Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 15th International Scientific and Practical Conference. Volume IV, 317-321

The Applicability of the EU Data Protection Rules in the Area of National Security in the Republic of Bulgaria

Martin Zahariev
Faculty of Information Sciences, National Security Department
University of Library Studies and Information Technologies
Sofia, Bulgaria
m.zahariev@unibit.bg

***Abstract*. The key acts shaping the EU data protection legal regime – the General Data Protection Regulation 2016/679 (GDPR) and the Law Enforcement Directive 2016/680 (LED) – explicitly stipulate that they do not apply in areas which fall outside the scope of EU law, such as activities concerning national security (recital 16 and 14 respectively). At the same time, Bulgarian legislation gives a very broad definition of "national security" as a dynamic state of society and the state in which values such as the territorial integrity, sovereignty and the constitutionally established order of the country are protected, and where the democratic functioning of institutions and the fundamental rights and freedoms of citizens are guaranteed. As a result, a variety of competent authorities contribute daily to the protection of these values such as the leading authorities from the legislative and executive power, the president, the law enforcement agencies, the courts, the various regulators, etc. A lot of the data processing activities of these authorities conducted while exercising their powers actually do fall into the scope of the GDPR and the LED and at the same time serve the protection of the national security. To that end, a strict dividing line between national security and other activities of these bodies often cannot be drawn. The present paper argues that the GDPR and the LED should apply to a lot of the activities contributing to the protection of national security which will also be an additional safeguard for the fundamental rights and interests of the individuals and increase the accountability of the competent authorities.**

Keywords: GDPR, LED, national security, data protection, competent authorities.

I. INTRODUCTION

The present study aims to explore the notion of national security from the perspective of the legislation of Republic of Bulgaria – a Member State of the EU – in the context of personal data processing activities. The goal of this analysis is to prove that the concept of national security is so broad that a strict dividing line between national security and other activities of the competent authorities and bodies whose powers serve the protection of the national security often cannot be drawn. Ultimately, the present paper argues that the EU laws on data protection should actually apply to a lot of the activities contributing to the protection of national security which will also be an additional safeguard for the fundamental rights and interests of the individuals and increase the accountability of the competent authorities.

The background of the researched problem can be summarized as follows: the key acts shaping the EU data protection legal landscape – the General Data Protection Regulation 2016/679 (GDPR) [1] and the Law Enforcement Directive 2016/680 (LED) [2] – explicitly stipulate that they do *not* apply in areas which fall outside the scope of EU law, such as activities concerning national security (recital 16 and 14 respectively). This is also reaffirmed by the Treaty on the European Union (TEU) [3] which stipulates that national security remains the sole responsibility of each Member State (Art. 4(2) of the TEU). At the same time, EU law lacks a specific definition for "national security", although the Court of Justice of the EU (CJEU) in its practice has shed some light on this concept. In particular, in its Judgement on Joined Cases C 511/18, C 512/18 and Case C 520/18 CJEU has interpreted the cited Art. 4(2) of the TEU, highlighting that the said responsibility of the Member States to ensure their national security *"corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly*

Print ISSN 1691-5402
Online ISSN 2256-070X
https://doi.org/10.17770/etr2024vol4.8234

threatening society, the population or the State itself, such as terrorist activities" [4]. Evident from the above, what constitutes national security and which activities fall or do not fall therein should be defined in the national legislation of each Member State. In any case, these activities should meet the following cumulative criteria (i) serve the essential state functions and the fundamental interests of the society and (ii) prevent and sanction activities threatening fundamental values such as constitutional, political, economic or social structures, the society, the population or the state itself. As the focus of the present study is the Republic of Bulgaria, the next section is devoted to clarifying this concept from Bulgarian legal perspective.

