Privacy and data protection: Legal aspects in the Republic of Macedonia

MSc Nora Osmani, PhD candidate
Information Technology Law,
Ss. Cyril and Methodius University, Skopje, Republic of Macedonia

Abstract

The purpose of this paper is to present a theoretical assessment of the existing Law on Personal Data Protection in the Republic of Macedonia. The paper aims to analyse whether there is a need for additional legal tools in order to achieve a balance between maintaining data integrity in the digital age and the use of modern technology. The paper discusses the meaning of "information privacy" in the age of big data, cyber threats and the domestic and international response to these issues. Special focus is dedicated to privacy policy enforcement in European Union Law.

Having regard to the development of new technologies, prevailing data protection legislation may no longer be able to provide effective protection for individuals' personal information. Therefore, existing laws should be continuously adapted to respond to new challenges and situations deriving from different online activities and communications.

Keywords: personal data; privacy; digital age; cyber threats; European Union law

Introduction

The advances in information technology in recent years is a fascinating development. On a technological level, our lives have been both greatly improved and simplified by such development. Yet, digital exchange of information has posed new challenges to our identity and privacy. Due to the impossibility of having full control of our personal data in the digital world, privacy and identity have lost their traditional meaning. This suggests that humans are entering into a new phase in the evolution of society. Mass communication via social media has led to the publication of personally sensitive information. Data protection is becoming a major concern to society. The development of technology and the use of the Internet have created countless problems with respect to the protection of personal data and privacy.

Data remain one of the key assets of our "Information Society". Online social networks allow journalists to report and follow events around the world. Data play a key role in assisting governments prevent identity theft and protect public safety. Medical data are used for identification of public health issues and the prevention of human

diseases[1]. Due to the enormous importance of data, the need for the regulation and control of such data has become urgent.

The primary aim of this paper is to provide an analysis of the applicable legal framework for data protection in the Republic of Macedonia and to indicate whether introduction of new data protection regulation is necessary. In the first part of the paper, basic information is provided about the definition of privacy in the age of big data and its evolution from a traditional meaning into a broader concept. Considering that Macedonia is a candidate country for European Union ("EU") accession, this paper also presents the EU approach to protection of personal data. In the second part, the paper addresses the continuing challenges the development of new technology poses to personal privacy and provides certain suggestions and new insights that legislators could profitably take into account, in order to achieve a more effective implementation of the existing legal provisions.

What is information privacy?

The link between personal data on the one hand and privacy on the other has always been difficult to distinguish. In their article "The right to privacy",[2] Samuel Warren and Louis Brandeis define the right to privacy as the "right to be let alone". In this respect, the right to privacy originally was linked with the right to property and other civil rights.[3] However, in the modern era, the right to privacy derives from other entitlements such as the right to a private life. Under article 8 of the European Convention of Human Rights[4] it is stated that everyone has the right to respect for his private and family life, his home and his correspondence. However, this right is not absolute. In some circumstances, public authorities may interfere with this right.[5] In this respect, Kilkelly describes the protection of personal data as of great importance to a person's enjoyment of his private and family life and, therefore, disclosing personal information to the public constitutes an interference with private life.[6] Kilkelly highlights that "the concept of private life is clearly wider than the right to privacy and it concerns a

[1] Consumer privacy bill of rights (2012) Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy. 5. Available at: https://www.whitehouse.gov/sites/default/files/privacy-final.pdf [January 2016]

[2] Samuel, D. W. & Louis, D. B. (1890) 'The Right to Privacy'. *Harvard Law Review*. 4 (5), 193. Available at: http://www.jstor.org/stable/1321160 [Accessed: February 2016].

[3] Warren and Brandeis explain that the scope of the right to life and property was broadened due to respect for one's spiritual nature; therefore, the term "property" has grown to compromise every form of possession, including feelings and intellect. See: Samuel and Brandeis (1980) 193.

