Articles

Studia Iuridica Lublinensia vol. 31, 3, 2022
DOI: 10.17951/sil.2022.31.3.61-84

Bashkim Nuredini
University for Business and Technology, Republic of Kosovo
ORCID: 0000-0002-9748-2047
bashkim.nuredini@ubt-uni.net

Jorida Xhafaj
University for Business and Technology, Republic of Kosovo
ORCID: 0000-0002-1191-150X
jorida.xhafaj@ubt-uni.net

Vesna Paukovska Dodevska
Legal and Corporate Affairs Department, North Macedonia
ORCID: 0000-0002-4849-0059
vesna.paunkoska@triglav.mk

A Comparative Overview of Data Protection in e-Commerce in the European Union, the United States of America, the Republic of North Macedonia, and Albania: Models and Specifics

Prawnoporównawcze ujęcie zasad ochrony danych osobowych w handlu elektronicznym w Unii Europejskiej, Stanach Zjednoczonych, Republice Macedonii Północnej i Albanii. Modele i specyfika

CORRESPONDENCE ADDRESS: Jorida Xhafaj, PhD (corresponding author), Assistant Professor at the Faculty of Law, University of Business and Technology (Prishtina), Lagjja Kalabria, 10000 Prishtine, Republic of Kosovo; Bashkim Nuredini, PhD, Assistant Professor at the Faculty of Law, University of Business and Technology (Prishtina), Lagjja Kalabria, 10000 Prishtine, Republic of Kosovo; Vesna Paukovska Dodevska, PhD, Head of the Legal and Corporate Affairs Department, Triglav Insurance, 1000 Skopje, North Macedonia.

ABSTRACT

The advantages of electronic communications in the e-commerce sector and the rapid exchange of information continue to have enormous benefits, but they come at a cost in terms of privacy protection and legal gaps. Privacy is defined differently in each jurisdiction – the EU and the US, and despite widespread agreement on the importance of privacy, there is no single definition of the concept in scientific circles. The difficulties of transferring personal data between the European Union and the United States were once again at the forefront of the country's highest privacy and data protection concerns. General Data Protection Regulation (GDPR) positioned data protection to the highest level of company directions throughout the requirements imposed on any organization that collects, processes, manages, or stores information about European citizens, requiring stricter standards and giving users more control over their data. The new regulation has an impact on businesses and users all over Europe. The study's goal is to compare the level of protection and security provided to e-commerce users in the European Union, the United States of America, the Republic of North Macedonia, and Albania. Also, the correlation between the obligations and the effect of the GDPR was studied in order to determine whether it will guarantee a higher level of protection of individuals' rights, or whether will it primarily result in the bureaucratization of the processes for protecting personal data performed in e-commerce actions.

Keywords: data protection; e-commerce; GDPR; jurisdiction; European Union; United States; Republic of North Macedonia; Albania

INTRODUCTION

Privacy is commonly defined as a person's or a group's ability to self-determine, protect, and selectively share information about themselves. The area of privacy intersects with the sphere of security, which might involve elements of proper usage, information, confidentiality, and protection. Many nations' privacy laws and, in certain countries, constitutions protect the right not to be exposed to unlawful invasions of privacy by the government, companies, or individuals. While both the right to privacy and the right to personal data protection is enshrined in Article 8 of the EU Charter of Human Rights, they are regulated differently in many countries throughout the world. The degree to which personal data and privacy are protected when conducting electronic transactions appears to be determined by how these two rights are regulated. Furthermore, the authors believe that the level of development of electronic commerce affects the development of information privacy and protection of personal data. E-commerce has undoubtedly grown dramatically as technology and the Internet have sophisticated. Of course, countries with higher levels of economic development saw faster growth in e-commerce. The perception is that e-commerce is slower in developing countries; however, the COVID-19 pandemic has accelerated the process of digitalization in low-income countries. E-commerce presents numerous benefits, the most notable of which are convenience and the broader availability of goods and services, and its rise is seen as becoming suitable

for both producers and consumers.[1] This expansion is completely explained given to the e-efficacy of commerce, such as the option to buy products instantaneously from anywhere, the vast array of options available when shopping online, and the increasingly competitive pricing. The advent of e-commerce, on the other hand, can bring with it a slew of legal, socioeconomic, and trust issues.

Since it is practically impossible to purchase without giving personal details, data privacy has suddenly emerged as one of the most critical and serious risks in e-commerce.

The data and information collected and their processing goes beyond the direct purposes of e-commerce, being used for purposes of customized advertising, personalized services, and strategic relationships with customers. Consequently, the awareness has grown steadily, especially in developing nations where these principles have been emphasized largely in the last two decades, and customers are being warned about the misuse of personal data, which may weaken their belief in the website's service.[2] In light of the issues surrounding privacy and the protection of personal data, many countries worldwide have introduced laws and regulations to safeguard their citizens' and organizations' information privacy. The main issues elaborated with the regulations, laws, and procedures are personal data protection principles such as data minimization and limited use, data characteristics, purpose determination, security safeguards, transparency, and accountability. The European Community recognized the need to harmonize data protection rules inside its Member States more than two decades ago intending to promote cross-border data transfers within the EU.[3] According to some authors, such as P. Voigt and A. Bussche, Data Protection Directive did not live up to its objectives and failed to align the level of data protection within the EU. The primary reason for this is that European directives are not directly relevant in all EU Member States and must be incorporated into national legislation. National data protection legislation at the time provided significantly diverse degrees of protection and could not give legal certainty for natural or juridical persons acting as data controllers and processors.[4] The heterogeneity of data protection between the EU Member States, as well as the associated legal uncertainty, were deemed to be an impediment to the development of economic activity at the EU level, resulting in competitive

[1] B. Nuredini, V. Paunkoska Dodevska, *Legal Aspects of Electronic Contracts*, UBT Conference, October 2020, https://www.researchgate.net/publication/353515427_Legal_aspects_of_electronic_contracts (access: 20.3.2022).

[2] R.R. Sarathy, C. Robertson, *Strategic and Ethical Considerations in Managing Digital Privacy*, "Journal of Business Ethics" 2003, vol. 46(2), pp. 111–126.

[3] P. Voigt, A. Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, "Axel von dem Bussche Taylor Wessing" 2020, vol. 13(2), pp. 1449–1452.

