Regina Hučková, PhD, Associate Professor
Faculty of Law, Pavol Jozef Šafárik University in Košice
Košice, Slovakia
regina.huckova@upjs.sk

Pavol Sokol, PhD Student
Faculty of Nature Sciences, Pavol Jozef Šafárik University in Košice
Košice, Slovakia
pavol.sokol@upjs.sk

Laura Rózenfeldová, PhD Student
Faculty of Law, Pavol Jozef Šafárik University in Košice
Košice, Slovakia
laura.rozenfeldova@student.upjs.sk

4TH INDUSTRIAL REVOLUTION AND CHALLENGES FOR EUROPEAN LAW (WITH SPECIAL ATTENTION TO THE CONCEPT OF DIGITAL SINGLE MARKET)[1]

ABSTRACT

Digital Technologies alter our everyday life and the world around us. Individuals and businessmen are confronted with significantly differentiated conditions in every area of social-economic relations in contrast with the state that existed a few years ago. These altered conditions are in the case of the European Union's Member States multiplied by this status and by the related facts, especially by the necessity to conform the domestic politics to the EU's politics in many areas.

Frontal offensive towards the creation of the digital single market was announced by the European Commission in May 2015 by releasing its 16 initiatives within three basic pillars. The year 2017 was characterized by various legislative activities motivated by the creation of optimal legislative conditions in the EU. Slovak Presidency of the Council of the EU was also significantly defined by the Digital Single Market Agenda, since the presidency's program explicitly states the new key aim of the EU to ensure the free flow of data as the 5th freedom within the EU's internal market.

[1] This paper was written within the project APVV-14-0598 Electronisation of business with emphasis on the legal and technical aspects

The Article analyses the most significant legislative changes introduced in 2017 which impact will be observable in the beginning of 2018 and in the following years.

Keywords: *Digital market, EU , Digital Single Market Agenda, EU internal market*

1. INTRODUCTION

Professor Klaus Schwab, founder and executive chairman of the World Economic Forum, has been at the center of global affairs for over four decades. He is convinced that we are at the beginning of a revolution that is fundamentally changing the way we live, work and relate to one another.[2]

Previous industrial revolutions deliberated humankind from animal power, made mass production possible and brought digital capabilities to billions of people. This Fourth Industrial Revolution is fundamentally different. It is characterized by a range of new technologies that are fusing the physical, digital and biological worlds, impacting all disciplines, economies and industries, and even challenging ideas about what it means to be human.[3]

New dimensions in business and acceleration of business activities are accompanied by the development of new technologies, especially, by the development of computer technologies.[4] The importance of computer technologies in the business sphere at present go along with the enormous virtual potential for conducting business, it means, the internet network.

As regards the technological development, the branch of commercial law is in the forefront among other branches of law which can be viewed from different perspectives. On one hand, these modern age inventions are considered as objects of conducting business activities; on the other hand, these conquests of science and technology are deemed to be instruments to facilitate processes in conducting business activities. Further considerations must be of accentuated European dimension, since the European Union declared the strategy of single digital market in the previous months that should be created until 2020 and serve as the virtual platform to the existing physical single market. The general intent drifts forward to prepare the European economy for the new period in commercial and economic relations that is determined by the development in the sphere of information technologies.

---

2 For details: [https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab] Accessed 21 January 2018

3 *Ibid*.

4 Suchoža, J., Husár J., *et al.*, *Obchodné právo,* Bratislava, Iura Edition, 2009, p. 11

This paper discusses some of the legislative changes in the European Union legal framework presented, discussed and implemented during the last months. Three different issues are discussed and incorporated into the separated parts of the paper: eIDAS Regulation, law of Cookies and issue of the Cybersecurity which all seem to be very different. But if we look closer and more into details all of the discussed topics are fundamental elements of the agenda of Digital Single Market.

2. EIDAS REGULATION AS CRUCIAL ELEMENT OF THE DIGITAL SINGLE MARKET CONCEPT

Only several forms of verification of declared virtual identity with the real identity were known in the recent period. These were exemplified by electronic signature or guaranteed electronic signature. Having adopted the Regulation of the European Parliament and Council (EU) no. 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC ("Regulation eIDAS"), the options of electronic identification of both natural persons and legal persons have been broadened and, we can say, improved.

