualitative and quantitative efficiency. Both these methods are very difficult to apply in practice. Qualitative efficiency needs to establish the time needed for any activity and quantitative efficiency needs to establish the maximum outputs. For this reason, efficiency is only estimated through alternative factors such as: 1. the number of financial controls per year; 2. periodicity of financial controls; 3. the time necessary for measuring qualitative efficiency (that means the time necessary for preparation, filing and paying the taxes); 4. total tax rate; 5. tax evasions; and 6. total tax incomes.

It is possible to state that the current approach to tax collection applied in the Czech Republic does not contribute to higher efficiency. The hypothesis is disproved. It is obvious that the efficiency of tax collection has to improve; it would be especially useful to reduce the time necessary for preparation, filing and paying taxes. The question is when it happens because politicians still prefer only short-term objectives and short-term outcomes and the current political situation does not indicate any positive change. Therefore, the improvement of the efficiency of tax collection in the Czech Republic will be slow.

References

1 Petr Mrkývka, Ivana Pařízková, Michal Radvan et al. *Finanční právo a finanční správa,* 2. díl [Financial Law and Tax Administration, Part 2] (Brno, Masarykova univerzita, 2004).
2 Hans-Bernd Schäfer, Claus Ott, *The Economic Analysis of Civil Law* (Cheltenham, Edward Elgar, 2004).
3 Adam Smith, *An Inquiry into the Nature and Causes of the Wealth of Nations*, 676–677 (The Pennsylvania State University: The Electronic Classics Series, 2005).
4 Lena Hiort af Ornäs Leijon, Tax policy, economic efficiency and the principle of neutrality from a legal and economic perspective, 12, in Uppsala Faculty Of Law, *Working Paper,* vol. 2 (2015), www.jur.uu.se/digitalAssets/585/c_585476-l_3-k_wps2015-2.pdf (accessed 21 August 2019).
5 Ronald H. Coase, The problem of Social Cost, in *The Journal of Law and Economics,* vol. 3 (1960). DOI: https://doi.org/10.1086/466560
6 Richard A. Musgrave, Peggy B. Musgrave, *Public Finance in Theory and Practice,* 61 (New York, McGraw-Hill Book Company, 1989).
7 Ibid.
8 Ibid.
9 William A. Niskanen, *Bureaucracy and Representative Government* (Chicago, New York, Aldine-Atherton, 1971). DOI: https://doi.org/10.4324/9781315081878
10 S. H. Taghavinezhadian, *Investigation of Effects of the Organizational Structure on the Efficiency of the Direct Taxes Organization,* M.A. Thesis, Tehran University, 1990.
11 Bernard Salanié, *The Economics of Taxation* (London, The MIT Press, 2002).
12 Alex Raskolnikov, Accepting the Limits of Tax Law and Economics, in *Cornell Law Review,* (March 2013). DOI: https://doi.org/10.2139/ssrn.1990430
13 Ulrike Mandl, Adriaan Dierx, Fabienne Ilzkovitz, The effectiveness and efficiency of public spending, in *European Economy, Economic Papers of the European Commission,* no. 301 (2008). https://doi.org/10.2765/22776
14 *Daňové ráje a pekla v Česku. Nový žebříček finančních úřadů* [Tax Paradise and Hell in the Czech Republic. New Ranking of Tax Administrators], 2018, https://zpravy.aktualne.cz (accessed 21 August 2019).
15 Doing Business, 2018, www.doingbusiness.org (accessed 21 August 2019).
16 *Total tax revenue by country, 1995–2016 (% of GDP),* Eurostat, 2018, http://ec.europa.eu/eurostat/statistics-explained/index.php?title=File:Total_tax_revenue_by_country,_1995-2016_(%25_of_GDP).png; *Finanční správa* [Tax Administration], 2018, www.financnisprava.cz/cs/dane/analyzy-a-statistiky/udaje-z-vyberu-dani (accessed 21 August 2019).
17 Isabel Correia, Consumption Taxes and Redistribution, in *American Economic Review,* vol. 100, no. 4 (2010). DOI: https://doi.org/10.1257/aer.100.4.1673; George Economides, Saqib Jafarey, Natasha Miaouli, Apostolis Philippopoulos, Consumption taxes and the efficiency-equity tradeoff, in *Working Paper Series,* vol. 24 (2013), Athens University of Economics and Business, https://ideas.repec.org/p/aeb/wpaper/2013024y2013.html (accessed 21 August 2019).
18 According to Police Reports, tax evasion with fuel reached 1.4 billion CZK. The company sold 276 billion litres of fuel between June 2010 and May 2011. *Ukončení vyšetřování miliardového krácení daní* [Termination of Investigations of Billion Tax Evasion], Police Reports, 2018, www.policie.cz/clanek/ukonceni-vysetrovani-miliardoveho-kraceni-dani.aspx (accessed 21 August 2019).
19 Finanční správa, *supra n.* 17.