II. METHODOLOGY OF THE STUDY

The results of the present study were obtained after applying scientific methods such as:

- *Documentary method* – consisting in analyzing and synthesizing information about the definition of national security from various documentary sources – e.g. from the primary and secondary EU law, from Bulgarian national legislation and from other publicly available (including online) sources, as well as in the systematization and summarization of this information.
- *Historical method* – this method is used to track the dynamics of the Bulgarian data protection legislation before and after the adoption of the GDPR and the LED and the transposition of the latter in the national legislation and the changes in the legal concept of national security.
- *Comparative analysis* – this method consists of comparing the common and the different between separate phenomena. In this report, this method is necessary to prove that often certain activities of the competent authorities cannot be classified in a straightforward manner whether they fall into one or another data protection regime.
- *Case study* – this method is used to illustrate how certain activities that fall into the EU data protection regime can contribute to protecting national security.
- *De lege ferenda* – this specific scientific method is used in the law science to propose future amendments in the legislation.

III. RESULTS

A. The Concept of National Security under Bulgarian Law

The Bulgarian law contains a definition of "national security" in the Management and Operation of the National Security Protection System Act (MONSPSA) [5] which reads as follows: *"National security is a dynamic state of society and the state, in which the territorial integrity, sovereignty and constitutionally established order of the country are protected, when the democratic functioning of the institutions and the basic rights and freedoms of the citizens are guaranteed, as a result of which the nation preserves and increases its well-being and develops, as well as when the country successfully defends its national interests and realizes its national priorities"* (Art. 4(2)). The Bulgarian legal scholars have emphasized that the term "national security" in the past has been defined in various legal acts such as the Protection of Classified Information Act [6] and the State Agency National Security Act [7] which reveal *"differences in some understandings",* but "*through the law (the MONSPSA – note of the author) a uniform definition of this concept has already been adopted"* [8]. This is also reaffirmed by the Updated Strategy for National Security of the Republic of Bulgaria (the Strategy), which provides that with the adoption of the MONSPSA, *"a uniform legal definition of the concept of national security has been adopted" (para. 6)* [9]. In addition, the Strategy acknowledges that *"the final product and the real meaning of the concept of "national security" is the guarantee of human security and the protection of the freedom and dignity of the citizen, as well as the protection of sovereignty, territorial integrity and the protection of the state border"* (para. 9) [9].

At the same time, various scholars have examined the notion of national security both in general [10], [11], [12] as well as in its different manifestation forms in areas such as (i) the migrant smuggling [13]; (ii) the importance of natural resources for the national security [14]; (iii) the policy of countries neighboring to Bulgaria such as Republic Turkey [15]; (iv) the internal activities of some public bodies and their importance for the national security [16]; (v) the demographic problems [17]; (vi) the possibility of the national security to be considered as part of the overriding mandatory provisions in private international law [18].

These nuances are important, because they outline different directions in which competent authorities by exercising their powers can ultimately contribute to safeguarding the national security.

B. Case Study

The present part is devoted to provision of several practical examples of activities both falling into the scope of the EU data protection laws and protecting national security:

Example: A foreign national – e.g. an undercover agent – is instructed by his government to hack key information systems of the Republic of Bulgaria such as the electronic records of the National Revenue Agency and the Ministry of Interior. He should instal malware therein which could result in unlawful extraction, alteration and/or loss of the contained data, including personal data of hundreds of thousands of Bulgarian citizens. The purpose is to create fear and uncertainty among the society, and ultimately – to destabilise the established state order by compromising the activity of important state authorities that are vital for the functioning of the economy and internal security.