[4] B. Wolford, *What is GDPR, the EU's New Data Protection Law?*, https://gdpr.eu/what-is-gdpr (access: 10.2.2022).

distortion.[5] In distinction to the Data Protection Directive, the GDPR applies automatically to the EU Member States. The GDPR would increase legal clarity and reduce any barriers to the free movement of personal data by standardizing data protection regulations. In terms of developing the digital economy across the EU-internal market, the EU intends to reestablish people's trust in the appropriate use of their data.[6] For this purpose, companies are experiencing increased data protection duties along with pre-existing obligations under the GDPR, taking into account the obstacles and difficulties of the global economic environment, emerging technologies industries, and also the consequent operating models, as well as developing a broad range of applications that affect many companies. The looming fines, as well as the data protection duties, have been drastically enhanced, and companies must meticulously restructure their internal data protection systems throughout to comply with the GDPR. So, the GDPR requires data processing subjects to implement operational conditions tailored to the nature, span, and circumstances of the processing, the purposes of the processing as well as the risks to individuals' rights and freedoms of varying likelihood and severity. In the United States, the laws aim to provide "reasonable" safeguards to protect the security, confidentiality, and integrity of private information by utilizing sectoral data protection.[7] This type of strategy has been regarded as one of the most successful approaches, and it is consistent with the EU's new approach to ensuring not only comprehensive data protection measures but also an appropriate level of protection.[8] In states like Illinois, a unique state law is applicable that sets rules on legal entities that acquire or obtain biometric data.[9] Financial services, healthcare, telecommunications, and education are just a few of the industries that have sector-specific legislation in place. In the same vein, personal information in the hands of commercial banks, insurance firms, and other financial institutions[10] is ensured, as is the restriction of the use of the information pertaining to a persons'

[5] Articles 7 and 9 of 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) (OJ L 119/1, 4.5.2016), hereinafter: the GDPR.

[6] *Data Protection Laws and Regulations 2021–2022: International Comparative Legal Guide*, Global Legal Group 2021, https://iclg.com/practice-areas/data-protection-laws-and-regulations (access:18.11.2021).

[7] S.M. Boyne, *Data Protection in the United States*, "American Journal of Comparative Law" 2018, vol. 66(1), pp. 299–343.

[8] R.M. Gömann, *The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement*, "Common Market Law Review" 2017, vol. 54(2), pp. 567–590; C. Ryngaert, M. Taylor, *The GDPR as Global Data Protection Regulation?*, "AJIL Unbound" 2019, vol. 114, pp. 5–9.

[9] Gramm-Leach-Bliley Act, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act (access: 7.9.2021).

[10] *Ibidem*.

credibility and history, financial capability, personal characteristics, or way of life to assert eligibility for certain financial interests, employment, insurance,[11] health status reporting[12] or payment for healthcare, restrictions on telephone solicitation, the use of automated phone equipment, pre-recorded voice messages, messages, and faxes, as well as automatic calling.[13]

METHODOLOGY

Different approaches to data privacy and protection exist in the United States, the European Union, and developing nations like Albania and the Republic of North Macedonia for a variety of reasons, with self-regulation and government regulation being the most prevalent.

The paper is divided into five sections. One of the objectives is to discuss the obligations provided by each legal framework, as well as to evaluate the legal mechanisms to address the issue of the expected and appropriate levels of protection. Second, the study analyzes regulation in both the EU and the US approach, intending to confront perspectives and identify the strengths and challenges of each of the systems, which appear to have the same principles but different levels of specification and regulation. The findings of the study determine which of them has a higher level of safeguard and security, and thus which system is more similar to the one used in the Republic of North Macedonia and Albania. The authors conducted a legislative assessment across several federal and state jurisdictions in the United States in the domain of data protection, as well as a review of the general aspects and specifics used in e-commerce. According to the empirical method, there is no single law in the United States that addresses information privacy and data protection. The study shows that regulation of personal data through specific policies in many federal and state laws can be compared to European Union regulation on personal data protection.

In addition, based on a systematic examination of the evolution of the legal framework and concerns in an e-commerce context, it should be emphasized that they are largely left to the development of their privacy policy statement based on industry standards and voluntary compliance.

---

[11] See Fair and Accurate Credit Transactions Act, http://uscode.house.gov/view.xhtml (access: 7.9.2021.

[12] See Health Insurance Portability and Accountability Act of 1996 (HIPAA), http://www.legalarchiver.org/hipaa.htm (access: 7.9.2021).

[13] Federal Statute on the Telephone Consumer Protection Act, 47 U.S.C. § 22, https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/8/viii-5-1.pdf (access: 7.9.2021).

RESEARCH AND DISCUSSION

1. Privacy and data protection in e-commerce

In this study section, the authors have analyzed EU e-commerce legislation to investigate the standards and their adaptability to dynamic technological developments and other circumstances, whether unexpected or significant, such as the COVID-19 pandemic situation. According to Statista's report retail e-commerce sales worldwide from 2014 to 2024, reached 4.28 trillion US dollars in 2020, with e-retail revenues expected to reach 5.4 trillion US dollars in 2022.[14] Online commerce is one of the most common and prominent activities around the world wide.[15] Without a doubt, the coronavirus pandemic has propelled e-commerce[16] to the forefront of retail, and the risks of personal data misuse are growing as e-commerce and the use of personal data through e-commerce become more prevalent. One of their major difficulties is the interception or misuse of users' data, as well as the illicit trade of their personal information for commercial purposes. According to D.J. Ugo, the main impediment to shopping on the Internet is privacy and security concerns which prevail in threats, impersonation and forged identity, children protection, email safety, and censorship. Based on the author's survey this led to the idea to allocate resources and efforts to address the concerns of IT users.[17] The authors consider that such a direct relationship between action and risk can have an impact on the consumers' final decision to discontinue using an e-commerce service. Threats to an e-commerce site can jeopardize its visitors' personal information. These could be unintentional, deliberate, or the result of human inaccuracy. The most mainstream consumer privacy vulnerabilities are phishing and social engineering[18] as well as the theft of financial or personal information via a variety of hacking techniques, all of which stress the role of having the proper data privacy precautions to protect customers and visitors to e-commerce sites.

[14] S. Chevalier, *Retail e-Commerce Sales Worldwide from 2014 to 2025*, 4.2.2022, https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales (access: 20.5.2021).

[15] *Ibidem*.

[16] A. Bhatti, H. Akra, H.M. Basit, A.U. Khan, S.M. Raza, M.B. Naqvi, *E-commerce Trends during COVID-19 Pandemic*, "International Journal of Future Generation Communication and Networking" 2020, vol. 13(2), pp. 1449–1452.

[17] G.J. Udo, *Privacy and Security Concerns as Major Barriers for e-Commerce: A Survey Study*, "Information Management & Computer Security" 2001, vol. 9(4), pp. 165–174.

[18] J. Jang-Jaccard, S. Nepal, *A Survey of Emerging Threats in Cybersecurity*, "Journal of Computer and System Sciences" 2014, vol. 80(5), pp. 973–993.

2. Legal privacy and data protection regulations for e-commerce in the European Union

As noted previously, the EU has well-developed legislation in the field of e-commerce, addressing primarily legal issues related to contractual information and the withdrawal period. The GDPR's application areas were previously considered concerning the protection of privacy and personal data through e-commerce at the EU level; the companies are expected to complete a sequential and expensive proposition to ensure compliance with the GDPR. As a result, based on Article 2 of the GDPR, it will enforce the processing of personal data that is wholly or partially automated, as well as the processing of personal data that is not automated and is part of or intended to be part of an operating or so-called filling system. This applies to any processing of personal data and is important for businesses that deal with e-commerce. The material scope is interpreted broadly in order to broaden its effect and ensure prevailing legal protection. The circumstances in which the GDPR applies to data controllers and processors located in the EU are outlined in Article 3 (1), whereas paras 2 and 3 of the same provision establish the circumstances under which the GDPR applies to entities operating outside EU territory or who are located in a country where Member State law applies following public international law, such as diplomatic missions or consular posts.[19] So, according to this paragraph, the main criteria are related to the direct appliance of the territorial criteria which led to connection with EU countries and bodies that function under the rules of international public law.

