



ANALYSIS

PRIVACY AND PROTECTION OF PERSONAL DATA OF YOUNG PEOPLE IN THE DIGITAL ERA

NATIONAL LEGAL FRAMEWORK AND EXPERIENCE

Skopje
2022



PRIVACY AND PROTECTION OF PERSONAL DATA OF YOUNG PEOPLE IN THE DIGITAL ERA

NATIONAL LEGAL
FRAMEWORK
AND EXPERIENCE

Skopje
2022

Skopje, 2022

Privacy and protection of personal data of young people in a digital era – national legal framework and experience - analysis

Publisher:

Macedonian Young Lawyers Association (MYLA)

Donbas St. 14/1-6 1000 Skopje

www.myla.org.mk | contact@myla.org.mk

тел. 02/ 3220 870

Author:

Manuela Stanoeska

Editors

Arben Gudaci

Maja Atanasova

Martina Drangovska Martinova

Language Editor:

Eleonora Popetrevska

Design:

Кома довел Скопје

Place of issue:

Skopje

МЕСТО ЗА ЦИП



The statements and analysis expressed in this report are solely those of the authors and have not been approved by the House of Delegates or the Board of Governors of the American Bar Association, nor the American Bar Association Rule of Law Initiative, nor present the position or policy of the American Bar Association/ ABA Rule of Law Initiative. Furthermore, nothing in this report is to be considered rendering legal advice for specific cases. The contents are the responsibility of the Macedonian Young Lawyers Association and do not necessarily reflect the views of the donor or the ABA/ ABA ROLI.

CONTENTS

LIST OF ABBREVIATIONS|5

INTRODUCTION|6

METHODOLOGY|10

STRUCTURE|12

THE CONSTITUTION OF THE RNM ON PROTECTION
OF PERSONAL DATA AND PRIVACY|14

PERSONAL DATA PROTECTION LAW AS

THE BASIC LAW|16

Consent as ground for processing
personal data|20

Right to personal data of the subjects|22

Personal Data Protection Agency
as a supervisory body|23

Right to submit a request to the PDPA|24

Right to effective judicial protection against
the decisions of the PDPA and the right to
effective judicial protection against a controller
or processor|25

Right to redress and liability|26

CRIMINAL CODE OF THE RNM|28

LAW ON JUSTICE FOR CHILDREN|30

LAW ON PROTECTION OF CHILDREN|31

LAW ON ELECTRONIC COMMUNICATIONS|32

LAW ON ELECTRONIC TRADE|34

LAW ON OBLIGATIONS|36

LAW ON SECONDARY EDUCATION|38

PRESENTATION OF DATA RECEIVED BY PDPA|40

STATE OF AFFAIRS WITH THE RIGHT TO PRIVACY|42

Conclusions|45

Challenges and recommendations|47

Bibliography|50

LIST OF ABBREVIATIONS

RNM	Republic of North Macedonia
MYLA	Macedonian Young Lawyer Association
PDPA	Personal Data Protection Agency
MES	Ministry for Education and Science
BDE	Bureau for Development of Education
PDPL	Personal Data Protection Law
CC	Criminal Code
LJC	Law on Justice for Children
LCP	Law on Child Protection
LEC	Law on Electronic Communications
LET	Law on Electronic Trade
LO	Law on Obligations
LSE	Law on Secondary Education

INTRO- DUC- TION



The last two years proved that online instead of office work is possible... that we can learn online instead of learning in the classroom. Even our social life, conversations, hanging together, exchanging opinions shifted online. Does the number of friends on the social networks correspond with the number of friends in real life and is our reality becoming more and more virtual?

Older generations are trying to follow the new online communication trends (in order to talk to each other and “see” their children, nephews and nieces on Viber or Facebook). Middle-aged people struggle with new digital world (working, hanging out, and purchasing online...), but the new generations (youth, secondary school students) live the digital reality (learning, hanging out, communicating, “gaming”,

liking each other with emoticons and stickers, getting to know each other, meeting in “chat rooms”, arguing, feeling offended, discrediting themselves... online).

¹ Toni Janevski,
“Internet
Technologies”,
University “Ss. Cyril
and Methodius” in
Skopje, Republic of
Macedonia, Skopje,
2015

The Internet¹ is a network of interrelated networks using Internet Protocol (IP) for inter-network connection and

exchange of information (irrespective of the type) between specific networks and their beneficiaries. The different services available (telephone, TV, computers, data and picture transmission, audio and video messages etc.) are clustered on the Internet as a unique platform for all services through a single global network.

Do the same rules apply on Internet as in real life? Does a slap bring about more pain than a written insult on social media seen by “everyone”?

If in reality there is someone who will scold us for improper behaviour (parents, teachers, relatives...). Can someone rebuke our behaviour in the virtual digital world (on social networks, on Internet...)? Do we have the courage to admit or recognize the mistake, to acknowledge that we were hurt, insulted, discriminated against in that virtual digital world? Is there anyone whom and where we can admit at all, and have we not offended, ridiculed, discriminated against someone else ourselves?

Should we respond, and what are the ramifications of such behaviour on the Internet? Who can protect us in a digital world?

The new virtual reality brought about many opportunities and benefits, but also new challenges and risks. Regardless of how different the new contemporary virtual world is, however, the old well-known maxima still applies: “Nothing is free in the world”. Services, products, profiles, subscriptions, films, books, music on Internet etc. are paid in Denars, Euros, Dollars, bitcoins and/or our personal data.

Do we not contribute ourselves to the increased possibility of invading our privacy by lavishly publishing our personal data on the social networks, platforms, Internet channels...? Does privacy have a price?

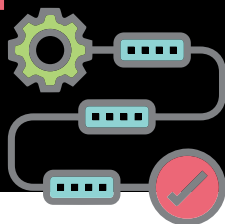
Part of our privacy diminishes by revealing every personal detail on the Internet. The control over what and how much about ourselves we want to reveal on the Internet must remain in the hands of the individual because the right to personal data protection and privacy of the individual is one of the pillars of a democratic society.