[4] See European Convention on Human Rights of 4 November 1950 as amended by Protocols Nos. 11 and 14 supplemented by Protocols Nos. 1, 4, 6, 7, 12 and 13.

[5] See article 8(2) of European Convention of Human Rights.

[6] Kilkelly, U. (2003) The right to respect for private and family life, a guide to the implementation of Article 8 of the European Convention on Human Rights; Human rights handbook No.1, 39. Available at: http://www.echr.coe.int/LibraryDocs/DG2/HRHAND/DG2-EN-HRHAND-01(2003).pdf [Accessed: February 2016].

sphere within which everyone can freely pursue the development and fulfillment of his personality".[7]

Privacy and personal data protection in the Republic of Macedonia

In the jurisdiction of the Republic of Macedonia, the right to privacy, which necessarily subsumes the right to personal data protection, is part of a human's basic and fundamental rights, which are the subject of national and international legal provisions. In the Constitution of the Republic of Macedonia it is stated:

> "The security and privacy of personal information are guaranteed. Citizens are guaranteed protection from any violation of their personal integrity deriving from the registration of personal information through data processing".[8]

The Law on Personal Data Protection ("DP Law")[9] governs personal data protection issues in the Republic of Macedonia. The DP Law defines personal data as

> "any information relating to an identified or identifiable natural entity, where an identifiable entity is an entity whose identity can be especially determined, directly or indirectly, on the basis of his/her personal identification number or on one or a combination of features that are specific to his/her physical, mental, economic, cultural or social identity" (article 2(1)).

According to the law, personal data processing is

> "any operation or a number of operations performed on personal data, automatically or otherwise, which refer to collecting, recording, organising, storing, altering, finding, using, publishing or otherwise making the data available to the public, as well as their archiving, deleting or annulling" (article 2(2)).

The competent authority responsible for supervising the implementation of DP Law and exercising regulatory oversight of the processing of personal data and the protection of such data in the Republic of Macedonia is the Directorate for Personal Data Protection ("DPA"), established in 22 June 2005 as an independent state agency. According to the DPA's annual report[10], during 2010 to 2014, in the Republic of Macedonia, 1715 complaints were registered regarding personal data and privacy violations (depicted in Figure 1). During 2014, 371 complaints were received by the DPA, of which 331 were from natural persons, 36 from legal entities and 4 from anonymous applicants. Of the total number of requests, 54% or 202 complaints were related to violations of personal data on social media (see Figure 2). Of this sub-set, 130 people required

[7] Ibid. 11.

[8] See article 18 of the Constitution of the Republic of Macedonia of 17 November 1991, as amended on April 2011.

[9] 'Official Gazette of the Republic of Macedonia', no. 7/05, 103/08, 124/08, 124/10, 135/11, 43/14 and 153/15.

[10] Annual report of Directorate for Personal Data Protection, 2014, 33-34. Available at: http://dzlp.mk/sites/default/files/u1002/MK.pdf [Accessed: February 2016].

deletion of fake Facebook accounts, 12 requested deletion of minors' fake profiles and 47 sought redress for password or username hacking. Another 10 requests were for the removal of certain content from Facebook and a further 3 requests related do the erasure of certain content from other social media.