The objective of this Regulation is to enhance the electronic transaction based on signature and promote trust in electronic transactions. The eIDAS Regulation is the first concrete measure of the European Commission taken towards the strategy of single digital market which should become real in the European Union until 2020. The mentioned regulation aims to harmonize the requirements for mutual recognition of electronic identification in respective Member States. As noted in the abstract of this paper, its aim is to simplify not only the electronic commerce but also all other cross-border transactions and to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between the citizens, businesses and public authorities and this way increase the effectiveness of public and private online services, electronic business and electronic commerce in the European Union. New regulation has been labelled as revolutionary with significant impact, especially, on the sphere of private-law proceedings and submission of documents in processes of authoritative application of law.[5]

The eIDAS Regulation stipulates the requirements for providing trust services for electronic transactions in the internal market which include services provided in the sphere of electronic signature and defines several new types of trust services.

---

5 Polčák, R., Nařízení eIDAS [http://ict-law.blogspot.sk/2014/09/narizeni-eidas.html] Accessed 21 January 2018

This regulation defines conditions under which the Member States can recognize means for electronic identification of natural persons and legal entities issued by the Member States. Moreover, this regulation also provides for the requirements for trust services, namely, services for issuance, verification and validation of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and services for issuance, verification and validation of certificates for website authentication and requirements under which the Member States provide certificates and recognize electronic signature creation devices and recognize the electronic identification means of natural persons and legal entities which are included in the notified electronic identification scheme of another Member State.

With the adoption of this regulation, the directive on electronic signature was repealed, and, as a result, the legislation on electronic signature in several Member States was repealed. The Slovak republic was no exception. According to the European Commission, the legislation in the Member States of the EU was not compatible, which significantly hindered the cross-border transactions. Under point 3 of this Regulation, the Directive 1999/93/EC addressed electronic signatures without delivering a comprehensive cross-border and cross-sector framework for secure, trustworthy and easy-to-use electronic transactions. Further, the Regulation also viewed as problematic those cases when the citizens of the European Union could not use their electronic identification to authenticate themselves in another Member State, because the national electronic identification schemes in their country were not recognized in other Member States. This barrier prevented the service providers from enjoying the full benefits of the internal market. According to the drafters of the Regulation, mutually recognized electronic identification means will facilitate cross-border provision of numerous services in the internal market and enable businesses to operate on a cross-border basis without facing many obstacles in interactions with public authorities. Based on this, the Act on e-Government was adopted representing the fundamental legal regulation of identification and authentication of persons in the Slovak republic. Its aim was to provide for general legal regulation of the electronic form of governance of public authorities including the related legal concepts, and thus enable the implementation of electronic services of public authorities in a uniform manner, without intervening into every special legal regulation governing the concrete cases of governance.[6]

---

[6] See Explanatory report to the Act on electronic form of governance of public authorities as amended (Act on e-Government) available at [http://www.nrsr.sk/web/Default.aspx?sid=zakony/zakon&MasterID=4500] Accessed 21 January 2018

The eIDAS Regulation was implemented by the Act no. 272/2016 Z.z. (Collection of Acts) on trust services for electronic transactions in the internal market (Act on trust services). We can say that it aimed to amend the eIDAS Regulation and adjust it to our legal conditions and environment. This Act repealed the Act no. 215/2002 Z.z. (Collection of Acts) on electronic signature and brought about changes connected with harmonization of procedure in providing trust services and securing supervision. Moreover, it also regulated the competences of the National Security Authority and the liability for infringement of duties. According to the explanatory report to the Act on trust services, this Act amended the eIDAS Regulation in those areas which were entrusted to the exclusive competence of the Member State so that the proposed legislation together with the eIDAS Regulation formed a compact, transparent and applicable legal regulation.[7]

Under the eIDAS Regulation, emphasis should be placed on the requirements for use of electronic signatures and on the documents that bear the electronic seal. The first requirement for the validity of the electronic signature to be fulfilled is that it must be issued by the acting person. The form of the carrier, whether the signatory signs on the paper or, for example, on the tablet, is not relevant. The second requirement concerns the implementation of the content of the legal act. It means that it is important to secure that the content of the signed document and the digital signature is implemented and contained (locked) in one file without any subsequent possibility to alter its content. Finally, the third requirement inevitable for the validity of the signature is the identification of the person who carried out the legal act, which can be done, for example, by providing the name and surname at the signature. Various specialized software tools are available on the market for electronic signatures which can guarantee the Contractual parties that electronic signatures are secure and comply with the valid legislation. Under the regulation, the signatory would have the option to entrust the qualified electronic signature creation devises to a third person on the condition that appropriate mechanisms and procedures are introduced that would secure the signatory can have sole control over the use of his data for the issuance of electronic signature, and when using the devise, all requirements for qualified electronic signatures be fulfilled. The above mentioned is also connected with the protection of personal data under the new General Data Protection Regulation (also "*GDPR*") which enters into effect in the entire European Union in May 2018.