Does the current national legislation provide basis for answering these open questions? Are there any grounds for responding to the new challenges, encountering risks on the Internet and are there any protection instruments?

Exactly these dilemmas make relevant laws subject of this analysis - in which way the current national legislation treat or should treat privacy and the effective enjoyment of privacy rights on Internet, including the freedom to use Internet by secondary school students as the most affected category of individuals as well as the gender-based online violence between secondary school students.



METH- ODOLOG- OGY



The analysis was developed on the basis of methodological and empirical research. For collecting data relevant for the analysis, basic cognition methods were applied, especially: analysis, synthesis, induction, classification, specialization and generalization.

The author of the analysis is a legal expert with years-long experience in the field of personal data protection. The research methods applied in the development of this analysis were the following:

- Analysis of the national legislation related to personal data protection and privacy, analysis of legislation pertaining to protection of children and secondary education, as well as analysis of the legislation in terms of misdemeanor and criminal liability for violation of privacy rights and/or gender-based violence online.

- Thematic questionnaires were distributed to four secondary schools whereas the key findings leading to the identification of the existing problems, challenges and risks in the protection of privacy of secondary school students on the Internet, including gender-based violence among secondary school students, were taken into consideration.
- For the purpose of this analysis, data was collected by applying the instrument for free access to public information from the Personal Data Protection Agency (PDPA), as the sole competent body supervising the implementation of activities undertaken in personal data processing on the territory of the RNM, including the protection of basic rights and freedoms of natural persons and the processing of their personal data. The responses of the Agency are elaborated in this analysis.
- In the development of this analysis, the contents published on the websites of relevant public bodies were also considered those being: PDPA - www.dzlp.mk, Ministry of Education and Science (MES) - www.mon.gov.mk and the Bureau for Development of Education (BDE) - www.bro.gov.mk.

The purpose of this analysis is to acquire better understanding of the current state of affairs in terms of effective exercise of the right to privacy of secondary school students on the Internet, including gender-based violence online among secondary school students leading to the identification of shortcomings, challenges and risks in accomplishing those rights.

STRUC- TURE



This analysis includes the following national legislation:

- Personal Data Protection Law (PDPL);
- Criminal Code (CC);
- Law on Justice for Children (LJP);
- Law on Child Protection (LCP);
- Law on Electronic Communications (LEC);
- Law on Electronic Trade (LET);
- Law on Obligations(LO) and
- Law on Secondary Education (LSE).

The analyzed laws, both directly or indirectly, are related to the right of privacy on the Internet and the freedom of secondary school students to use the Internet, including gender-based violence online among secondary school students.

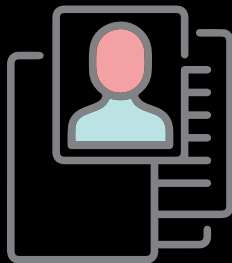
In addition, relevant provisions of the Constitution of the RNM will be analyzed, especially those pertaining to the basic freedoms and rights of the citizens, with a focus on the Personal Data Protection

Law as the most relevant legal act on the specific subject. The data received by applying the instrument for free access to public information from the PDPA will also be included.

The analysis will elaborate on the findings derived from the questionnaires answered by more than 900 secondary school students, including the information received from the Supervisory Board related to the submitted requests for determining violations of the right to personal data protection of children, violations of personal data protection of children on social networks and determined offenses in these cases. Finally, the analysis will result with conclusions and recommendations.

In this respect, we stress the fact that the RNM adopted the following: Law on Ratification of the Additional Protocol to the Convention on Protection of Individuals with regard to Automatic Processing of Personal Data, related to supervisory bodies and cross-border transmission of personal data, Law on Ratification of the Convention for Protection of Individuals with regard to Automatic Processing of Personal Data (in 2005), in 2002 the European Convention on the Exercise of Children's Rights was adopted within the framework of the Council of Europe in Strasbourg on 25th January 1996, the Additional Protocol to the Convention on Protection of Individuals with regard to Automatic Processing of Personal Data was ratified, related to supervisory bodies and cross-border transmission of data adopted by the Council of Europe in Strasbourg 8th November 2001, as well as the Law on Ratification of the Protocol for Amending the Convention on Protection of Persons with regard to Automatic Processing of Personal Data (adopted in Strasbourg 10th October 2018 and signed by the RNM 5th December 2019).

THE CONSTITUTION OF THE RNM ON PROTECTION OF PERSONAL DATA AND PRIVACY



Part II “Basic Freedoms and Rights of the Individual and Citizen (Civil and political freedoms and rights), Article 9 determines:

“Citizens of the Republic of Macedonia are equal in their freedoms and rights, regardless of sex, race, colour of skin, national and social origin, political and religious beliefs, property and social status.

All citizens are equal before the Constitution and law”.

Further, Article 18 of the Constitution guarantees the protection of personal data:

“The security and confidentiality of personal information are guaranteed.

Citizens are guaranteed the protection from any violation of their personal integrity deriving from the registration of personal information through data processing”.

In addition, Article 25 of the Constitution protects the privacy of the individual:

“Each citizen is guaranteed the respect and protection of the privacy of his/her personal and family life and his/her dignity and reputation.”

In other words, these provisions of the Constitution guarantee the security and confidentiality of personal data. Citizens are protected from violations of their personal integrity as a result of the registration of the information received from data processing. Every citizen is guaranteed respect and protection of the privacy of his/her personal and family life, dignity and reputation.

PERSONAL DATA PROTECTION LAW AS THE BASIC LAW



The Personal Data Protection Law was adopted 2005² and it “accomplished” its role at the time applied. It practically laid down the pillars of personal

² Personal Data Protection Law, “Official Gazette of the Republic of Macedonia” No.: 7/05, 103/08, 124/08, 124/10, 135/11, 43/14, 153/15, 99/16 and 64/18).

data protection in the RN Macedonia. 27th April 2016, the European Parliament and the Council of the European Union adopted Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the movement of such data, thereby repealing Directive 95/46/EC (Directive 95/46/EC was the act transposed within the Personal Data Protection Law in 2005). With the

adoption of the new regulation (known as GDPR - General Data Protection Regulation), a reform process was initiated in the area of personal data protection providing for a 2-year transitional period. The implementation

³ Personal Data Protection Law, “Official Gazette of the Republic of North Macedonia” No.: 42/20 and 294/21).

of the Regulation in the European Union started 25th May 2018. In the RN Macedonia, this Regulation was appropriately approximated within the new Personal Data Protection Law³ that went into effect 24th February 2020.