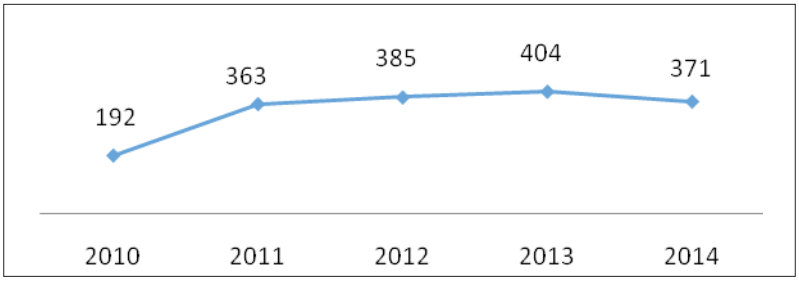

Figure 1. Number of complaints during 2010-2014

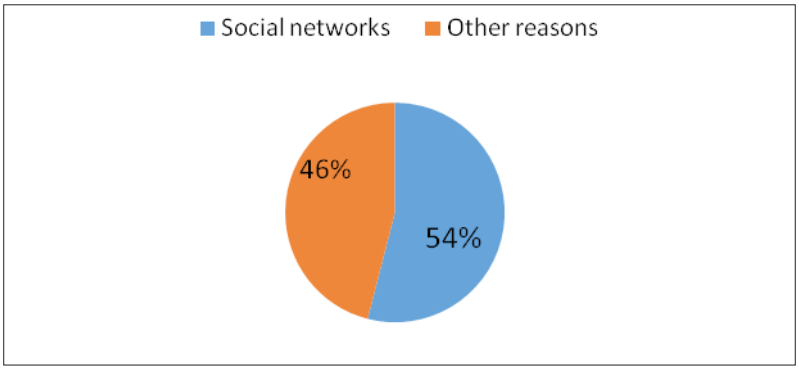

Figure 2. Complaints by percentages

The possibilities for infringement of privacy and misuse of personal data are enormous in a world where everyone can easily access information by use of digital tools; yet most of the complaints submitted to the DPA were related to fake profiles on social networks. This suggests that public awareness of the regulatory framework for data protection in the Republic of Macedonia is not sufficiently developed to enable citizens invoke the full gamut of their rights for safeguarding digital privacy.

Under article 45 of the DP Law, it is stated that whenever a violation of data protection provisions takes place, the Directorate is obliged to eliminate the reason for the violation and to adopt additional protective measures for personal data collection. However, the current provisions do not establish procedures and measures for protecting privacy interests and personal information in response to notification of

cyber threat indicators. It is crucial that the law define procedures describing how the DPA is to be permitted to use cyber threat information for dealing with violations of personal data and the protection of personal privacy. The current law also lacks an effective framework of penalties for subjects who are engaged in activities that violate individual privacy. Sanctions are provided only by article 149 of the Criminal Code of Republic of Macedonia.[11] The article states that "any person, who collects personal data contrary to the conditions determined by law, will be punished by a fine or by imprisonment of up to one year". Given the importance of data protection and considering that there are a multiplicity of different data offenses—some of which cause great harm to an individual's privacy—it is argued that the sanctions are too low. The existing provisions are also open to interpretation, as the amount of the fines is not determined. The potential detriment to individual data subjects arising from the absence of an effective coercive apparatus—which encourages personal data misuse—appears to be of little concern to legislators in the Republic of Macedonia.

Another legal gap in the Macedonian legislative framework relates to the processing of sensitive personal data. Sensitive information must receive considerable attention in a networked world, for—as researchers point out—every online interaction involves one or more parties disclosing information to known and unknown audiences. Some of these interactions involve extremely sensitive personal information such as financial or health data.[12] Moreover, in recent years a great deal of health data, dealing with issues such as problems of patients, medications, progress notes, medical history, etc. have been digitalized due to low cost and improvement of health care efficiency and quality.[13] Even though publishers may take protective actions in relation to such data (e.g. data de-identifitication and anonymisation), there is always a potential risk arising from the external knowledge the attackers possess, enabling them associate information accessible from various online sources (e.g. social networks) with the health data.[14] It is indisputable that medical data transmitted via online networks become vulnerable and raise concerns about threats to privacy; this has triggered calls for effective protection. Whilst the DP Law includes a modified term about sensitive

[11] Criminal Code of Republic of Macedonia of 23 July 1966 (consolidated version with the amendments from March 2004, June 2006, January 2008 and September 2009).

[12] Lampinen, A., Page, X. & Vitak, J. (2015) 'The Future of Networked privacy: Challenges and Opportunities, CSCW'15 Companion', March 14–18,, Vancouver, BC, Canada, 268. Available at: https://www.academia.edu/17330201/The_Future_of_Networked_Privacy [Accessed: January 2016].