According to N. Feiler, N. Forgó, and M. Weigl, the GDPR will be obligatory if there is a substantial and particularly economic connection between the operations of the EU establishment and the processing of the data that occurs outside the EU.[20] According to the Court of Justice of the European Union in the case of *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*,[21] a very broad reading of the phrase "in the context of the activities of an establishment" gives the GDPR exterritorial effect. A. Azzi defines the GDPR's results as significantly increasing the scope of EU data protection rules unilaterally and even to a greater extent than nearly any other national authority globally.[22] Significantly, the GDPR was designed to have a specifically extraterri-

[19] T. Maria, *Data Protection / Data Privacy*, [in:] *Elgar Encyclopaedia of Human Rights*, https://ssrn.com/abstract=3859440 (access: 10.2.2022).

[20] *The EU General Data Protection Regulation (GDPR): A Commentary*, eds. N. Feiler, N. Forgó, M. Weigl, New York 2018, p. 331.

[21] Judgement of the CJEU of 13 May 2014 in case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*.

[22] A. Azzi, *The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation*, 2018, vol. 9, "Journal of Intellectual Property, Information Technology and E-Commerce Law" 2018, vol. 9(2).

torial scope because it affects any controller or processor supplying goods to any EU data user or monitoring their behavior. Without changing the responsibility or liability of the controller or processor for the processing activities, the foreseen obligation ensures that Supervisory Authorities and data subjects have a written representation in the EU.[23] In a more concrete sense, e-commerce entities located outside the EU that conduct commercial activities will process orders and store customer data. The company might appoint a representative in at least one Member State where data subjects are impacted by the entity's processing activities because it has no branches or representations outside. Cases in which the legislator determined a minimal risk for data privacy are covered by the GDPR exclusions outlined in Article 27. This includes infrequent processing that won't have a negative impact on certain categories of personal data or information about prior convictions and criminal acts but isn't likely to endanger an individual's freedoms and rights. All three conditions must be met concurrently. Based on a thorough understanding of the provisions, it is logical to argue that the GDPR does not define "occasional" or large-scale processing, which may lead consequently to numerous conflicts, requiring the courts to define the criteria. In general, data processing should be regarded as "incidental" if it represents a small portion of the activity, lasts just briefly, or occurs just once. The nature, context, scope, and purposes of the processing must all be considered by the controller or processor to determine the likelihood of a threat to individuals' rights and self-determination. The second exemption states that governmental authorities or institutions are not required to do anything. The representative's main duties include serving as the supervisory authority's contact point, maintaining the controller's records of processing activities, and being liable for enforcement actions if the controller or processor fails to comply with the GDPR.

Entities planning or dealing with e-commerce must also take additional steps to comply with the GDPR and meet organizational requirements. We have put a halt to one of the requirements that must be met, such as the implementation of records of their processing activities, which allow them to demonstrate to the Supervisory Authorities their conformity to the GDPR and enable them to fulfill their obligations to data subjects. The most discussed one is the instrument of the so-called "opt-model" which requires consumer consent for personal information processing is required under the GDPR before data can be collected, and data can only be collected and processed sufficiently that is "reasonably necessary" according to Article 5 (1) of GDPR. In this way, the entities should ensure that data subjects access information about data processing, data erasing, and rectifying incomplete personal data.[24] This is the known GDPR's obligation of transparency regarding the processing of personal data. By enabling data subjects and users to

[23] According to Article 80 of the GDPR.
[24] According to Article 17 (3) of the GDPR.

comprehend and, if required, contest such processes, transparency seeks to instill confidence in those practices. It also embodies the fairness concept. The data protection principles involve transparency as a key component in the GDPR and are linked to fairness and accountability.[25]

The records of data must, along with other things, contain information on the processing's goals, the categories of data impacted, and a description of the organizational and technical security measures used. In some cases, if the intended processing activity, particularly the use of innovative tools or methods, is expected to pose a significant risk to the privacy rights of the involved subjects, so the entities planning or dealing with e-commerce must conduct a preventive Data Protection Impact Assessment. The Data Protection Impact Assessment seeks to determine the most effective countermeasures for data protection threats. Other steps that entities planning or dealing with e-commerce should take include implementing technical and organizational safeguards for personal data. The appropriate level of data protection and security precautions must be decided on an individualized basis and the findings from the risk analysis.[26] This leads the study to the conclusion that a specific and concrete estimation of appropriate requirements must be defined based on the characteristics of the information that is controlled, its sensitivity, the time that must be controlled, and the level of risk that each of the controllers faces. As a result, what is largely covered by the regulation as current legislation will be classified and specified depending on the details of the activities and the dangers associated with the data and information received from them. It appears to be a similar model to the American one but on a more concrete and sub-sectoral level.

Aside from the procedural obligations of controllers during the data collection and usage phases, a dedicated chapter of the GDPR outlines the anticipated transparency requirements that apply to data subjects' rights and more specifically on the information given to data subjects, communications with data subjects about the use of their rights,[27] and communications related to data breaches.[28]

The paper also examines in-depth Article 12 of the GDPR and the requirements that the aforementioned information or communication must follow. In practice, this would imply that any entity contemplating or engaged in e-commerce should publish a privacy notification on its website. Every page of the website should include a direct and visible connection to this notification, usually under one of the frequently utilized words, like "Data Protection Notice" or "Privacy Policy". The primary criteria that define a familiar and effective notice are evident text through

[25] According to Articles 13 and 14 of the GDPR.

[26] M. Hintze, K. El Emam, *Comparing the Benefits of Pseudonymisation and Anonymisation under the GDPR*, "Journal of Data Protection & Privacy" 2018, vol. 2(2), pp. 145–158.

[27] According to Articles 15 to 22 of the GDPR.