If we ask ourselves why was it necessary to adopt a new personal data protection regulation on EU level, two main reasons come to mind. The first one is the galloping technological development stride including scientific technological solutions, while the regulation of the previous directive was lagging behind in terms of resolving technical and organizational measures for securing confidentiality and protection of personal data during data processing, and the second main reason is the growing wave of automatic data-processing. Personal data is processed automatically nowadays, and paper (manual) administration is slowly but surely going into history. Therefore, the previous directive was insufficient in terms of principles guaranteeing the security of personal data adequate to the processing risk bearing in mind the new digital era.

The Personal Data Protection Law regulates the protection of personal data and the right to privacy with regard to personal data processing, especially the principles related to personal data processing, the rights

of the personal data holder, the position of the controller and processor, the transmission of personal data in other countries, establishment, status and competencies of the Personal Data Protection Agency, special processing operations of personal data, legal recourse and liability in processing personal data, supervision of personal data protection as well as misdemeanor and misdemeanor procedure in the area concerned. This law is applied to fully or partially automatic personal data processing and other kind of processing of personal data which are part of an existing personal data collection or are intended to be part of a personal data collection.

Every natural person is guaranteed personal data protection without discrimination based on his/her nationality, race, skin colour, creed, ethnic

**The Personal
Data Protection
Law regulates
the protection of
personal data and
the right to privacy**

background, gender, language, political or other beliefs, wealth, birth origin, education, social origin, citizenship, place and type of residence or any other personal features.

The Personal Data Protection Law defines the terminology used and some of the terms listed below have the following meaning:

“Personal data” is any information pertaining to an identified or identifiable natural person (personal data entity), the identifiable entity being an entity whose identity can be determined - directly or indirectly - especially on the basis of an identifier such as name and surname, personal identification number of the citizen, data on the location, identifier on the Internet or on the basis of one or more features specific for his/her physical, physiological, genetic, mental, economic, cultural or social identity of that particular natural person;

“Personal data processing” is every operation or sum of operations performed on personal data or a group of personal data, automatically or otherwise such as: collecting, recording, organizing,

structuring, storing, adjusting or altering, withdrawing, consulting, accessing, using, revealing through transmission, publishing or making them otherwise available, aligning or combining, restricting, deleting or destroying.

PDPL envisages all personal data processing to be in compliance with the basic principles of legality, fairness and transparency, restricted goals, minimum quantity of data, accuracy, restricted storage deadlines and integrity and confidentiality.

In addition, the law regulates which processing could be considered legal i.e., personal data processing is legal only if one of the following requirements are fulfilled to a specific degree:

- the personal data subject agreed to have his/her personal data processed for one or more specific purposes;
- processing is necessary for implementing an agreement where the personal data subject is a contractual party or for undertaking activities upon the request of the personal data subject prior to his/her becoming party to the agreement;
- processing is necessary for fulfilling legal obligations of the controller;
- processing is required for the protection of essential interests of the personal data subject or some other natural person;
- processing is required for undertaking public interest duties or in the course of executing public authority of the controller determined by law;
- processing is required for the purpose of legitimate interests of the controller or a third party, provided those interests do not exceed basic rights and freedoms of the personal data subject demanding personal data protection, especially when the personal data subject is a child.

CONSENT AS GROUND FOR PROCESSING PERSONAL DATA

When processing is undertaken on the basis of consent, the controller is obliged to demonstrate that the personal data subject gave his/her consent for personal data processing. If the consent of the personal data subject is provided in the form of a written statement referring to other issues as well, the consent request must be presented in a manner that clearly distinguishes other issues, in a comprehensive and easily available form, applying clear and simple components. Every part of such a statement violating the provisions of this law is not compulsory.

The personal data subject is entitled to withdraw his/her consent at any time. The withdrawal does not affect the legality of processing based on provided consent prior to the withdrawal. Before securing the consent, the personal data subject is appropriately informed, and the withdrawal of the consent must be equally simple as obtaining it. When estimating whether the consent was voluntarily given, as much as possible, consideration will be given, inter alia, to whether the execution of the agreement pertaining to a specific service is conditioned by obtaining consent for personal data processing which is not required for implementing the agreement.

In principal, personal data processing through social networks, video-gaming, using and downloading applications, watching films and music is based on certain consent provided by the beneficiary (personal data subject). Hence, when using specific Internet services, we voluntarily leave our personal data, for example we create profiles and publish photographs and videos on the social networks.

One must stress the fact that we “feed” applications used to follow wellness, fitness and health data for portable devices with special categories of personal data (ex. health status data).

As far as consent is concerned, one should emphasize that the consent provided by a child in terms of information society services is a novelty. Namely, for everything else, as a goal that entails personal data processing of children, the processing is legal only if a consent was provided or authorized by a legal representative of the child concerned. In case of information society related services however, the personal data processing is legal provided the child is at least 14 years old. The new Personal Data Protection Law provides for conditions applicable to the consent of the child pertaining to information society services. In case when the personal data subject gives his/her consent for personal data processing for one or more specific purposes, related to the direct offer of information society services to children, personal data processing is legal only if the child is at least 14 years old. If the child is less than 14 years old, the processing is legal only if a consent has been obtained from the legal representative of the child. In such cases, the controller is obliged to invest reasonable efforts to verify the consent proving that it was provided by a legal representative of the child considering the available technology.