[13] Li, F. et al. (2011) 'New threats to health data privacy'. *BMC Bioinformatics*, Washington, 1. Available at: https://www.researchgate.net/publication/51905603_New_threats_to_health_data_privacy [Accessed: March 2016].

[14] Ibid. 2 [Accessed: March 2016].

personal data,[15] it does not address in detail the conditions in which law enforcement authorities may collect and process such data.

A recent public concern regarding privacy threats in the Republic of Macedonia is related to traffic data processing. In February 2015, Zoran Zaev, leader of the opposition party (Social Democratic Union of Macedonia, SDSM) published the first in a series of wiretapped conversations, which appear to provide evidence of government corruption. It concerned a mass surveillance of thousands of Macedonian citizens, including government ministers, government employees, journalists, and others.[16] This has put the spotlight on the privacy of personal communication in the Republic of Macedonia. The DP Law does not contain express rules specifying the conditions in which authorities can process traffic data; however it provides that

> "personal data should be collected for precise legal objectives and should be used and processed in a way which is in compliance with the aims for which the personal data have been collected" (article 5).

On the other hand, privacy of communications is guaranteed in article 17 of the Macedonian Constitution, which states that

> "the freedom and confidentiality of correspondence and other forms of communication is guaranteed. Only a court decision may authorize non-application of the principle of the inviolability of correspondence and other forms of communication, in cases where it is indispensable to a criminal investigation or required in the interests of the defense of the Republic".

In light of this, Amnesty International has called on the Macedonian government to take a number of specific measures, such as: Ensure that prompt, independent, thorough and impartial criminal investigations are conducted into all allegations of criminality, including corruption and human rights violations, arising from the publication of surveillance tapes; Ensure that the legal framework on data protection, electronic communications and the interception of electronic communications is brought into line with international standards; And that any authorized surveillance is necessary, proportionate and meets a legitimate aim.[17] Moreover, Privacy International recommends that the Macedonian government ensure that private and public telecommunications and internet service providers review warrants

[15] Article 2(10) of Data Protection Law of Republic of Macedonia ('Official Gazette of the Republic of Macedonia', nos. 7/05, 103/08, 124/08, 124/10, 135/11, 43/14 and 153/15) refers to sensitive data as "special categories of personal data" under which are listed personal data related to the following characteristics: racial or ethnic origin, political views, religious or other beliefs, membership of trade union and data relating to the health condition of natural entities, including genetic data, biometric data or data referring to sexual life. The term "sensitive data" was present in the previous legal provisions for data protection in the Republic of Macedonia; however, it was adjusted in the above mentioned law.

[16] Amnesty International report (2015) Former Yugoslav Republic of Macedonia, submission to the Human Rights Committee, 114th session, 11. Available at: https://www.amnesty.org/download/Documents/EUR6517682015ENGLISH.pdf [Accessed: March 2016].

[17] Ibid. 16

before any interception of personal data from their networks takes place, and that it undertakes reform of the current system of surveillance by establishing an effective and independent oversight body for abuses prevention.[18]

EU legal framework for protection of personal data

Data protection, as a field of law, has progressed rapidly since its humble beginnings in the early 1970s.[19] In the literature, all convention rights are interpreted broadly.[20] Some of the rules are considered as negative obligations, i.e. the state should not undertake any action which violates a person's right of privacy, whereas others are viewed as positive obligations, i.e. the state should provide safeguard measures to protect an individual from others. According to Walden, data protection laws fall into the second category.[21]

The centerpiece of EU data protection legislation is Directive 95/46/EC ("The Directive"), which regulates the protection of individuals with regard to the processing of personal data and the free movement of such data. An important point to make is that the Directive does not make it entirely clear how data protection legislation applies to individuals who are posting third party personal information online.[22] For instance, let us consider the example of parents who take photographs of their children at school and then post them to social media. Those pictures often include the children's friends and the photographs are thus shared online without the consent of the children's parents.[23] Although there is no direct harm, personal life is, nonetheless, indirectly affected.