[28] According to Article 34 of the GDPR.

positioning or color schemes, specification, concrete terms, and easy accessibility to guarantee that information can always be accessed with just two clicks. Furthermore, based on Article 12 of the GDPR it is thought that clear and plain language fulfills the requirement because information should be given as clearly as possible, with compound words and language patterns avoided. The information should be explicit and conclusive; it should not be conveyed abstractly or ambiguously, nor should it necessitate clarification. Particularly, the reasons for data processing, as well as the legal grounds for it, must be made clear. In response to the need for greater clarity, the article is interpreted more thoroughly, in terms of language,[29] sentence structure, and simplicity of paragraphs should be written in an active and well-structured manner, with bullets and indents to signal hierarchical relationships and no excessively judicial, specialist, or professional terminology. Above all, the transparency component implies that any information provided under transparency obligations cannot be made based on business activities such as sales transactions. In this regard, it is worth noting that even if a controller shows certain consent characteristics, the GDPR restricts the scope of consent to processing authorization. In other words, consent does not exclude the controller from other GDPR requirements like reduction, accuracy, or erasure. In the case of violation of personal data, which might occur as a result of a technological or physical occurrence according to the GDPR, the controller is obliged to report to Supervisory Authorities. The notice must be made within 72 hours of being notified of the violation. In the case that the data subjects' rights are incidentally affected, the controller must also notify them of the breach, to whom the national authority will be available. The GDPR addresses a wide range of potential informational issues in order to enable people to conduct their daily lives electronically. We believe that the GDPR attempts to provide useful information questions in advance and before the risqué occurs, with the goal of not only ensuring, but also preventing misuse of data usage and clarifying all parties' responsibilities. Does the GDPR require this elevated consent, on par with major life decisions, or has it created only a principal, idealized, and ambitious regulation? According to R. Baldwin, M. Cave, and M. Lodge, the GDPR could be described as principles-based regulation,[30] referring to its general level of addressing the issue and lack of specificity. The authors deem that the regulation has created a comprehensive structure that supports data subjects' awareness and willingness to decide on their data usage while also defining the obligations of data controllers. This led to the necessity of a Data Protection Management System, as an

[29] Qualifiers such as "may", "might", "some", "often", and "possible" are classified avoidably. See *International Classification of Functioning, Disability and Health*, Geneva 2001, http://whqlibdoc.who.int/publications/2001/9241545429.pdf (access: 10.7.2021).

[30] R. Baldwin, M. Cave, M. Lodge, *Understanding Regulation: Theory, Strategy, and Practice*, Cambridge 2011, p. 303.

internal monitoring system that identify and eliminates issues and risks associated with data protection law. Even though the GDPR hasn't foreseen explicitly the implementation of a Data Protection Management System, an analysis of all of its requirements may reveal the need for such a system. This ensures the continuous optimization of processes and documents, as well as the establishment of clear and specific responsibilities.

3. Data protection regulations for e-commerce in the United States of America

As stated in section 2, there is no unified legal system for personal data protection in the United States of America. However, the entities which are planning or dealing with e-commerce in the USA are controlled by state and federal data protection laws. Also, entities founded in other countries may be accountable to both federal and state data privacy regulations for actions or activities concerning citizens of the United States and whose data is collected, hold, transmit, processed, or share. Practically it is similar to the territorial scope of the GDPR. Transparency, the lawful basis for processing, purpose limitation, data minimization, proportionality, and retention are the key principles defined in US data protection legislation, as they are in the GDPR. The Federal Trade Commission (FTC) has published guides promoting the principle of transparency in the context of e-commerce, recommending that entities planning or dealing with e-commerce:

- providing clear, shorter, and more standardized privacy notice/policy that helps customers to better understand privacy practices,
- giving consumers appropriate access to their data,
- increasing campaigns to educate consumers about commercial data security practices.

Although according to the US legislation there is no "lawful ground for data processing" prerequisite, the FTC recommends that entities provide notification to consumers of their data collection and administration and also should get their consent[31] when sensitive data is collected. The FTC also promotes privacy-by-design techniques such as restricting data gathering to what is necessary for the context of the company.

Almost identical to the GDPR, the US legislation prescribes the respective individual rights: the right of access to data or their copies, the right of correction of errors; the right of erasure, to object to processing, to restrict processing; the right to withdraw consent, to data portability; the right to oppose to advertising, and the

[31] K. Jamal, M. Maier, S. Sunder, *Enforced Standards versus Volution by General Acceptance: A Comparative Study of e-Commerce Privacy Disclosure and Practice in the United States and the United Kingdom*, "Journal of Accounting Research" 2005, vol. 41(1), pp. 73–96.

right to complain with the competent supervisory authority. Taking all of these rights into account, it is recommended that entities planning or dealing with e-commerce cover all of these rights and how they can be exercised in the Privacy Policy, which is published on their website. Few American states, such as California, Colorado, or Virginia, have implemented special state-level legislation to secure customer data. Another consideration is the appointment of a Data Protection Officer, which is not mandatory under US special laws,[32] contrary to what is stated in the GDPR. Other acts, however, demand the election or appointment of a person or group charged with enforcing the statute's compliance and data protection standards. As a result, the specific qualifications for the Data Protection Officer, his responsibilities and registration as well as notification to the relevant data protection authority are not described and there is no definition of a notification or an analogous document. The Federal Computer Fraud and Abuse Act address the prospect of filing a legal claim against the use of cookies for promotional messages, which results in the use of cookies as a surveillance tactic with a massive impact on the devices that store the data. Cookies collection and disclosure are required in some regions,[33] but not uniformly as is the case of the GDPR in Europe and all entities that operate with EU citizens' data collected from their online activities. The necessary disclosure must also include information on how the operator reacts to "do not track" notifications or other equivalent techniques. Personal data security is a general requirement for entities planning or dealing with e-commerce, and the shift in approach reflects not only the necessity but also the relationship between the needs of growing consumer faith and legal requirements. By this, we mean that the processes and obligations are important not only in terms of litigation but also of good practices and reputation. According to the FTC, private data security precautions must be a "reasonable", factoring criteria; criteria such as the amount and importance of data stored by the business, the organization and scope of its operations, and the cost of resources needed to manage risks. Certain federal laws as well as certain state laws prescribe a responsibility to ensure the safety of personal data and information gained from them. As we mentioned, there is no statutory obligation to officially communicate data breaches and violations to the relevant authority. There are separate rules in a specific sector law on a federal level, like the health sector[34] and financial sector. Under specific law requirements in several states, it is required data breaches are to

[32] C.J. Hoofnagle, B. van de Sloot, F.Z. Borgesius, *The European Union General Data Protection Regulation: What It Is and What It Means*, "Information & Communications Technology Law" 2019, vol. 29(1), pp. 65–98.

[33] Cookie disclosures are required in at least two jurisdictions, *California* and *Delaware*. See G.E. Kennedy, L.S.P. Prabhu, *Data Privacy Law: A Practical Guide*, Kindle Edition, 2020, pp. 15–36.

[34] Health Insurance Portability and Accountability Act of 1996 (HIPAA) is the legislative act at the federal level that mandated the development of national standards to prevent sensitive healthcare data of being revealed without the patient's prior consent.

be reported to a governmental agency or the Attorney General. Based on state laws, the amount of information that is required differs according to the specifications of the regulation, but usually contains a summary of the incidence, as well as the people affected, types or categories revealed data, event timing and identification, methods of preventing future incidents, records of notifications issued to affected parties and any services provided to them.