The Personal Data Protection Law provides for a fine of 2% of the total annual income of the controller or the legal person-processor (expressed in an absolute amount) realized in the business year prior to the year when the offense was committed, or from the total income realized for a shorter period of time in the year prior to offense provided the legal person started business that particular year, to be imposed for an offense to a legal person if: conditions are not secured to verify that the consent was given by a legal representative of the child regarding the information society services.

Conditions are not secured to verify that the consent was given by a legal representative of the child regarding the information society services.

RIGHT TO PERSONAL DATA OF THE SUBJECTS

Related to “leaving” personal data on the Internet, the PDPL secures the personal data rights of the subjects:

- **Transparency implying: transparent information, communication and manner in exercising the right to personal data of the subject;**
- **Information and access to personal data related to:**
 - information submitted in the course of collecting personal data from the personal data subject,
 - information submitted when personal data is not received from the personal data subject,
 - right to access the personal data subject;
- **Correction and deletion including:**
 - right to retraction,
 - right to deletion (“right to be forgotten”),
 - right to restricted processing,
 - obligation to notify in case of retraction or deletion of personal data or restricted processing and
 - right to data portability;
- **Right to appeal and automatic making of individual decisions:**
 - right to appeal,
 - automatic making individual decisions, including profiling.

For example, when creating an user profile on a website for downloading films, transparency is accomplished by publishing the Privacy Policy on the website itself, which should reveal data on the owner of the

website, whether the data submitted in the course of registration is used for other purposes, is that data shared with other websites, and how to deactivate the profile and request deletion of the submitted data.

One of the six grounds on which a request can be submitted for exercising the right to deletion (“right to be forgotten”) is if personal data was collected related to an offer for information society service, in case when the personal data subject gave his/her consent when he/she was less than 14 years old (or if the consent was given or permitted by the legal representative of the child) for processing personal data for one or more specific goals, and related to the direct information society service offered to children. According to this ground, the personal data subject may demand from the provider/browser to delete one or more results if personal data related to the information society offer to the child was collected. For example, one can require deletion of his/her personal data submitted by a child for the purpose of downloading or joining some online game.

PERSONAL DATA PROTECTION AGENCY AS A SUPERVISORY BODY

In 2005, with the adoption of the PDPL for supervising the legality of the undertaken activities in the course of personal data processing and protection, the Personal Data Protection Directorate was established as a legal person and independent and autonomous public body.

The new PDPL dated 2020 transformed the Personal Data Protection Directorate into a Personal Data Protection Agency (PDPA) as an independent and autonomous public body competent for supervising the legality of undertaken activities in the course of personal data

processing on the territory of the RNM, including the protection of basic rights and freedoms of natural persons with regard to personal data processing. PDPA has a supervisory, advisory and corrective competences.

Supervision of personal data protection, with regard to this law, is systemic and independent control of legality of undertaken activities in the course of personal data processing and protection in the implementation of the PDPL and the regulations stemming therein, especially related to researching, checking, providing directions and prevention of controllers and processors. The Agency performs supervision through personal data protection supervisors.

Apart from the authority and competences of the PDPA, the law regulates the duties to be implemented. One of the legally determined duties of the Agency is to “promote public awareness and identify the risks, rules, protective measures and rights with regard to personal data processing, especially activities directed towards children”.

RIGHT TO SUBMIT A REQUEST TO THE PDPA

Every personal data subject is entitled to submit a request to the PDPA if he/she deems that the act of processing his/her personal data violates the provisions of the PDPL notwithstanding any other administrative or judicial remedies for legal protection. The Agency informs the person filing the request about the course of the procedure, including the opportunity of judicial protection. The PDPA facilitates the submission of the request by means of measures such as: request form that can be filled in electronically in compliance with the law, without excluding other communication tools. PDPA will decide whether the personal data of the requester will be revealed during the procedure to the interested party and the witness. The PDPA implements supervision for the request submitted.

There is a possibility for submitting a web-form request, and the form for filing a request to the PDPA⁴ is also published. In addition, the website has the form for “Requesting the deletion of a fake profile created in your name”⁵.

⁴ www.dzlp.mk

⁵ https://dzlp.mk/sites/default/files/u4/baranje_socijalni_mrezi_2.pdf

RIGHT TO EFFECTIVE JUDICIAL PROTECTION AGAINST THE DECISIONS OF THE PDPA AND THE RIGHT TO EFFECTIVE JUDICIAL PROTECTION AGAINST A CONTROLLER OR PROCESSOR

Every natural or legal person is entitled to effective judicial protection against a legally binding decision of the PDPA pertaining to him/her notwithstanding any other administrative or outside-of-court legal protection means.

Every personal data subject is entitled to effective judicial protection if the PDPA does not inform the personal data subject within three months of the submitted request about the outcome of the procedure (in case he/she deems that the provisions of the law were violated regarding his/her personal data).

Notwithstanding any other available administrative or out-of-court legal protection, including the right to submit a request to the PDPA (in case he/she deems that the processing of his/her personal data is a violation of the provisions of this law), every personal data subject is entitled to effective judicial protection when deemed that his/her rights determined by law were violated as a result of personal data processing contrary to this law.

The personal data subject exercises the right to judicial protection by initiating a lawsuit in the competent court in accordance with the law.

RIGHT TO REDRESS AND LIABILITY

Every person who suffered material or non-material damage as a result of the PDPL has the right to indemnity from the controller or processor for the damaged inflicted.

Every controller involved in personal data processing is responsible for the damage caused by the processing that violated the provisions of the law. The processor is liable for the damage inflicted by the processing act only if he/she does not respect the obligations of the PDPL, especially addressing the processors or when he/she acted outside or opposed to the legal guidelines of a controller.

The procedure for exercising the right to redress takes place in the competent court according to the law.