In any case, this is an unlawful activity threatening key elements of the national security enlisted above such as (i) the constitutionally established order, (ii) the democratic functioning of the institutions and (iii) the basic rights and freedoms of the citizens. At the same time, *at leas*t the following authorities may need to be involved to

investigate and sanction the matter and to protect the rights of the affected citizens (and by exercising their powers, to conduct related data processing activities):

- Ministry of Interior, the State Agency "National Security" and competent investigators – to investigate the crime;
- State Agency "Technical Operations" – to apply special intelligence means, in case such are needed for revealing the perpetrator(s);
- Prosecutor – to supervise the investigation during the pre-trial phase of the criminal proceedings, to decide when there are sufficient evidence to press charges, which person(s) to be charged and for what type of crime(s), to maintains the charge before the court during the trial phase of the criminal proceedings;
- Criminal court – to consider the case, and if the charges are proven – to impose criminal liability;
- Competent cybersecurity authorities – to the extent that the crime constitutes severe cybersecurity accident;
- Ministry of Electronic Government, Ministry of Defence and Ministry of Finance – to cooperate to the extent they are competent – with the above authorities, as the crime could affect the spheres where they are competent;
- State Commission for Protection of the Information – if classified information is affected;
- The President of the Republic, the Council of Ministers and the National Assembly – as key state authorities, may need to take appropriate actions to ensure the stability of the state and the society – depending on their powers;
- Commission for Personal Data Protection – where the affected citizens may file complaints to seek protection of their data protection rights and which – as data protection supervisory authority – should be competent to evaluate the data protection implications of the crime, as it constitutes a data breach under the GDPR (Art, 4, item 12 and Art. 33-34) and the LED (Art. 3, item 11 and Art. 30-31);
- Administrative Courts – where the affected citizens may file claims for monetary compensation of the damages suffered by the data breach.

C. Key Takeaways from the Case Study

In the light of the case study, two possible approaches exist when dealing with data protection in the context of national security:

A *formalistic (restrictive) approach* which automatically excludes any activity related to national security from the scope of the data protection rules. This approach is supported by the quoted provisions of the TEU, the GDPR and the LED. Also, Bulgarian Personal Data Protection Act (PDPA) contains the restrictive rule that it does *not* apply to the processing of personal data for the purposes of the country's defense and national security, *unless* a special law provides otherwise (Art. 1(5)) [19].

A *non-formalistic (realistic) approach* – a more balanced approach which aims to acknowledge that the notion of national security and the related activities are not black and white. This approach demonstrates that variety of data processing activities conducted by the competent state authorities when exercising their powers contribute on daily basis to the protection of national security and that the latter should not be limited solely to intelligence and counterintelligence activities. Of course, in the last two scenarios, the data protection rules shall apply with numerous and reasonable limitations. But it would be contrary to sense and the spirit of both the definition of national security and the EU data protection laws to generally and indiscriminately deny the application of the data protection rules in contexts such as the above presented in the case study. The latter, in particular the GDPR, provide for enhanced data subject's rights (the GDPR extended existing data protection rights and added the new right of data portability [20]) and increased accountability of the data controllers (such as the public authorities). The last requirement according to the legal doctrine is related to the new philosophy of the GDPR and requires proactive approach from the data controllers with regard to the data processing activities [21]. Such rules in any case serve as an additional security for the lawfulness of the competent authorities' activities. Also, if the formalistic approach is followed, this would deny the affected citizens from the possible tools for redress granted by the data protection rules (complaint, damage claim, etc.) which is hardly compatible with the element of national security guaranteeing the basic rights and freedoms of the citizens.

The non-formalistic approach is also supported by several arguments: First, the fact that the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties falls within the scope of EU data protection law, namely the LED. The majority of the activities enlisted in the case study actually can be classified as one or more of the above concepts, so the related data processing should be subject to the rules of the LED. Second, there are other activities that are borderline, i.e. that could simultaneously fall into different data protection regimes or at least where a strict borderline cannot be drawn – examples of such activity is the border control where sometimes it is very difficult to distinguish when a given processing operation related thereto is carried out for the purpose of combating crime and falls under the regime of LED when it is purely administrative by its nature and as such falls under the general regime of GDPR. As some authors have rightly pointed out, this often leads to an excessively broad interpretation of the LED, thereby undermining the application of the GDPR, and they point to border control, migration and asylum issues in many Member States as a specific example [22]. Third, some authors when analyzing the figure of data protection officer (DPO) have emphasized that the data controller does not appoint a DPO for each different processing purpose which means that the controller will be supported by one DPO (alone or with a team) for all processing purposes [23]. This

shows that even if the formalistic approach is followed and certain activities are defined as "strictly" national security-related, at least certain other data protection activities of public authorities with powers ultimately safeguarding the national security (such as the law enforcement agencies, courts, prosecution etc.) would still be subject to the GDPR and the LED.