4. Legal regulations on data protection regarding e-commerce in the Republic of North Macedonia

From a Balkan perspective, the personal data protection regime in the Republic of North Macedonia is legalized for the first time by the adoption of a special Law on Personal Data Protection in 2005,[35] the provisions of which lay the foundations of the right to personal data protection in the Republic of Macedonia. The relevant legal framework for the protection of personal data in the Republic of North Macedonia is supplemented by the ratification of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, as well as the Law on Ratification of the Additional Protocol to the Convention (Official Gazette of Republic no. 103/08), about supervisory bodies and cross-border data transmission With the adoption of the Law on Personal Data Protection, a new concept was established, implying the inclusion of the right to privacy in the Republic of Macedonia, protection of citizens' right to information confidentiality of the citizens. The Law on Personal Data Protection was adopted in 2005 and gave citizens the authority to choose which of their data will be made public and which will not. The new Law on Personal Data Protection[36] went into effect in February of 2020, with a transitional period of 18 months after its enactment. So, with the implementation of the new LPDP, there will be greater alignment with European regulations in the field of personal data protection, particularly the GDPR. The LPDP regulates the right to autonomy privacy and security as a fundamental freedom and right of natural persons and clearly defines the scope of personal data protection, i.e., it expressly states that personal data only refer to natural persons. The law applies to all cases of fully or partially automated personal data processing. The authors have structured several significant novelties pursuing the implementation of the new LPDP. The following issues should be highlighted:

[35] Law on Personal Data Protection (Official Gazette of the Republic of Macedonia 2005, no. 7), https://www.slvesnik.com.mk/Issues/9E33C7CB857DDD40B0D7CD580F53F59C.pdf (access: 15.12.2021).

[36] Law on Personal Data Protection (Official Gazette of the Republic of North Macedonia 2020, no. 42), https://www.slvesnik.com.mk/Issues/606043d405e847ee92c7eaed5c8bd389.pdf (access: 19.12.2021), hereinafter: LPDP.

- the introduction of new principles on data protection,
- a more comprehensive classification of the personal data, profiling and pseudonymization, consent, special groups of personal data, genetic data, biometric data, and data related to human health,
- technical and integrated processing of personal data (data protection by design and by default),
- impact assessment of personal data protection, and
- the certification and code of conduct are introduced.

The new LPDP promotes the so-called accountability principle, which requires controllers to be able to prove the fulfillment of law obligations.

In terms of the application of measures both technical and operational, a novel feature is that they are now designed and implemented under several criteria that take into account the nature, scope, circumstances, and objectives of the processing, along with adding to the threats of increasing incidence and seriousness to natural persons' rights. Furthermore, they are designed and implemented following the most recent technological advances (state-of-the-art technology), which necessitates that technical and organizational measures be reviewed and updated regularly, in a manner that is appropriate to the time in which they are designed and implemented.

Technological and integrated processing of personal data (data protection by design and by default) is designed based on controller responsibilities, which may be divided into two parts: first, at the time of defining the methods of processing as well as at the time of assessment, to apply measures and procedures that will enable successful understanding and application of data protection and privacy; second, by applying all needed precautions during the process that satisfy the criteria for legitimate data protection and to defend the interests of the law subjects. Regarding the Data Protection Impact Assessment, which is also a significant novelty, the LPDP requires an impact assessment whenever new technologies are used for some sort of personal data processing and it is possible to put citizens' information privacy at risk, accounting for the fact of various characteristics, applicability, circumstances, and treatment objectives. As a result, the LPDP requires that the assessment be carried out in the case of a systematic and comprehensive assessment of private issues concerning natural persons that are based on automatic processing, including subject identification. The LPDP strengthens the position of the Data Protection Officer and introduces an obligation for the controllers to always appoint a personal data protection officer when:

- the processing is performed by the state authorities,
- the controller's or processor's basic activities correspond to performing data analysis that, due to their type, the scope of processing, or objectives, necessitate extensive systematical monitoring of personal data subjects; or
- the controller's or processor's basic activities come in the form of extensive processing of specific types of data or personal data related to criminal

records. From a sanctioning standpoint, the LPDP increases the number of misdemeanors by 2% for category misdemeanors and 4% for category II misdemeanors of the controller's total annual income.[37] According to the stated changes in the Republic of North Macedonia's legislation on personal data protection, entities planning or dealing with e-commerce must make the necessary changes, i.e., harmonize their work with the new LPDP. In practice, this implies that before committing to the processing of personal data, all entities planning or dealing with e-commerce must be aware of the specific circumstances and components of risk processing, and must develop adequate procedures and policies on that basis. Also, they need to perform a catalog identification of all collections of personal data in terms of processing reasons; the categories of natural persons and the IRL data; the transfer of personal data to other countries; the envisaged deadlines for storage, i.e., deletion of the diverse types of data.

Additionally, if the requirements of the LPDP are met, and if the risk analysis determines it as necessary, the entities which are planning or dealing with e-commerce need to mandate a Data Protection Officer. The LPDP has established in a listed manner the minimal obligations of the Data Protection Officer, which primarily rely on the obligation "to inform and advise the controller or processor and the employees who perform processing by their obligations; to monitor the compliance with the special law and other relevant laws related to personal data protection in the Republic of North Macedonia",[38] as well as the policies of the Data Protection Officer; to assist with the impact evaluation of personal data protection as needed, as well as to monitor the assessment's execution; to collaborate with the Agency and serve as a primary contact for the Agency on problems, especially consulting, as well as to advise on all other issues as needed.

Regarding the establishment of processes for informing natural persons (personal data subjects) about their rights and how they are realized, such as the right to information, to access, to verify the accuracy and relevance of information, right of erasure, control, and limitation of processing, data portability, and objection. By this entities planning or dealing with e-commerce must publish a clear and concise Privacy Policy and Cookie Policy that contains all of the information.

[37] According to Article 110 of the LPDP.

[38] According to Articles 41, 42 and 43 of the LPDP.

5. Legal regulations on data protection regarding e-commerce in Albania

Albania's e-commerce sector has shown the same effects and benefits as in other countries, boosting various sectors of the economy ranging from retail trade to services. The general population's increased use of information and communication technology has objectively facilitated electronic transactions, particularly during the pandemic, while also increasing demand for more efficient privacy protection measures.[39] Based on the Albanian Constitution,[40] the control and security of private data in Albania are currently governed by the Law on Protection of Personal Data no. 9877 of 10 March 2008, amended with Law no. 120/2014 which was enacted as a necessity during a period when Albania needed to achieve the consistency and adaptability standards of data protection comparable to the European Union policies. Even though it was enacted before the GDPR entered into force, it is considered in compliance with it because it contains many provisions that are transported from the European Directive 95/46 foreseen in the Regulation. Furthermore, the law releases the main regulatory areas of digital privacy and includes specific rules expanding the range of data subjects' rights while strengthening measures to ensure them, giving citizens greater control over their data, providing additional obligations for controllers/processors, which are integrated into legislation for the first time, and influencing the effectiveness of information security in the process of managing private data. Primarily, criminal law enforcement authorities create laws on the handling of personal data, which are regarded as lexis in this sector. Second, reviewing administrative sanctions demonstrated the importance of protecting personal data and enforcing legal obligations. Third, strengthening the competencies of the Information and Data Protection Commissioner, including for the first time the inspective and correctional functions in the interest of institutional independence. We consider that the special law, which incorporates and develops the main principles and standards of individual data control, and the primary authority's role, establishes a comprehensive regulatory and institutional framework for data privacy. Moreover, a thorough examination of the law reveals that Albania follows the EU model by allowing personal data transfers to other countries that provide a sufficient level of protection based on contractual obligations, allowing businesses to outsource some of their data management needs.