Public Governance, Administration and Finances Law Review Vol. 4. No. 2. (2019) • 95–100.

10.53116/pgaflr.2019.2.8

Case study

New Legal Regulation of the Administrative Justice in the Slovak Republic[1]

Juraj Vačok*

* Associate Professor, JUDr. Juraj Vačok, PhD, Comenius University in Bratislava, Faculty of Law, Department of Administrative Law. (e-mail: vacok1@uniba.sk)

Abstract: Administrative justice is a very strong element of control of public administration. Its decisions not only control but also guide the future directions in an application of particular legal norms. The author evaluates the new changes of administrative justice in the Slovak Republic. He points out the main changes in comparison with the previous legal regulation and tries to evaluate them. He points out that it is too early to evaluate the whole new legal regulation. Despite this fact, he states that it is possible to make a partial evaluation on the basis of a result and experiences acquired to this time.

Keywords: administrative justice; civil judicial proceedings; branch of law; general courts; new legal regulation

1. The Current Legal Regulation

Administrative justice in the Slovak Republic is now connected to many changes. One of the most important is adopting the new legal act. It is Law No. 162/2015 Coll. on Administrative Judicial Order, as amended[2] (hereinafter: Administrative Judicial Order). It entered into force on 1 July 2016.

This law can be specified as a general law for administrative justice and administrative judicial proceedings. It means that special laws can regulate particular matters in a different way.[3] The relation between special laws and the Administrative Judicial Order is based on the principle of subsidiarity.[4]

Nevertheless, it can be stated that most of the legal regulation is included in the Administrative Judicial Order. However, it is difficult to predict its future development. The current situation is influenced by the fact that the Administrative Judicial Order is valid only for a relatively short period. Due to this fact, there was not enough time for the legislation to change special laws and create its own system of judicial review in particular areas of law.

Despite this fact, I suppose that special laws will not depart significantly from the general legal regulation in the Administrative Judicial Order. I think that special laws will

complete the gaps in the legal regulation in most situations or regulate specifics in particular proceedings which are typical for these kinds of proceedings.

2. Legal Regulation before the Administrative Judicial Order

Administrative Judicial Order replaced Law No. 99/1963 Coll. on Civil Judicial Order, as amended (hereinafter: Civil Judicial Order). This law regulated the procedure in matters of administrative justice in its fifth part with subsidiary use of the first part and second part of the Civil Procedural Order.

This was a very big change in the area of administrative justice. Civil Judicial Order was established to regulate the procedures within the civil procedures.[5] I think that it was not appropriate to regulate the area of administrative justice in the same Law.[6]

Of course, there could be more opinions for this. Among the colleagues of my university, there were also many discussions about the position of administrative justice in the system of law. These disputes were mainly between scholars with specialisation in civil judicial proceedings and scholars with specialisation in administrative proceedings.[7]

Despite the different opinions about this question, administrative justice was considered a part of civil proceedings. It was because of Section 1 § (1) of the Civil Judicial Order which defined the subject-matter of this act. This provision connected the whole legal regulation with civil judicial procedure. It means that if proceedings in administrative justice were regulated in the Civil Judicial Order, this law had to be considered a part of civil judicial proceedings.

3. The New Position of the Administrative Justice after Adopting the Administrative Judicial Order

The adoption of the Administrative Judicial Order strengthened the position of the Administrative Justice. This new legal regulation demonstrates that proceedings in administrative justice cannot be regarded as a part of civil judicial proceedings. Proceedings before administrative courts have their own separate legal regulation which reacts to their own needs and specifics.