[7] See Explanatory report to the Act on trust services for electronic transactions in the internal market available at [https://www.nrsr.sk/web/Dynamic/Download.aspx?DocID=426794] Accessed 21 January 2018

The eIDAS Regulation defines several types of electronic signatures which are classified based on the level of security assurance. It distinguishes electronic signature, advanced electronic signature, advanced electronic signature based on a qualified certificate and qualified electronic signature. Viewed from the eIDAS Regulation, the qualified electronic signature provides the highest level of security assurance, and this electronic signature is issued by the signatory with data for the creation of electronic signature (private key) which are located in the qualified electronic signature creation devices (QSCD) for which the qualified certificate containing data for the validation of electronic signature (public key) was issued, identity of this person (signatory) and the person responsible for the issuance of this certificate (qualified trust service provider for issuance and authentication of certificates). The definition of the qualified electronic signature, in its essence, corresponds to the definition of guaranteed electronic signature which was used in our conditions based on the repealed Act on electronic signature. The procedure of technical implementation of this type of signature remains intact. This procedure is, however, supplemented by another option when the qualified trust service providers administering data for the issuance of qualified electronic signature in the name of the provider may disseminate data for the issuance of qualified electronic signature only for back-up purposes. The eIDAS Regulation also contains definitions of various types of electronic signatures which for the purposes of this paper will not be further analyzed.[8]

As regards the electronic signature and legal acts implemented by virtually secured electronic signature, the practical application has drawn major attention to various methods of electronic signing. In relation to mutual recognition of electronic signatures, the eIDAS Regulation stipulates that such acts require high level of security assurance, although electronic signatures of lower level of security assurance can also be accepted. The legal effect of the legal act bearing electronic signature which fails to comply with the requirements for the qualified electronic signature, though, is questionable. Under the Regulation, such electronic signature cannot be denied its legal effect despite that it fails to comply with the requirements of qualified electronic signature, and it provides for the national legislation to resolve on the legal effect of such signatures. Under the Regulation, the qualified electronic signature has the equivalent legal effect of a handwritten signature. This must also be guaranteed in national legislation. Moreover, its importance must also be highlighted in connection with court proceedings considering, for example, the validity of electronic contract or the validity of electronic signature. The consid-

[8] Treščáková, D., *Virtuálna identita a elektronické schránky – vzájomné súvislosti*, in Studia Iuridica Cassoviensia (Law Journal of Law Faculty, can be reached here: [http://sic.pravo.upjs.sk/]) Vol. 5, No. 1, 2017, pp. 113-120

eration of electronic signature is essential with regards to evaluation of electronic evidence submitted in court proceedings.

The eIDAS Regulation complies with the above given and underpins the importance of the electronic documents in the further development of cross-border electronic transactions in the internal market. This Regulation should provide for a principle under which the electronic document should not be denied its legal effect by reason that it is in the electronic form and it is important to secure, through this Regulation as well, that the electronic transaction is not to be rejected just because the electronic document is issued in electronic form. As noted earlier, electronic business is actually proper (traditional) business activity which is conducted in the virtual world in the electronic environment by making use of electronic means. Electronic documents and the electronic business must be conducted in compliance with legal regulations and it may not contradict the national and European legislation. This is connected with the trust in electronic transactions and services. Full-scope use of electronic services requires the online services be trustworthy and ease-to-use. To this end, the EU trust mark should be introduced for identifying qualified trust services provided by qualified trust service providers. This EU trust mark for qualified trust services would clearly differentiate between qualified trust services and other trust services and eventually lead to transparency on the market. Using the EU trust mark on the part of qualified trust services providers should be on a voluntary basis and would not require any additional requirements apart from those enshrined in this Regulation.

3. LAW OF COOKIES

Legislative changes can also be identified with regard to the protection of privacy in the digital environment. Current legislation regarding the protection of privacy in electronic communications is contained in the Directive 2002/58/EC on privacy and electronic communications[9]. However, due to the implementation problems associated with this Directive, a new regulation[10] has been proposed, focusing on various issues. One of the most significant aims of the new proposal is to alter the current regulation of cookies.