---

[39] J. van de Hoven, M. Blaauw, W. Pieters, M. Warnier, *Privacy and Information Technology*, [in:] *Stanford Encyclopedia of Philosophy*, 2020, https://plato.stanford.edu/entries/it-privacy (access: 20.12.2021).

[40] Article 35 of the Constitution addresses the importance of protection of personal data and highlights the prerequisites before the data processing takes place with focus on the users' permission as the primary safeguard. See *Responsible Innovation 1: Innovative Solutions for Global Issues*, eds. J. van de Hoven, N. Doorn, T. Swierstra, B.-J. Koops, H. Romijn, http://ndl.ethernet.edu.et/bitstream/123456789/18722/1/112..Jeroen%20van%20den%20Hoven.pdf (accesss: 10.8.2022).

The Law on Data Protection defines concretely the categories of personal data, particularly sensitive ones, as valuable assets for a person. The law clarifies one of the main aspects of legitimately collecting and managing personal data; the subjective rights, including the ability to retrieve one's private information, request its amendment or demand its deletion, responding in this way to the concerns for the protection of Albanians in e-commerce activities. There is secondary legislation[41] in addition to the Law that applies to data protection, addressing the security measures to be implemented in specific sectors' activities completing the legislative framework. In any case, we consider that the most clarity and consistency of data safeguard is ensured by a law, which complies with the GDPR requirements. We analyzed the entire framework to understand how businesses embed security measures and predefine their methodological approach into their practices in order to be more explicit about the security ensured in e-commerce.

To begin, according to legal and constitutional principles, Albanian citizens are equal before the law, and their data is protected at the same level. In this regard, para. 2 of Article 4 of the Law has foreseen the frame of relevant institutions, among which setting up the scope of law on who collects and processes the statistics of Albanian citizens. The law applies to controllers founded under Albanian jurisdiction, its diplomatic missions or consular offices, and controllers who aren't founded in Albania, utilizing at least one device to perform operations in its territory. At first sight, the main categories of controllers are covered, as the territoriality of the legal status of controllers or their processing devices is the referencing criteria of Albanian law. But, considering the fact that GDPR extends and includes the data management of entities inside the EU, regardless of whether the activity occurs in the Union or not, it seems that foreign controllers who take care of citizen facts without the usage of any tool which is located to perform inside the Republic of Albania are not blanketed.

Given the GDPR's extraterritorial applicability,[42] its extraterritoriality with regard to controllers who do not operate in Albania but deal with data of Albanians and other residents in her territory may need to be re-examined as well. This program of the rules for the processing of data of Albanian residents should indeed be evaluated in the context of technologies that introduce new possibilities and without legal obstacles for data processing to function everywhere, irrespective of presence in a specified jurisdiction. The reform is important to secure all citizens without risking their rights based on whether the controller is established in Albania or beyond its borders, which might breach Albanians' data with the same consequence.

[41] See Information and Data Protection Commissioner in Albania, https://www.idp.al/category/activities-of-the-commissioners-office/?lang=en (access: 13.10.2021).

[42] According to Article 3 of the GDPR.

According to M. Goddard, "the GDPR represents the strengthening, expansion, and accountability of EU data protection laws".[43] In this regard, the authors also support the opinion that data is a larger notion than personally identifiable information, which makes accountability for the lawfulness and sufficiency level of data processing more significant. The revision of the territorial extent of the legislation should be seen as an essential question of conformity with EU rules and improved protection of citizens' data, particularly in e-commerce. The second aspect examined in Albanian law is the recognized legitimate basis for the lawful handling of personal data, with consent being highlighted as an important legitimate justification for their processing in line with the GDPR. The lawfulness of data processing in Albania is based on the same grounds as those mentioned in Article 6 of the GDPR.[44] As mentioned earlier in the paper, the issue of granting consent on data collection and management, represents the proclamation of the prerequisite of free will, which implies approval to the private data processing, via a statement or by utilizing a direct intervention based on self-responsibility.[45] The regulation provides limitations and obligations on the validity of consent, as well as the right of data subjects to withdraw consent at any time, which clarifies the requirements on how consent is obtained, used, and changed over time. Albanian law[46] refers to consent as a legal criterion and is analogous to the GDPR provisions, including the controller's duties in obtaining the data subject's consent and informing them of their rights. Personal data processing is permitted in the framework of crime prevention and prosecution activities, according to paras 2 and 3 of Article 6 of the Law. As a result, in circumstances of offenses affecting public security and other

[43] M. Goddard, *The EU General Data Protection Regulation (GDPR): European Regulation that Has a Global Impact*, "International Journal of Market Research" 2017, vol. 59(6), pp. 703–705.

[44] Article 6 of the GDPR lists specific cases or justifications that, when at least one of them is met, render the processing lawful, such as: the data subject's consent for one or more specific purposes; the need to perform out a contract related to the data subject's interests; the controller's compliance with a legal obligation; the protection of the data subject's or another natural person's vital interests; the performance of a task carried out in the public interest or by an authority having public interest in the processing, or in case of existence other legitimate interests that are overridden by other protected by law interests or fundamental rights and freedoms, in particular where the data subject is a child.

[45] According to Article 4 (11) of the GDPR.

[46] Article 6 of the Law on Protection of Personal Data no. 9887 (Data Protection Law) (Official Gazette of the Republic of Albania no. 44, 1.4.2008) states that for processing personal data is required one of the following legal criteria: personal data subject has given his consent; processing is necessary for the performance of a contract to which the data subject is party or in order to negotiate or amend a draft/contract at the request of the data subject; to protect the vital interests of the data subject; to comply with a legal obligation of the controller; for the performance of a legal task of public interest or in exercise of powers of the controller or of a third party to whom the data are disclosed; processing is necessary for the protection of the legitimate rights and interests of the controller, the recipient or any other interested party. Explicitly is emphasized that "in any case, processing of personal data cannot be in clear contradiction with the data subject right to protection of personal life and privacy".

violations of law, safety, and border security, official authorities must perform their duties lawfully. If the controller or processor handles personal data for the aim of promoting commercial products, the data must be drawn from any publicly available listed data. The last hypothesis concerns the lawful processing of publicly available data even without the individual's agreement, even though the GDPR requires sought consent regardless of whether the data is private or public. This is risqué and an example of how the law does not conform with EU laws; moreover, data processing in e-commerce is vulnerable if it has been handled without authorization because it is publicly accessible. Even though Albania is in the process of implementing programs of remedial activities to address identified compliance gaps, some of them are evident and in direct correlation with some of the most discussed novelties of the GDPR. Concerns are heightened by the widespread adoption of e-government services in Albania, and according to the Annual Report of Albanian Data Protection Commissioner for 2021,[47] the focus is on monitoring public bodies' implementation of "transparent programs" on the use of personal data and overseeing compliance by individual enterprises, either through investigations of complaints received from individuals or by their ex officio inspections. Consultations with stakeholders and experts, however, show that individual and small company awareness of Albania's data protection regulations remains insufficient, restricting citizens' faith in the country's e-commerce and other digital enterprises. Updating privacy regulations in order to seek EU adequacy ruling is regarded as a way of increasing trust in Albania's emerging e-commerce sector.