Of particular importance to privacy issues are also the following EU data protection laws: The Charter of Fundamental Rights of the European Union (2007/C 303/01), which under article 8 implies the significance of data privacy, by stating that "Everyone has the right to the protection of personal data. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law."; Convention for the Protection of individuals with regard to Automatic Processing of Personal Data of 28 January 1981, which extends the safeguards for everyone's rights and fundamental freedoms, and in

[18] Privacy International report (2015) The Right to Privacy in the Former Yugoslav Republic of Macedonia Available at: https://www.privacyinternational.org/sites/default/files/PI%20submission%20Macedonia.pdf [Accessed March 2016].

[19] Danagher, L. (2012) 'An Assessment of the Draft Data Protection Regulation: Does it Effectively Protect Data?'. *European Journal of Law and Technology*. 3 (3), Conclusion. Available at: http://ejlt.org/article/view/171/260 [Accessed: January 2016].

[20] See Walden, I. (2002) 'Anonymising personal data'. *International Journal of Law and Information Technology*. 10 (2), 229. Oxford University Press.

[21] Ibid.

[22] Bessant, C. (2015) The application of Directive 95/46/EC and the Data Protection Act 1998 when an individual posts photographs of other individuals online'. *European Journal of Law and Technology*. 6 (2), 3. Available at: http://ejlt.org/article/view/390/571 [Accessed: March 2016].

[23] Ibid. 2.

particular the right for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing[24]; and the Directive 2002/58/EC on privacy and electronic communications of 12 July 2002, which deals with a number of important privacy issues, such as confidentiality of communications, and security in the processing of personal data.

Conclusion

In this paper, the current legal framework for privacy and data protection in the Republic of Macedonia was presented, analysed and discussed with special focus on revealing potential spheres of privacy threats, which are not fully covered by the legislation in force. Provisions of Data Protection Law in the Republic of Macedonia are clear, precise and consistent with international standards. However, the legal tools available for protection of such data are useful and effective only if they adapt to current socio-technological changes.

Despite the existence of a legal framework to safeguard privacy and online data, there still remains a potential for violation of personal data and privacy. The main privacy challenges associated with big data are two-fold: lack of control and transparency; and data re-identification.[25] Lack of control and transparency occurs when data are collected from a multiplicity of different sources and flow from one system to another in such a way that individuals can easily lose control of the data. Data re-identification arises where different data sets, including non-personal data, are combined by linking different sources; in this way, individuals' private lives are capable of being affected by disclosure of confidential information.[26] In the literature, public disclosure of personal data is recognized as "context collapse" where several distinct relational contexts become a homogenous unit.[27] This is due to the impossibility of recognizing the full audience for a shared content. Even though people imagine an audience when sharing a piece of information, a discrepancy is always present between the imagined audience and those who actually view the shared content.[28]

The continuing evolution of information and communication technologies leads to new opportunities for threats to privacy in the digital world; therefore, legislation must also adapt and respond to the new challenges. Considering the fact that privacy and

[24] See the preamble of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28.1.1981.

[25] European Union Agency for Network and Information Security ("ENISA") report (2015) Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics,, ISBN: 978-92-9204-160-1, DOI: 10.2824/641480 -1, pp.13-14. Available at: https://www.enisa.europa.eu/media/news-items/privacy-by-design-in-big-data-an-overview-of-privacy-enhancing-technologies-in-the-era-of-big-data-analytics [Accessed: March 2016]/

[26] Ibid.

[27] Lampinen (2015), 268.

[28] Ibid.

data protection issues are a global problem, the Macedonian legislature should seek to provide an effective global solution for data protection. This will help Internet users to not only fully enjoy the benefits of information technology, but also to preserve full control over their digital representations and to enjoy other fundamental rights such as freedom of expression.