CRIMINAL CODE OF THE RNM



The Criminal Code⁶ is not applied for a child who was not fourteen years old at the time of committing the criminal act. For

⁶ Criminal Code ("Official Gazette of the Republic of Macedonia" No.: 37/1996, 80/1999, 4/2002, 43/2003, 19/2004, 81/2005, 60/2006, 73/2006, 7/2008, 139/2008, 114/2009, 51/2011, 135/2011, 185/2011, 142/2012, 166/2012, 55/2013, 82/2013, 14/2014, 27/2014, 28/2014, 41/2014, 115/2014, 132/2014, 160/2014, 199/2014, 196/2015, 226/2015, 97/2017 и 248/2018).

minors and younger adults committing criminal acts provided for in the law or ratified international agreements in compliance with the Constitution of the RNM, the provisions of the CC are applied, if not foreseen otherwise by law.

According to the terminology of the CC, the meaning of the phrase "victim of criminal action" implies every person who has suffered damage, including physical or mental pain, emotional suffering, material loss or other kind of injury or having his/her basic freedoms and rights threatened as a consequence of the committed criminal act.

The phrase **"child as a victim of criminal act"** implies a minor person less than 18 years old.

“Violence against a child”, according to the Criminal Code, inter alia, implies: psychological violence, **violence through the Internet**, peer violence as well as stalking and following the child.

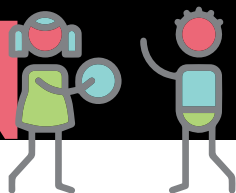
The Criminal Code regulates the criminal action: **“Violence against a child”** - He/she who will perform physical, psychological or other type of violence against a child, shall be sanctioned with a fine or imprisonment of six months to three years”.

The part covering criminal actions against human freedoms and rights of the citizen, the criminal act **“Abuse of personal data”** is regulated: He/she, opposed to the conditions determined by law, without the consent of the citizen, collects, processes or uses his/her personal data will be fined or imprisoned up to one year.

In compliance with Paragraph 1, a penalty will be imposed to the person accessing a computer information system of personal data with the intention of using the data for oneself or for some other person to benefit from it or to inflict some kind of damage to another person”.

Regarding discrimination on whatever ground, the Criminal Code defines the criminal act “Racial and other discrimination” as - “Whoever based on the difference in sex, race, skin color, class, membership in a marginalized, ethnic background, language, nationality, social background, religious belief, other types of beliefs, education, political affiliation, personal or social condition, mental or physical disability, age, family or marital status, property status, health condition or any other ground foreseen by law or ratified international agreement, violates the basic human rights and freedoms acknowledged by the international community, shall be sentenced to imprisonment of six months to five years”.

LAW ON JUSTICE FOR CHILDREN



The Law on Justice for Children⁷ regulates actions with children at risk and children perpetrators of acts foreseen as crime or misdemeanor

⁷ Law on Justice for Children
("Official Gazette of the Republic of Macedonia"
No. 148/2013 and
"Official Gazette of the Republic of North Macedonia"
No. 152/2019 and 275/2019)

by law, determining the conditions for use of assistance measures, care and protection, educational and alternative sanctioning of children and younger adults, the position, role and competence of bodies participating in actions with children and enforcement of educational and alternative measures and punishment.

This law regulates the measures for protection of children victims of acts which are foreseen as crime by law and children witnesses, and measures for prevention of child offending.

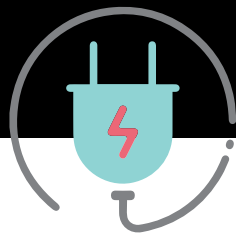
The Law and its implementation aim at achieving priority interest and protection of children from crime, violence and all other forms of endangering their freedoms and rights and their proper development, protection of children perpetrators of acts which by law are prescribed as crime and misdemeanor and from recurrent offenses, their socialization, education and upbringing, assistance and care for children and protection of their freedoms and rights guaranteed by the Constitution of the Republic of North Macedonia, the Convention of the Rights of the Child and other international agreements applying to children and ratified in compliance with the Constitution of the Republic of North Macedonia, in procedures in courts and other bodies.

LAW ON PROTECTION OF CHILDREN

The Law on Protection of Children⁸ regulates the system and organization for protection of children. Children protection is an organized action based on children's rights, as well as parents' rights and obligations for family-planning as well as the State and local self-government units for adopting a humane population policy. Protection of children is achieved by providing conditions and level of living standard adequate to the physical, mental, emotional, moral and social development of the children. The protection of children, under this law, is achieved by the provision of specific rights, means and forms of child protection. The application of these legal provisions implies principles of protection of the right to life and development of the child, protection of the child's best interest, providing minimum standard for each child under equal conditions, exclusion of any form of discrimination, respecting the child's right to freedom and safety of personality, their own opinion and free expression, association and education, conditions for healthy life and exercising other social rights and liberties of the child.

⁸ Law on Electronic Communications ("Official Gazette of the Republic of Macedonia" No. 39/2014, 188/2014, 44/2015, 193/2015, 11/2018 and 21/2018 and "Official Gazette of the Republic of North Macedonia" No. 98/2019 and 153/2019

LAW ON ELECTRONIC COMMUNICA- TIONS



⁹ Law on Electronic Trade ("Official Gazette of the Republic of Macedonia" No. 133/2007, 17/2011, 104/2015 and 192/2015 and "Official Gazette of the Republic of North Macedonia" No. "Official Gazette of the Republic of Macedonia" No. 31/2020)

The Law on Electronic Communications⁹, inter alia, defines the following expressions: "Information society services": paid services are provided from a distance via electronic means upon personal request of the receiving party.

"From distance" means that the service is provided without simultaneous presence of both parties.

"Via electronic means" implies that the service is sent from the starting/source point and received at the final destination via electronic processing equipment (including digital compression) and data storage, and is fully sent, transferred and received via cable, radio waves, optics or other electromagnetic means.