CONCLUSIONS

Based on a thorough analysis of the legal frameworks in force in the United States and the European Union for protecting the data and information of online customers, it is clear that this is a sensitive issue that is covered by specific legal requirements. When the territoriality effects of measures to address consumer requests for the protection of their data transcend beyond the country in which they are located, the research findings have been extended to two developing Balkan countries to show the degree of compliance with the regimes that have been examined.

Referring to the American system's sources of law at the state and federal levels, there is a collection of federal laws that do not offer a distinctive method of data protection, and therefore to safeguard various forms of data autonomously. Moreover, the sectoral model firmly applied for the data protection in the e-commerce area is considered very specific and by this designated to answer the concrete

[47] See Annual Report of Albanian Data Protection Commissioner, 2021, https://www.idp.al/wp-content/uploads/2016/10/RAPORTI-VJETOR-2021.pdf (access: 7.10.2021).

concerns, but without delegating the supervision to the public authority. In Europe on the other hand, the GDPR established a system of inclusion in specific data protection in commercial activities by regulating the data controllers' obligations framework and demanding the execution of the concept of the appropriateness of protective measures.

In this regard, the American and European data protection regimes intersect at the point of data protection in selected states, such as California, Colorado, and Virginia, which have established particular state-level legislation to secure customer data. Comparable safeguards to those imposed by the GDPR are also established in other State Privacy Acts in America and Federal Trade Commission agreements with corporate entities, although with a weaker approach and fewer restrictive forms.

In Europe, the GDPR has increased the goal of properly protecting personal data by responding with appropriate safeguards and reversing the one-size-fits-all mindset. So, the GDPR has increased legal clarity and also the legal certainty by avoiding fragmentation among EU members and strengthening the pre-existing obligations. The authors deem that the consequence of a tougher regulatory framework regarding data protection of EU citizens indicates a larger scope of responsibilities for controllers, which will certainly cause more financial implications, as well as spending more human resources.

Although the study results show that both legal regimes are similar to the point of some key principles ensuring data massing and managing since the US legal system does not offer unified protection, the EU regulation is the strictest. However, the legal regulation of both regimes tends is to guarantee e-commerce users and to ensure desired outcomes such as fully implementing data minimization, better transparency, communication with data users, and avoidance of discriminated access in cases of unapproved data collection.

According to the legal framework evaluation findings, the GDPR intends to give valuable information questions in advance and before the risqué occurs, with the goal of not only ensuring, but also avoiding misuse of data usage and clarifying all parties' obligations. The implementation of the GDPR will reveal whether a higher level of protection of individuals' rights is truly provided, or if it is simply additional bureaucracy of performed personal data protection processes.

Also both developing countries examined in this study, the Republic of North Macedonia and Albania, demonstrated the GDPR compliance. They have a comparable improvement in consistency and responsiveness of personal data protection when compared to GDPR's assured approach to data misuse prevention and protection. The Republic of North Macedonia has addressed e-commerce by putting in place the required operational and technical controls under the adopted special law of 2020, taking into account the most current technological breakthroughs, operating expenses, the type, scope, context, and purposes of the processing, and also various threats to individual rights that vary in probability and severity. Under the GDPR,

the new data protection law now covers a wider geographic area and applies to all businesses that handle the personal data of people living in North Macedonia, including foreign businesses that operate there and provide merchandise or monitor people's behavior. As a result, a large number of companies that were previously exempt from the old personal data protection legislation are now governed by the new data protection law, particularly online enterprises that handle the personal data of people in North Macedonia. Such internet operating enterprises must appoint a local data protection representative in North Macedonia, unless the processing of personal data is incidental, does not include the processing of special categories of data on a wide scale and is unlikely to result in a privacy breach.

Based on the findings about Albania, even though the Data Protection Law was enacted before the GDPR entered into force, it is considered in compliance with it because it contains many provisions that are derived from the European Directive 95/46 that's also incorporated into the GDPR. We conclude that the special law establishes a comprehensive legislative and institutional framework for data privacy by including and developing the key concepts and norms of individual data management, including the function of the state authority. The Law enacts secondary laws to address security measures to be adopted in various sectors' activities, thus completing the legislative framework.

As a result, the Law ensures the most clarity and consistency of data safeguard, which conforms with GDPR criteria. Second, the Law provides detailed definitions for several categories of personal data, including sensitive data. It specifies one of the key elements of lawfully collecting and managing personal data, namely the subjective rights, which include the capacity to access and demand the deletion of one's personal information in response to Albanians' protection concerns in online transactions. Third, it is concluded that the extraterritorial applicability of the GDPR may need Albanian law to be re-examined. Last but not least, Albania is one of the examples of legislation that has a thorough data protection law, which refers to consent as a legal criterion analogous to the GDPR provisions but also faces issues with the lawful processing of publicly available data without the individual's consent, although the GDPR requires consent regardless of whether the data is private or public.

In conclusion, the presented advantages and requirements for handling personal data in Albania and North Macedonia are in line with the European integration processes of their countries.

Concerning data collection in e-commerce activities, the authors see the need for appropriate requirements to be defined based on the characteristics of the information that is controlled, its sensitivity, the time that must be controlled, and the level of risk that each of the controllers faces.

REFERENCES

Literature

Azzi A., *The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation*, 2018, vol. 9, "Journal of Intellectual Property, Information Technology and E-Commerce Law" 2018, vol. 9(2).

Baldwin R., Cave M., Lodge M., *Understanding Regulation: Theory, Strategy, and Practice*, Cambridge 2011, **DOI: https://doi.org/10.1093/acprof:osobl/9780199576081.001.0001**.

Bhatti A., Akra H., Basit H.M., Khan A.U., Raza S.M., Naqvi M.B., *E-commerce Trends during COVID-19 Pandemic*, "International Journal of Future Generation Communication and Networking" 2020, vol. 13(2).

Boyne S.M., *Data Protection in the United States*, "American Journal of Comparative Law" 2018, vol. 66(1), **DOI: https://doi.org/10.1093/ajcl/avy016**.

Feiler N., Forgó F.L., Weigl N. (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, New York 2018.

Goddard M., *The EU General Data Protection Regulation (GDPR): European Regulation that Has a Global Impact*, "International Journal of Market Research" 2017, vol. 59(6), **DOI: https://doi.org/10.2501/IJMR-2017-050**.

Gömann R.M., *The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement*, "Common Market Law Review" 2017, vol. 54(2), **DOI: https://doi.org/10.54648/COLA2017035**.