Opposite to this fact, it can be mentioned that Section 25 of the Administrative Judicial Order refers to a subsidiary use of Law No. 160/2015 Coll. on Civil Dispute Order, as amended (hereinafter: Civil Dispute Order). This law regulates proceedings before courts in the private law dispute matters.[8]

Truly, I am not satisfied with Section 25 of the Administrative Judicial Order. In my opinion, the proceedings before administrative courts should be separated from the proceedings in civil matters.

I have more reasons for this opinion, which are connected mainly with the aim of administrative justice. This is not to solve disputes between two parties which are in horizontal relations to each other. The aim of administrative justice is the control of public

administration. Because of that, administrative justice controls the legality of acts and activities of public administration.

Even if we take into account the Slovak legal history and tradition, administrative judicial proceedings are closely connected to the civil judicial proceedings. Nevertheless, this fact does not mean that administrative judicial proceedings and civil judicial proceedings are identical. These proceedings can be similar and they have some common features, too. But this does not mean that it is correct to build only one kind of judicial proceedings. Moreover, if this legal regulation is influenced mainly by amendments which are connected with the requests to the better civil judicial proceedings.[9]

Because of these facts I consider one of the most important advantages that the amendments of the Administrative Judicial Proceedings will react only to the needs of administrative justice. They will not be independent and they will be affected by a need to change and influence other areas of law.

The separate legal regulation is also very important for the position of administrative justice. I am convinced that the separate law strengthens the position of every particular area of law. The separate legal regulation stresses the specifics and independence of this area. Division of the previous legal regulation into separate laws should demonstrate that there are independent proceedings with their own aims and ways to reach them.

4. The Main Changes of the New Legal Regulation of Administrative Justice

The new legal regulation follows up the previous legal regulation which was in the Civil Judicial Order. It can be stated that the concept of reviewing is the same as some new kinds of actions. Despite these facts I assume that the main part of the cases will still be connected with the reviewing of the legality of decisions, measures, inactivity and interferences of public administration.[10]

If we take into account conceptual changes, I draw attention to one of them, which is connected with the transformation of appeals to extraordinary remedies.

The transformation of appeals to extraordinary remedies means that an appeal was replaced by a cassation complaint which can be filed against the final decision of administrative courts. Pursuant to the Civil Judicial Order, judicial proceedings were built on the principle of proceedings in two instances. The first instance judicial decision could be reviewed by a higher instance administrative court which was usually the Supreme Court of the Slovak Republic.

The new legal regulation changed this principle. According to that, administrative courts decide in one instance. The final decisions of administrative judicial courts can be reviewed by the Supreme Court of the Slovak Republic which has the status of a cassation court. This court decides on the basis of the filed cassation complaints, as an extraordinary remedy.

It means that decisions of the administrative courts issued in one instance proceedings produce legal effects.[11] This is different from the previous legal regulation which connects filing of the appeal with the suspensory effect.

Moreover, reviewing of decisions of the administrative courts by the Supreme Court of the Slovak Republic is built on the cassation principle. It is connected with the fact that a court of cassation cannot repair legal defects. It can only cancel acts which were issued in previous proceedings and return cases back with its legal opinion.

This situation has an impact on legal certainty. It is connected mainly with the factor of time. If we take into account the length of the proceedings before a cassation court,[12] it is possible to presume that decisions of the cassation court are issued at the time when decisions of administrative courts may be enforced. If decisions of administrative courts are enforced before issuing of decisions of cassation courts, decisions of the cassation courts may constitute only a formal outcome.

In this context, it is important to notice that a cassation complaint is not the final remedy within the system of reviewing of administrative decisions. Decisions of the Supreme Court of the Slovak Republic can be reviewed by the Constitutional Court of the Slovak Republic. According to Article 127 § (1) of Law no. 460/1992 Coll. on the Constitution of the Slovak Republic, as amended (hereinafter: Constitution of the Slovak Republic) there is a possibility to bring the constitutional complaint to the Constitutional Court of the Slovak Republic if the particular private persons invoke the violation of the own fundamental rights and freedoms.[13]

The new legal regulation changed the situation within the system of legal remedies in the area of reviewing of final administrative decisions. That means that internal legal regulation offers three legal remedies which are built on the cassation principle and can intervene in the final legal situation.