---

9 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). *OJ L 201, 31.7.2002,* p. 37–47

10 Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). *COM/2017/010 final - 2017/03 (COD)*

In general, we can describe cookies as small text files placed in the end-user's terminal equipment by a website´s server for storing and transmitting desired information back to the website's server[11]. GDPR recognizes cookies as online identifiers that „*may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them*"[12]. It is our view, that the use of cookies that are uniquely assigned to a device and can therefore identify an individual, fall within the scope of the term 'personal data' and are protected by the relevant provisions of GDPR.

The Proposal together with GDPR proposes various changes to the existing legislation. Firstly, with regard to the need to obtain consent. In the current practice websites usually inform their end-users about the use of cookies and do not require them to provide explicit consent for their use through an active action. Therefore, only implicit consent is provided. However, the new regulation is clearer in this regard, as it stipulates the need to obtain the explicit consent of the end-user with the use of cookies. Furthermore, the controller will have to be able to demonstrate that such consent has been provided.

Secondly, to make the provision of consent more user-friendly, the Proposal stipulates a new process for providing consent consisting of expressing user's consent through appropriate settings of a browser or other application and not separately for every website. A set of privacy settings should be available to users that range "*from higher (for example, 'never accept cookies') to lower (for example, 'always accept cookies') and intermediate (for example, reject third party cookies' or 'only accept first party cookies')*"[13]. Moreover, browsers will also be obligated to inform users about cookies and their privacy settings options in and after installation, which is currently absenting in most browsers. These, of course, are not the only changes contained in the Proposal, but from our point of view, the most relevant for the ordinary end-user.

---

11 See [https://europa.eu/youreurope/business/cookies/index_en.htm] Accessed 21 January 2018

12 Recital 30 of the Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). *COM/2017/010 final - 2017/03 (COD)*

13 Recital 23 of the Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). *COM/2017/010 final - 2017/03 (COD)*

4. CYBERSECURITY AS ONE OF THE PILLAR OF THE DIGITAL SINGLE MARKET

2017 was the year, in which sophistication and complexity of attacks or other malicious actions in cyberspace continue to increase. The top threats in the last year's cyberthreat landscape is malware, web based attacks, phishing, ransomware etc.[14] These threats can have a huge impact on the functioning of the organizations' and states´ basic services. As example we can mention ransomware WannaCry, which affected organizations and states across the European Union, including hospitals (e.g. UK, Slovakia), postal services (e.g. FedEx), passenger and freight transport (e.g. Deutsche Bahn). Another example is ransomware NotPetya that disrupted a transport companies (e.g. TNT, Maersk), but also Ukrainian nuclear plant.

The European Union reflects these threats when it states that the main aim of the second pillar of Digital Single Market Strategy is to enable secure environment for information society services. In other words, it is important to ensure the security of networks and information systems that create an environment for implementation and operation of the information society services. Article 4(2) of The Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (hereby "NIS Directive") defines security of network and information systems as "the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems"[15].

To protect the Europe's networks and information systems, it is needed to tackle cybersecurity challenges on a daily basis. In other words, events need to be addressed, which have an actual adverse effect on the security of network and information systems. These events are defined as (security) incident[16]. All procedures supporting the detection, analysis and containment of an incident and the response thereto can be defined as (security) incident handling[17].

---

14 Marinos, L., Belmonte A, Rekleitis E., T*hreat Landscape Report 2017: 15 Top Cyber-Threats and Trends,* Heraklion: European Union Agency for Network and Information Security Publishing. ISBN 978-92-9204-250-9

15 Article 4(2) of NIS Directive

16 Article 4(7) of NIS Directive

17 Article 4(8) of NIS Directive

4.1. Legal framework for the incident handling

The last years was significant from the perspective of cybersecurity. In year 2016, a basic European legal framework has been adopted to clarify the rules for incident handling.

The basic legal document for the incident handling is also above mentioned NIS Directive. This directive was adopted by the European Parliament on 6 July 2016 and entered into force in August 2016. Member states had 21 months to transpose this directive into their national laws. The deadline for member states transposing this directive into domestic legislation is 9 May 2018. For example, in the Netherlands a mandatory breach reporting law for critical sectors was adopted in 2017 and went into force on 1 January 2018. In Slovakia, Cyber security Act was adopted in January 2018 and went into force on 1 April 2018.

For the area of personal data incident handling it is important Regulation 2016/679 on protection of natural persons with regard to the processing of personal data and on free movement of such data, and repealing Directive 95/46/EC. This regulation was adopted by the European Parliament on 27 April 2016 and entered into force in 25 May 2018.