Hintze M., El Emam K., *Comparing the Benefits of Pseudonymisation and Anonymisation under the GDPR*, "Journal of Data Protection & Privacy" 2018, vol. 2(2).

Hoofnagle C.J., Sloot B., Borgesius F.Z., *The European Union General Data Protection Regulation: What It Is and What It Means*, "Information & Communications Technology Law" 2019, vol. 29(1), **DOI: https://doi.org/10.1080/13600834.2019.1573501**.

Jamal K., Maier M., Sunder S., *Enforced Standards versus Volution by General Acceptance: A Comparative Study of e-Commerce Privacy Disclosure and Practice in the United States and the United Kingdom*, "Journal of Accounting Research" 2005, vol. 41(1), **DOI: https://doi.org/10.1111/j.1475-679x.2004.00163.x**.

Jang-Jaccard J., Nepal S., *A Survey of Emerging Threats in Cybersecurity*, "Journal of Computer and System Sciences" 2014, vol. 80(5), **DOI: https://doi.org/10.1016/j.jcss.2014.02.005**.

Kennedy G.E., Prabhu L.S.P., *Data Privacy Law: A Practical Guide*, Kindle Edition, 2020.

Ryngaert C., Taylor M., *The GDPR as Global Data Protection Regulation?*, "AJIL Unbound" 2019, vol. 114, **DOI: https://doi.org/10.1017/aju.2019.80**.

Sarathy R., Robertson C., *Strategic and Ethical Considerations in Managing Digital Privacy*, "Journal of Business Ethics" 2003, vol. 46(2), **DOI: https://doi.org/10.1023/A:1025001627419**.

Udo G.J., *Privacy and Security Concerns as Major Barriers for e-Commerce: A Survey Study*, "Information Management & Computer Security" 2001, vol. 9(4), **DOI: https://doi.org/10.1108/EUM0000000005808**.

Voigt P., Bussche A., *The EU General Data Protection Regulation (GDPR): A Practical Guide*, "Axel von dem Bussche Taylor Wessing" 2020, vol. 13(2).

Online sources

Annual Report of Albanian Data Protection Commissioner, 2021, https://www.idp.al/wp-content/uploads/2016/10/RAPORTI-VJETOR-2021.pdf (access: 7.10.2021).

Chevalier S., *Retail e-Commerce Sales Worldwide from 2014 to 2025*, 4.2.2022, https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales (access: 20.5.2021).

Data Protection Laws and Regulations 2021–2022: International Comparative Legal Guide, Global Legal Group 2021, https://iclg.com/practice-areas/data-protection-laws-and-regulations (access:18.11.2021).

Hoven J. van de, Blaauw M., Pieters W., Warnier M., *Privacy and Information Technology*, [in:] *Stanford Encyclopedia of Philosophy*, 2020, https://plato.stanford.edu/entries/it-privacy (access: 20.12.2021).

Hoven J. van de, Doorn N., Swierstra T., Koops B.-J., Romijn H. (eds.), *Responsible Innovation 1: Innovative Solutions for Global Issues*, http://ndl.ethernet.edu.et/bitstream/123456789/18722/1/112.. Jeroen%20van%20den%20Hoven.pdf (accesss: 10.8.2022).

Information and Data Protection Commissioner in Albania, https://www.idp.al/category/activities-of-the-commissioners-office/?lang=en (access: 13.10.2021).

International Classification of Functioning, Disability, and Health, Geneva 2001, http://whqlibdoc.who.int/publications/2001/9241545429.pdf (access: 10.7.2021).

Maria T., *Data Protection / Data Privacy*, [in:] *Elgar Encyclopaedia of Human Rights*, https://ssrn.com/abstract=3859440 (access: 10.2.2022).

Nuredini B., Paunkoska Dodevska V., *Legal Aspects of Electronic Contracts*, UBT Conference, October 2020, https://www.researchgate.net/publication/353515427_Legal_aspects_of_electronic_contracts (access: 20.3.2022).

Wolford B., *What is GDPR, the EU's New Data Protection Law?*, https://gdpr.eu/what-is-gdpr (access: 10.2.2022).

Legal acts

Fair and Accurate Credit Transactions Act, http://uscode.house.gov/view.xhtml (access: 7.9.2021).

Federal Statute on the Telephone Consumer Protection Act, 47 U.S.C. § 22, https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/8/viii-5-1.pdf (access: 7.9.2021).

Gramm-Leach-Bliley Act, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act (access: 7.9.2021).

Health Insurance Portability and Accountability Act of 1996 (HIPAA), http://www.legalarchiver.org/hipaa.htm (access: 7.9.2021).

Law on Protection of Personal Data no. 9887 (Data Protection Law) (Official Gazette of the Republic of Albania no. 44, 1.4.2008).

Law on Personal Data Protection (Official Gazette of the Republic of Macedonia 2005, no. 7).

Law on Personal Data Protection (Official Gazette of the Republic of North Macedonia 2020, no. 42).

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) (OJ L 119/1, 4.5.2016).

Case law

Judgement of the CJEU of 13 May 2014 in case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*.

ABSTRAKT

Zalety elektronicznych środków komunikacji w sektorze e-commerce oraz szybkiej wymiany informacji nadal przynoszą olbrzymie korzyści, ale kosztem ochrony prywatności i powstawania luk prawnych. W każdym systemie prawnym – czy to unijnym, czy to amerykańskim – prywatność jest definiowana inaczej; pomimo tego, że waga prywatności jest szeroko akceptowana, brak jest jednolitej definicji tego pojęcia w środowisku naukowym. Trudności w przenoszeniu danych osobowych pomiędzy Unią Europejską a Stanami Zjednoczonymi znów wyszły na pierwszy plan pośród najważniejszych kwestii związanych z prywatnością i ochroną danych w poszczególnych krajach. Rozporządzenie o ochronie danych osobowych (RODO) postawiło ochronę danych na najwyższym poziomie działalności przedsiębiorstw poprzez wymagania nałożone na każdą organizację zbierającą, przetwarzającą, zarządzającą lub przechowującą informacje o europejskich obywatelach, wymuszając surowsze standardy i dając użytkownikom większą kontrolę nad swoimi danymi. Nowe rozporządzenie oddziałuje na przedsiębiorców i użytkowników w całej Europie. Celem opracowania jest porównanie poziomu ochrony i bezpieczeństwa zapewnianego użytkownikom e-commerce w Unii Europejskiej, Stanach Zjednoczonych Ameryki, Republice Macedonii Północnej i Albanii. Ponadto zbadano korelację pomiędzy obowiązkami a skutkami RODO w celu stwierdzenia, czy zapewni ono wyższy poziom ochrony praw jednostek czy też raczej przede wszystkim wywoła zbiurokratyzowanie procesów ochrony danych osobowych prowadzonych w ramach czynności e-commerce.

Słowa kluczowe: ochrona danych; e-commerce; RODO; system prawny; Republika Macedonii Północnej; Albania