"Upon personal request of the receiving party" implies that services are provided upon personal request via data transfer.) This law also regulates actions in case of "Unsolicited communications" (Article 174): (1) The use of automated calling and communication systems for making calls to

subscriber telephone numbers without human intervention (automated machines for calls, SMS, MMS), such as facsimile machines or electronic mail, for the purposes of direct marketing, may only be allowed if the subscribers have given consent thereto. (2) Natural and legal persons may use electronic contact data for e-mail obtained by consumers of their products or services, for direct marketing and sale only of their similar products and services provided they have given to those consumers a clear and unambiguous opportunity to object in a simple manner and free of charge to such use of the electronic contact data when said data are being obtained and when each message is received, in cases the consumer have not refused in advance the use of its electronic contact data. (3) Unsolicited communications for the purpose of direct marketing differing from those stated in paragraphs (1) and (2) of this Article (for instance, voice telephone calls), shall be permitted only when the subscribers or users have provided consent thereof and shall be free of charge. 4) Sending e-mails for direct marketing or for encouraging visits of specific websites by concealing the sender's identity on whose behalf the communication has been made, and without valid address where the communication recipient may send a request for termination of such communication is hereby prohibited.

Article 26-a of the Law on Electronic Communications foresees the establishment of a special organizational unit within the Electronic Communication Agency – National Computer Incidents Response Centre (MKD-CIRT), representing the official national contact and coordination point for dealing with security incidents with networks and information systems that will identify and respond to security incidents and risks (website www.mkd-cirt.mk).

LAW ON ELECTRONIC TRADE



This Law¹⁰ regulates information society services related to electronic trade, responsibilities of information society service providers,

commercial communication and rules applicable for signing contracts in electronic form.

¹⁰ Law on Electronic Trade ("Official Gazette of the Republic of Macedonia" No. 133/2007, 17/2011, 104/2015 and 192/2015 and "Official Gazette of the Republic of North Macedonia" No. "Official Gazette of the Republic of Macedonia" No. 31/2020)

The Law on Electronic Trade regulates the information that needs to be provided in commercial communication:

"(1) The information society service provider shall be obliged to make at least the following information easily, directly and permanently accessible to the recipient of services and to competent state bodies of the Republic of Macedonia: name i.e. company of the service-provider,

legal person seat, service-provider or address if a natural person is concerned, service-provider data based on which the recipient of the service can directly and efficiently contact him/her, including electronic address, trade register where the service-provider is recorded and its registration number or equivalent means

of identification in the Register, when the service-provider is recorded in the Trade or other adequate Register; competent body data, if the service-provider requires a license or other type of approval and tax number if the service-provider is a VAT taxpayer. (2) In addition to the information from paragraph (1) of this Article, the information society service-provider performing a regulated profession shall be obliged to make the following information also available: data on the institution where the service-provider is registered; professional title and the country where the title was obtained and referral to professional rules in the country where the activity is performed and how to access them.”

These provisions of the Law on Electronic Trade correspond with the transparency principle determined by the Personal Data Protection Law, especially with regard to information on identity of the controller in cases where sales via website is performed.

In addition, the law incorporates provisions which refer to commercial communications (Article 8) and unsolicited commercial communication (Article 9).



LAW ON OBLIGATIONS



The Law on Obligations¹¹ regulates the following: “The willingness to sign a contract may be expressed in words, usual signs or other behavior from which its existence, content and identity of the person giving the statement can be concluded with certainty. The willingness to sign a contract can be expressed also by means of various communication means (telephone, fax, **internet connection** etc.). (3) The willingness statement must be produced freely and seriously.

¹¹ Law on Obligations
("Official Gazette
of the Republic of
Macedonia" No.
18/2001, 4/2002,
5/2003, 84/2008,
81/2009, 161/2009
and 123/2013 and
"Official Gazette of
the Republic of North
Macedonia" No.
215/2021)

The Law on Obligations also regulates liabilities in cases of damage caused by a child.

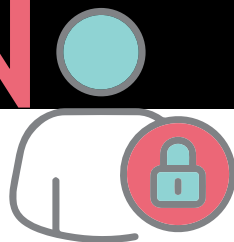
Other person's responsibility for over a minor person: According to Article 154 of this Law: (1) Where damage has been caused by a minor while under the supervision of a guardian, school or other institution, the guardian, school or the other institution shall be held liable, unless they provide evidence for the correct supervision they were obliged to conduct or that the damage would have been caused

even with careful supervision. (2) Where the minor is liable for the damage as well, the liability shall be joint.

Special parental responsibility: According to Article 155 of this Law: (1) Where the duty to supervise a minor is not with the parents, but with some other person, the damaged party shall be entitled to request compensation from the parents if the damage was caused due to poor parental guidance, bad examples or vicious habits given by the parents, or if the parents can otherwise be liable for damage. (2) In such a case, where the third person responsible for supervising the minor pays compensation to the damaged party, the guardian shall be entitled to request reimbursement for the compensation from the parents.

Liability on grounds of fairness: According to Article 156 of the Law: (1) Where damage is caused by a person not liable for it, and compensation cannot be obtained from the person responsible to supervise the damaging person, the court, taking into consideration the financial state of the damaged and the damaging party, may when the principle of fairness indicates so, decide on partial or full compensation by the damaging party. (2) Where damage is caused by a minor capable of making judgement, but unable to pay compensation, the court, especially taking into consideration the financial state of the parents and the damaged party, may, when the principle of fairness indicates so, decide on full or partial compensation by the parents regardless of the fact that they are not being at fault.

LAW ON SECONDARY EDUCATION



The Law on Secondary Education¹² was analyzed, and the websites of the Ministry of Education and science www.mon.gov.mk, and of the Bureau

¹² 3 Law on Secondary Education ("Official Gazette of the Republic of Macedonia" No. 44/1995, 24/1996, 34/1996, 35/1997, 82/1999, 29/2002, 40/2003, 42/2003, 67/2004, 55/2005, 113/2005, 35/2006, 30/2007, 49/2007, 81/2008, 92/2008, 33/2010, 116/2010, 156/2010, 18/2011, 42/2011, 51/2011, 6/2012, 100/2012, 24/2013, 41/2014, 116/2014, 135/2014, 10/2015, 98/2015, 145/2015, 30/2016, 127/2016, 67/2017 and 64/2018 and "Official Gazette of the Republic of North Macedonia" No. 229/2020)

for Development of Education www.bro.gov.mk were reviewed in the development of this analysis. The Law on Secondary Education incorporates several norms which refer to personal data only in context of the need for processing the data for integrated databases of the Ministry of Education and Science ("The secondary school collects, processes, stores, sends and uses data contained in the collective data in line with the regulations for personal data protection, for the needs of the integrated database of the Ministry"), and in context that the secondary school receives these data from the parents/guardians of the students.