The incident handling is also part of other legal documents. Example is Directive 2015/2366 on payment services in the internal market (hereby "PSIM Directive"). This directive was adopted by the European Parliament on 25 November 2015 and entered into force in December 2016. Member states had to adopt and publish the measures necessary to comply with this directive by 13 January 2018.

In the following section we deal with one of the important aspect of incident handling - notification of (security) incident.

4.2. Notification of (security) incident

Notification of (security) incident is part of (security) incident handling. Within this chapter, we focus on notification of (security) incident from the point of view of three legal acts, namely the NIS Directive, the GDPR and the PSIM Directive. Notification of (security) incident can be classified as mandatory notification (Article 14 of GDPR, Articles 33,34 of NIS Directive, Article 96 of PSIM Directive) and voluntary notification (Article 20 of NIS Directive). Voluntary notification means that "entities which have not been identified as operators of essential services and are not digital service providers may notify, on a voluntary basis, incidents

having a significant impact on the continuity of the services which they provide[18]. The following text will be addressed mandatory notification.

In the notification of (security) incident, answer several issues need to be:

- Who notifies the (security) incident?
- Whom is the (security) incident notified?
- What kinds of (security) incidents shall be notified?
- What is the time period for notify the (security) incident?

The first and the second issue are linked to entities who are required to notify the (security) incident (hereby "breached entity") and the persons to whom the (security) incident is notified (hereby "notified entity"). According to the NIS Directive the breached entities are operators of essential services and digital service providers (e.g. provider of e-shops). They report (security) incidents to competent authority or Computer security incident response team (hereby "CSIRT").

In case of personal data incidents (e.g. personal data breach), breached entities are the controller and the processor. They notify (security) incidents to supervisory authorities. When (security) incident (the personal data breach) is likely to result in a high risk to the rights and freedoms of natural persons, they notify this type of (security) incident to the data subject.

An intersection of these two sets exists: operators of essential services and digital service providers, the controller, the processor. Therefore, there will be situations where the entity will have to notify an incident to multiple entities. For example, digital service providers are an Internet Service Provider (ISP), and an attack on its infrastructure is underway. The result might be data leakage, including personal data. In this case, the ISP notifies the incident to the CSIRT team, the supervisory authorities, and will need to consider reporting to the data subject.

In the case of the payment services, breached entity is payment service providers (e.g. credit institutions, electronic money institutions, payment institutions). They notify competent authority of the (security) incidents in their home member state. If (security) incident has or may have an impact on the financial interests of its payment service users, the payment service provider shall inform its payment service users. Specific element of payment services is hierarchical notification of (security) incidents, because competent authority of the home member state shall inform the European banking authority (EBA) and the European Central

[18] Article 20(1) of NIS Directive

Bank (ECB). In some cases, ECB shall notify the members of the European System of Central Banks on issues relevant to the payment system.

The third issue is type of the (security) incident, which needs to be notified., the operators of essential services notify of incidents having a significant impact on the continuity of the essential services they provide[19]. In order to determine the significance of the impact of the (security) incident, the following parameters shall be taken into account[20]:

a) the number of users affected by the (security) incident
b) the duration of the (security) incident
c) the geographical spread with regard to the area affected by the (security) incident.

On the other hand, that digital service providers (e.g. provider of e-shop) notify of any (security) incident having a substantial impact on the provision of a service[21]. In order to determine whether the impact of an incident is substantial, same parameters like significance of the impact shall be taken into account. Moreover, two parameters shall be taken into account[22]:

a) the extent of the disruption of the functioning of the service
b) the extent of the impact on economic and societal activities.

The GDPR focuses on specific type of the (security) incident – a personal data breach. It means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed[23]. It's a different point of view on a security incident. While The NIS Directive divides types of (security) incident according to their impact, the GDPR does not consider impact but it behavior itself.

The PSIM Directive states the major operational and security incidents, but it doesn't define the terms. Usage of words operational and security leads to conclusion that this directive does not apply onto to notification of security incidents, but also incidents related standard operations of payment systems, where it may not necessarily be a security breach, for example incidents that might occur while replacing hardware parts, or switching to different internet service provider (ISP).