Of course, there are also possibilities to protect particular rights and duties at the international level. Of particular importance in this context is the protection according to Article 34 of the Convention for the protection of Human Rights and Fundamental Freedoms before the European Court of Human Rights. Through this remedy, it is also possible to open the final legal situation.

5. Conclusion

It is hard to evaluate the current legal regulation of administrative justice. The main reason is that this regulation is very young and every society needs time to adapt to the changes. After a certain time of application of the new law, we can identify the main advantages and disadvantages and make a systematic evaluation. Now we have only partial results which we reach from the direct assessment of the impact of the current legal regulation on the legal application practice.

Despite these facts we can conclude that the new legal regulation strengthens the position of the administrative justice because of the own separate legal regulation in the particular fields of law. It is also possible to state that the new legal regulation is more complex and more detailed.

It will be interesting to monitor the changes within the system of remedies. The system amendment of replacing an appeal by a cassation complaint can help the participants to solve the matter in the administrative judicial proceedings in a shorter time by the final

judicial decision of administrative courts, but on the other hand, there are more possibilities to interfere in the existing legal situation which was guaranteed as final. That is a further possible intervention in the principle of legal certainty which can have an impact on the costs and time in which the case will be finally solved.

References

1 This contribution is a part of the research project "Legal Consequences of Final Individual Administrative Acts" supported by the Scientific Grant Agency of the Ministry of Education, Science, Research and Sport of the Slovak Republic and the Slovak Academy of Sciences. The registration number of this project is 1/0686/18.
2 This Law was amended two times until the present day.
3 For instance Section § 228d § (8) of Law no. 233/1995 Coll. on enforcement agents and enforcement activities (Enforcement Order) and amending of other acts as amended establishes a different jurisdiction of administrative courts in matters of disciplinary delicts of enforcement agents.
4 For the principle of subsidiarity see Soňa Košičiarová, *Správne právo procesné. Všeobecná časť,* 115 (Šamorín, Heuréka, 2015).
5 It was established in Section 1 of the Civil Procedural Order. For the term civil procedure see Svetlana Ficová, Marek Števček et al., *Občianske súdne konanie.* 2. Vydanie, 19–30 (Praha, C. H. Beck, 2013).
6 This confirms also the General Part of the Explanatory Memorandum of the Administrative Judicial Order. See www.nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=408731 (accessed 1 February 2019).
7 This is a personal experience of the author.
8 See Section 1 and Section 3 of the Civil Dispute Order.
9 This can be demonstrated by the number of amendments to the Civil Judicial Order. This law was amended more than eighty times. Only around thirty from these amendments were adopted with the purpose to regulate also the administrative justice. These information were taken from the system ASPI and www.slov-lex.sk/pravne-predpisy/SK/ZZ/1963/99/20160614#predpis.cast-piata (accessed 26 February 2019).
10 These terms are defined in Section 3 of the Administrative Judicial Order.
11 See Ida Hanzelová, Ivan Rumana, Ina Šingliarová, *Správny súdny poriadok. Komentár,* 71 (Bratislava, Wolters Kluwer, 2016).
12 We can take into account the length of the proceedings before a cassation court for the period up to one year. Of course the length of the proceedings can be longer. See Zuzana Hamuľáková, Preskúmavacia činnosť správneho kolégia Najvyššieho súdu Slovenskej republiky z hľadiska dĺžky konania, 60–65, in *Právoplatnosť správnych rozhodnutí – právna istota vs. legalita* (Bratislava, Univerzita Komenského v Bratislave, Právnická fakulta, 2018).
13 Article 127 § (1) of the Constitution of the Slovak Republic stated: *"The Constitutional Court decides on complaints by natural persons or legal persons objecting to violation of their basic rights and freedoms, or the basic rights and freedoms ensuing from an international treaty ratified by the Slovak Republic and promulgated in a manner laid down by law, unless other court makes decision on the protection of such rights and freedoms."* The English version is published on www.ucps.sk/Ustava_SR_anglicky (accessed 7 March 2019).