Bibliography

1. Amnesty International report. (2015) Former Yugoslav Republic of Macedonia, submission to the Human Rights Committee, 114th session. Available at: https://www.amnesty.org/download/Documents/EUR6517682015ENGLISH.pdf
2. Bessant, C. (2015). The application of Directive 95/46/EC and the Data Protection Act 1998 when an individual posts photographs of other individuals online. *European Journal Of Law And Technology, 6*(2), 1-27. Retrieved from http://ejlt.org/article/view/390
3. Consumer privacy bill of rights (2012) Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy, 5. Available from: https://www.whitehouse.gov/sites/default/files/privacy-final.pdf
4. Constitution of the Republic of Macedonia of 17 November 1991, as amended on April 2011. Available at: http://www.wipo.int/wipolex/en/text.jsp?file_id=239364
5. Criminal Code of Republic of Macedonia of 23 July 1966 (consolidated version with the amendments from March 2004, June 2006, January 2008 and September 2009).
6. Danagher, L. (2012). An Assessment of the Draft Data Protection Regulation: Does it Effectively Protect Data?. *European Journal Of Law And Technology, 3*(3). Available at: http://ejlt.org/article/view/171/260
7. Directorate for Personal Data Protection annual report (2014). 33-34. Available at: http://dzlp.mk/sites/default/files/u1002/MK.pdf
8. European Union Agency for Network and Information Security ("ENISA") report (2015). Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics, ISBN: 978-92-9204-160-1, DOI: 10.2824/641480 -1, 13-14. Available at: https://www.enisa.europa.eu/media/news-items/privacy-by-design-in-big-data-an-overview-of-privacy-enhancing-technologies-in-the-era-of-big-data-analytics
9. European Convention on Human Rights of 4 November 1950 as amended by Protocols Nos. 11 and 14 supplemented by Protocols Nos. 1, 4, 6, 7, 12 and 13.

10. Kilkelly, U. (2003). The right to respect for private and family life. A guide to the implementation of Article 8 of the European Convention on Human Rights. Human rights handbook No.1, 39. Available at: http://www.echr.coe.int/LibraryDocs/DG2/HRHAND/DG2-EN-HRHAND-01(2003).pdf
11. Lampinen, A., Page, X. & Vitak, J. (2015). The Future of Networked privacy: Challenges and Opportunities. CSCW'15 Companion', March 14–18, Vancouver, BC, Canada. 267-272 Available at: https://www.academia.edu/17330201/The_Future_of_Networked_Privacy.
12. Li, F., Zou, X., Liu, P., & Chen, J. (2011). New threats to health data privacy. *BMC Bioinformatics*, *12*(Suppl 12), S7. Available at: http://dx.doi.org/10.1186/1471-2105-12-s12-s7
13. Personal Data Protection Law of Republic of Macedonia ('Official Gazette of the Republic of Macedonia', no. 7/05, 103/08, 124/08, 124/10, 135/11, 43/14 and 153/15).
14. Privacy International report (2015). The Right to Privacy in the Former Yugoslav Republic of Macedonia. Available at: https://www.privacyinternational.org/sites/default/files/PI%20submission%20Macedonia.pdf
15. Samuel, D. W. & Louis, D. B. (1890). The Right to Privacy. *Harvard Law Review*, 4 (5), 193. Available at: http://www.jstor.org/stable/1321160
16. The Right to Privacy. (1891). *Harvard Law Review*, *5*(3), 148. Available at: http://dx.doi.org/10.2307/1322232
17. Danaj, Lorenc, and Aleks Prifti. "Respect for privacy from the Strasbourg perspective." *Academicus International Scientific Journal* 5 (2012): 108-118.
18. Walden, I. (2002). Anonymising Personal Data. *International Journal Of Law And Information Technology*, *10*(2), 224-237. Available at: http://dx.doi.org/10.1093/ijlit/10.2.224