---

19 Article 14(3) of the NIS Directive
20 Article 14(4) of the NIS Directive
21 Article 16(3) of the NIS Directive
22 Article 16(4) of the NIS Directive
23 Article 4(12) of the GDPR

The last issue is period for notification of the (security) incident. The security incidents shall be notified without undue delay. In case of personal data incidents, not later than 72 hours after the controller or the processor having become aware of the (security) incident. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

Only GDPR states the maximum threshold for notification without undue delay. Other legal documents leave it for consideration by notified entity. Time of notification is determined by several factors, whether it be technical, legal, or organizational. It should be considered depending on type and impact of the incident. In the future, when concrete statistical data will be available, it should be possible to set a real estimated time needed for notification of an incident. However here as well, one will have to consider the specifics of notified entities.

Aforementioned notes are summarized in **Table 1.**

Legal framework	Breached entity	Notified entity	Type of (security) incident	Period for notification
NIS Directive	Operators of essential services Digital service providers	competent authority, CSIRT	Incident - significance of the impact Incident - substantial impact	without undue delay
GDPR	controller and the processor	supervisory authorities, data subject	personal data breach	without undue delay (max. 72 hours)
PSIM Directive	payment service providers	competent authority, payment service users, EBA, ECB, European System of Central Banks	major operational and security incidents	without undue delay

5. CONCLUSION

The Digital Single Market denotes the strategy of the European Commission to ensure access to online activities for individuals and businesses under conditions of fair competition, consumer and data protection removing geoblocking and copyright issues.

On 10 May 2017, the Commission published a mid-term review of the Digital Single Market Strategy.[24] It presents and evaluates the progress in implementing the Strategy since 2015[25] and highlights where further actions are needed.[26] The mid-term review is accompanied by the European Digital Progress report which gives an in-depth assessment of how the EU and Member States are progressing in their digital development and identifies potential steps to help improve national performance in digital.

In this paper only three legislative tools of the Digital Single Market are discussed. Authors are aware that also other aspects and their legal regulation should be also discussed but due to the limited space, abovementioned issues were chosen to be analyzed and presented in the paper. Last year was according to the legislative plans of the European law very important. The Joint Declaration on EU legislative priorities highlighted a political responsibility for the EU institutions to finalize key legislation under the Digital Single Market by the end of 2017. Legislation in the last year was concentrated on the internet connectivity for all, a better online marketplace for consumers and businesses, building an innovation-friendly environment though effective enforcement, the protection of privacy and personal data in the internet, improvement the conditions to create and distribute content in the digital age.

There are several policy actions under way within the Digital Single Market Strategy, which need increased efforts in order to seize the opportunities and address the challenges of digitization. Further legislative and political attention will be dedicated to the digital skills and opportunities for all, startups and digitization of industry and service sectors, digital innovation for modernizing public services, necessary investments in digital technologies and infrastructures. The last mentioned area is connected with the actions in the sphere of a European Open Science Cloud, high performance computing and European data infrastructure. Also actions concerning artificial intelligence must be discussed and prepared. Artificial intelligence can bring major benefits to our society and will be a key driver for future economic and productivity growth. Equipping devices and ser-

---

24 Mid-Term Review of the Digital Single Market Strategy: [https://ec.europa.eu/digital-single-market/en/news/digital-single-market-mid-term-review] Accessed 21 January 2018

25 The Digital Single Market Strategy was adopted on the 6 May 2015 and includes 16 specific initiatives which have been delivered by the Commission by January 2017. Full text of Digital Single Market Strategy: [http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX-%3A52015DC0192] Accessed 21 January 2018

26 [https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market] Accessed 21 January 2018

vices with some form of intelligent behavior can make them more responsive and autonomous.

REFERENCES

BOOKS and ARTICLES

1. Marinos, L., Belmonte A, Rekleitis E., *Threat Landscape Report 2017: 15 Top Cyber-Threats and Trends*, Heraklion: European Union Agency for Network and Information Security Publishing. ISBN 978-92-9204-250-9
2. Polčák, R., *Nařízení eIDAS*, [http://ict-law.blogspot.sk/2014/09/narizeni-eidas.html] Accessed 21 January 2018
3. Suchoža, J., Husár J. et al., *Obchodné parvo*, Bratislava, Iura Edition, 2009
4. Treščáková, D., *Virtuálna identita* a *elektronické schránky – vzájomné súvislosti*, in Studia Iuridica Cassoviensia (Law Journal of Law Faculty, [http://sic.pravo.upjs.sk/]) Vol. 5, No. 1, 2017, pp. 113-120

EU LAW

1. Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union ("NIS Directive")
2. Directive 2015/2366 on payment services in the internal market ("PSIM Directive")
3. 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, GDPR")
4. Regulation (EU) 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC ("Regulation eIDAS")