Having reviewed the websites of the Ministry of Education and Science www.mon.gov.mk and of the Bureau for Development of Education www.bro.gov.mk, it became

obvious that no data was published on projects and documents (for example, manuals, guides, brochures, curricula etc.) related or pertaining in some way to privacy and effective use of the right to privacy on the Internet and the freedom to use the Internet of high school students, as well as gender-based online violence among high school students.

Furthermore, it should be emphasized that in Macedonia, the subject Information Technology was introduced relatively early - in 1986 - and that the first more serious computerization of schools took place in 2002 when China donated 6,000 computers for the schools.

In October 2020, several websites¹³ published that every seventh student in Macedonia could not participate in the online teaching process that started 1st October (due to Covid 19 situation), because they did not have electronic device – computer, tablet or smartphone. A total of 40,000 primary and secondary school students had to follow recorded lectures on one of the new channels of the Macedonian Radio-Television or to study from printed material provided by the teachers.

¹³ <https://makfax.com.mk/top/40-%D0%B8%D0%BB%D1%98%D0%B0%D0%B4%D0%B8-%D0%B4%D0%B5%D1%86%D0%B0-%D0%BD%D0%B5%D0%BC%D0%B0%D0%B0%D1%82-%D0%BA%D0%BE%D0%BC%D0%BF%D1%98%D1%83%D1%82%D0%B5%D1%80%D0%B8-%D0%B7%D0%B0-%D0%B4%D0%B0-%D1%81/>

<https://www.novamakedonija.com.mk/makedonija/%D1%87%D0%B5%D1%82%D0%B8%D1%80%D0%B8%D0%B5%D1%81%D0%B5%D1%82-%D0%B8%D0%BB%D1%98%D0%B0%D0%B4%D0%B8-%D0%B4%D0%B5%D1%86%D0%B0-%D0%BD%D0%B5%D0%BC%D0%B0%D0%B0%D1%82-%D0%BA%D0%BE%D0%BC%D0%BF%D1%98%D1%83/>

PRESENTATION OF DATA RECEIVED BY PDPA



A request for free access to information was filed to the PDPA regarding the following issues:

- How many requests have been filed to the PDPA by minors (via their legal representatives) in 2021 related to deleting fake social network profiles, locked profiles or photographs used from their profiles?
- Did PDPA undertake any activities in 2020 and 2021 which refer to privacy protection of minors and secondary school students on social networks?

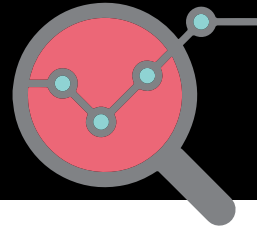
The following is the answer received by PDPA:

- A total of 488 submissions were filed to PDPA in the period from 01.01.2021 until 31.10.2021. Most of complaints refer to social network abuse and harmonization with the new personal data protection regulation, especially regarding the documentation of technical and organizational measures for providing personal data processing security adequate to the risk, followed by appointing

an authorized person (personal data protection officer), personal data protection impact assessment etc. The remaining part of the submissions refer to personal data processing via video supervision system, information regarding personal data rights of the subject, direct marketing etc.

- Regarding supervisions, the Agency's supervisors carried out 269 supervisions in the period from 01.01.2021 until 31.10.2021. Despite the ongoing challenges of the Covid-19 pandemic, the number of supervisions carried out in 2021 increased compared to 2020. Also, in this period supervisors responded to 75 requests to determine violation of the right to personal data protection. The requests referred to: exercising personal data rights of the subjects (access to personal data, deleting personal data), video surveillance, processing citizens' personal data with the aim of receiving fast loans etc. One (1) of the requests referred to publishing a photograph of a child taken in a kindergarten, used for marketing purposes by a photo studio without parental consent. The Agency identified violations of the right to personal data protection in 18 cases.
- 28th January 2021, on the occasion of celebrating the 40th Anniversary of the European Personal Data Protection Day, the Agency organized a presentation via online platform in order to inform citizens of their respective rights, thus enabling more efficient exercising of these rights. The document Privacy of children and youth in the world of modern technologies (Internet and social networks) was published in February, meaning that the Agency started its outreach activities to bring the subject closer to children and youth.

STATE OF AFFAIRS WITH THE RIGHT TO PRIVACY



A questionnaire intended for secondary school students with the following questions was sent to four (4) secondary schools:

- Which social networks do you use?
- How much time do you spend on the Internet daily?
- When creating a new user-profile on a social network do you use your real personal data?
- Was there a case when your photographs published on social network were used without your consent?
- Do you publish other people's photographs on social networks without asking for consent?
- Have you been offended on the social networks by someone?
- Have you been a victim of gender-based online violence? Describe.
- Do you know a peer student/friend who was a victim of gender-based on line violence (offended via social networks)? Describe.
- Do you ever buy online?

- Have you used your parents' user profile or created a new profile when buying online?
- Have you downloaded music or played an Internet game requiring your personal data?
- In case of violation of privacy via social networks and/or Internet do you know where to turn to? Where?