Finally, it should be noted that recently Bulgarian PDPA has *diminished* the level of protection of individuals, as it reversed its approach towards data processing activities in the context of national security and law enforcement. In the past, before the amendments in PDPA from 2019 were made to align the PDPA with the GDPR and to transpose the LED, the PDPA stated that unless otherwise provided in a special law, the PDPA *also applied* to the processing of personal data for the purposes of: 1. the defense of the country; 2. national security; 3. the protection of public order and the fight against crime; 4. criminal proceedings; 5. the execution of punishments (Art. 1(5) of the PDPA – redaction before February 2019). As explained above, the current version of Art. 1(5) of the PDPA reads quite the opposite – the PDPA does *not* apply in these areas, unless otherwise provided for by specific law.

De lege ferenda it could be recommended that the old wording of the provision before the amendments of February 2019 is reinstated. This will ensure that the competent authorities adhere to the high standards of the GDPR and the LED when processing personal data and will ensure that the citizens (data subjects) whose personal data is processed by the said authorities when exercising their powers enjoy the enhanced level of protection granted by the said acts. This will also be in line with the historical traditions of the local data protection legislation, which, as already mentioned, used to apply to these spheres as well. In addition, as each Member State is solely responsible for its national security (as explained by the TEU and the CJEU), then every Member State is free to determine what data protection standards to apply to the competent authorities is these areas and the decision to subdue them to the rules under the PDPA transposing the LED for data processing in criminal and punishment context (a term introduced by some scholars to encompass the detailed enlisting in LED: prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties [23]) would not violate any EU laws.

Conclusion

In conclusion, the statement that in variety of scenarios a strict borderline between activities safeguarding the national security and the EU data protection laws cannot be made, seems justified. The criminal and punishment activities of the competent authorities when combating crime, the activities of the regulators when handling complaints and signals of the citizens, the activities of the courts when exercising their judicial powers are only minor examples of data processing activities subject to EU laws that contribute to the protection of national security. Ultimately, such an approach would be in line with the rule of law and the aim to ensure an additional protection for the fundamental rights and interests of the individuals and enhanced accountability of the competent authorities.

References

[1] Official Journal of EU, L 119, 4.5.2016, p. 1–88. Available: EUR-lex, https://eur-lex.europa.eu/eli/reg/2016/679/oj [Accessed February 14, 2024].

[2] Official Journal of EU, L 119, 4.5.2016, p. 89–131. Available: EUR-lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680 [Accessed February 14, 2024].

[3] Official Journal of EU, C 202, 07.06.2016, p. 13–46. Available: EUR-lex, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12016ME/TXT [Accessed February 14, 2024].

[4] CJEU, Judgement on Joined Cases C 511/18, C 512/18 and Case C 520/18, para. 135, Available: Curia, https://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1579363 [Accessed February 14, 2024].

[5] Promulgated in State Gazette, Issue 61 of 11.08.2015; last supplemented issue 15 of 22.02.2022 г., in force as of 22.02.2022.

[6] Promulgated in State Gazette, Issue 45 of 30.04.2002; last amended and supplemented issue 84 of 06.10.2023, in force as of 06.10.2023.

[7] Promulgated in State Gazette, Issue 79 of 13.10.2015, in force as of 01.11.2015; last amended issue 84 of 06.10.2023, in force as of 06.10.2023.

[8] P. Bogdanov. Basics of the national security of the USA and the Republic of Bulgaria. Collection Knowledge Society and 21st Century Humanism The 20th International Scientific Conference Sofia, 1st November 2022. Sofia: Za bukvite – O pismeneh, 2022, p. 423–435. ISSN: 2683-0094.

[9] Adopted via a decision of the National Assembly from от 14.03.2018, Promulgated in State Gazette, Issue 26 of 23.03.2018.

[10] E. Manev. Global, Regional and National Secuirty. Sofia: Softtrade, 2012, p. 382-486, ISBN: 978-954-334-141-2.

[11] P. Bogdanov. Comparison of the National Security Systems of the USA and the Republic of Bulgaria. Collection of reports from the National Scientific Conference with international participation, held on April 21, 2023 at the University of Library Studies and Information Technologies "Security and Defense. Current Status, Opportunities and Perspectives", Sofia: Za bukvite – O pismeneh, 2023, p. 72 – 85, ISBN: 978-619-185-593-3.

[12] G. Angelov. Statehood and National Security. Sofia: Military publishing house, 2022, p. 54-74, ISBN: 978-954-509-581-8.

[13] J. Deliversky. Migrants Smuggling as a Threat for the Economic, Social and National Security. Collection of reports from the Sixth National Conference with international participation MHANS, BAS, May 29 and 30, 2017, p. 221-226, ISSN: 1313-8308.

[14] V. Lazarov. National Security Challenges in Relation to Resources. Collection Knowledge Society and 21st Century Humanism The 17th International Scientific Conference Sofia, 1st November 2019. Sofia: Za bukvite – O pismeneh, 2019, p. 625-632, ISSN: 2683-0094.

[15] P. Teodosiev. Turkey's Politics in Regional Conflicts – a Factor for the Threats and Risks to Bulgaria's National Security. Collection of reports from the National Scientific Conference with international participation, held on April 21, 2023 at the University of Library Studies and Information Technologies "Security and Defense. Current Status, Opportunities and Perspectives", Sofia: Za bukvite – O pismeneh, 2023, p. 387 – 396, ISBN: 978-619-185-593-3.

[16] P. Teodosiev. Activity of the "Dossiers Commission" and its Impact on the National Security of the Republic of Bulgaria. Collection Academic Partnerships in the Field of National Security - Shumen: "Konstantin Preslavsky" Univ., Assoc. Sci. and Appl. Research, 2022, p. 137 – 143, ISBN: 978-619-201-571-8.

[17] M. Neykova, I. Prodanova. The Demographic Problem - a Threat to National Security. Juridical Collection of Bourgas Free University, vol. XXIV, 2017, p.11-18, Available: https://www.bfu.bg/uploads/pages/jur_sbornik_20171.pdf [Accessed February 14, 2024], ISSN: 1311-3771.

[18] Ts. Dimitrova. Hardship and Force Majeure in Private Law Relations with an International Element. The Question of Applicable Law. Sofia: Norma Magazine, Issue 1-2/2021, p. 60, ISSN: 1314-5126 (print).

[19] Promulgated in State Gazette, Issue 1 of 04.01.2002, in force as of 01.01.2002; last amended issue 84 of 06.10.2023, in force as of 06.10.2023.

[20] S. Dibble. GDPR For Dummies. Hoboken, New Jersey: John Wiley&Sons, Inc., 2020, p. 32. ISBN: 978-1-119-54609-2.

[21] D. Toshkova-Nikolova and N. Feti, Personal Data Protection. Sofia: IK Trud I Pravo, 2019 p. 101, ISBN: 978-954-608-263-3.

[22] T. Quintel. Data Protection, Migration and Border Control: The GDPR, the Law Enforcement Directive and Beyond. Oxford: Hart Publishing and Bloomsbury Publishing Plc., 2022, p. 110-111, ISBN ePDF: 978-1-50995-965-5.

[23] N. Feti and D. Toshkova-Nikolova, Application of the Personal Data Protection: Methodics, Recommendations and Practical Steps. Sofia: IK Trud I Pravo, 2020 p. 505-506; 484-485, ISBN: 978-954-608-279-4.