Over 1000 answered questionnaires were received by the secondary school students. The analysis of the responses indicated the following:

- The initial number of questionnaire responses received is represents a solid indicator of the interest on the topic at hand;
- Most of the secondary school students use different social networks; only five of them responded that they did not use any social network;
- Most of the interviewed secondary school students spend from two to five hours per day on the Internet;
- Approximately two thirds of the respondents use real personal data when creating a new user profile;
- Most of the interviewed secondary school students don't publish other people's photographs without consent; and photographs of more than 100 respondents were published on a social network without obtaining their consent;
- Part of the interviewed secondary school students had been offended via social networks, but did not feel comfortable to describe the event;
- Small part of the respondents admitted that in some cases they received messages that could be considered as gender-based violence;

- Most of the interviewed secondary school students knew someone (peer student/friend) who had been a victim of gender-based violence, but they did not describe the exact situation (for example, they said “it’s too vulgar to describe”), whereas some of them believed that “everyone from these generations was subject to online gender-based violence at a certain period”;
- Over 700 interviewed secondary school students bought goods/ services on the Internet, whereas less than half of them used their existing profiles while the remaining part created new user profiles;
- Most of the respondents had downloaded music or played games on the Internet where personal data were required, and some of them gave their real personal data to receive the service;
- Small part of the respondents from secondary school knew where to turn to if violation of privacy happened on the Internet (some of the answers were: cybercrime police, police, it is not regulated...), whereas a significant number stated that they would seek the help of their parents.

CONCLUSIONS

The existing PDPL is harmonized with the European acquis and makes emphasis on automated processing of personal data and protection of privacy, hence there is a good basis for protection of privacy and personal data processing in the RNM. PDPL pays attention to personal data of children when offering information society services, stressing the validity of the consent given for personal data processing, information and transparency.

One of the tasks of the PDPA foreseen by the PDPL is promotion of public awareness and understanding risks, rules, protection measures and rights related to personal data processing, especially activities directed towards children. From the information received by the PDPA and from the website www.dzlp.mk in the period of entering into force of the new law and its application, no information was available on projects and activities undertaken by the PDPA for achieving this task directed towards children.

In 2021, despite the situation with the Covid 19 virus, the PDPA carried out numerous supervisions, among which acting only upon one request for determining violation of personal data protection. The Agency does not keep separate records of the number of requests filed by minor persons (via their legal representatives) in the course of 2021 which refer to deleting fake profiles on social networks, locked profiles or photographs used from their profiles.

Further, it can be stated that formal secondary education does not include programs, contents and topics on privacy on the Internet, personal data protection and gender-based violence, implying that there is a need

to include activities, topics and content on the respective topics with informal education.

The analysis of the questionnaires responded by secondary school students shows that although students spend a large portion of their time on the Internet, they don't know exactly where to turn to if violation of privacy via social networks and/or Internet happens to them. In addition, students can, in general, recognize gender-based violence on the Internet.

CHALLENGES AND RECOMMENDATIONS

- The need to amend secondary school curricula by including topics on effective exercising of rights to privacy on the Internet and freedom to use Internet, as well as gender-based online violence among students in secondary education is evident.
- Having in mind that formal education does not include educational topics on exercising rights to privacy on the Internet and freedom to use Internet for secondary school students, as well as gender-based violence online among secondary school students, it is recommended to use informal education to enable secondary school students to develop competences that fully equip them to research and use numerous possibilities offered by the Internet, but at the same time to be able to manage (recognize and deal with) challenges and risks on the Internet. In addition, this education must include contents and information about the rights and responsibilities when using the Internet, especially regarding personal data protection and respecting other people's privacy on the Internet.
- Competent bodies (PDPA, MOS, BDE) need to cooperate with each other and promote public awareness and identifying risks, rules, protection measures and rights with regard to personal

data processing, and especially on activities directed towards children. Even more, they need to cooperate with nongovernmental organizations that implement projects intended for education and exercising rights to privacy of children and secondary school students, including gender-based violence.

- Training on the specific topic needs to be implemented on micro level also, and each school should act educationally, preventive and effective. Secondary schools should encourage training of their students in exercising the rights to privacy on the Internet and freedom to use the Internet and secure adequate response to gender-based violence online among students in secondary schools, but also education them on the responsibilities when using the Internet.
- Secondary schools need to provide high level training for their staff (teachers, pedagogues, physiologist...) on the respective topics so that they will be able to guide secondary school students in exercising their rights and responsibilities on the Internet.
- There is a need to find a way to train parents on the respective topics so that they can participate in students' education on exercising their rights and responsibilities when using the Internet.
- It is necessary to introduce appropriate mechanisms for reporting violations of privacy and right to personal data protection and gender-based violence on the Internet within the schools (for example, appointing teacher, pedagogue, psychologist or personal data protection officer to whom students can report or get informed about violations of the right to privacy on the Internet and gender-based violence, which depending on the specific situation will further direct them to the appropriate competent body – for example to file a request to the PDPA).

- In addition to the need to train secondary school students on the topics, they ought to be encouraged to report violations of privacy and gender-based violence on the Internet. It is necessary to consider that recommended activities should be directed to dealing with the essential challenge: protection of privacy and personal data to be an element integrated into the behavioral culture and thus part of the educational process of secondary school students.

BIBLIOGRAPHY

Toni Janevski, "Internet Technologies", University "Ss. Cyril and Methodius" in Skopje, Republic of Macedonia, Skopje, 2015

Personal Data Protection Law, "Official Gazette of the Republic of Macedonia" No. 7/05, 103/08, 124/08, 124/10, 135/11, 43/14, 153/15, 99/16 and 64/18).

Personal Data Protection Law, "Official Gazette of the Republic of North Macedonia" No. 42/20 and 294/21).

Criminal Code ("Official Gazette of the Republic of Macedonia" No. 7/1996, 80/1999, 4/2002, 43/2003, 19/2004, 81/2005, 60/2006, 73/2006, 7/2008, 139/2008, 114/2009, 51/2011, 135/2011, 185/2011, 142/2012, 166/2012, 55/2013, 82/2013, 14/2014, 27/2014, 28/2014, 41/2014, 115/2014, 132/2014, 160/2014, 199/2014, 196/2015, 226/2015, 97/2017 and 248/2018)

Law on Justice for Children ("Official Gazette of the Republic of Macedonia" No. 148/2013 и "Official Gazette of the Republic of North Macedonia" No. 152/2019 and 275/2019)

Law on Protection of Children ("Official Gazette of the Republic of Macedonia" No. 23/2013, 12/2014, 44/2014, 144/2014, 10/2015, 25/2015, 150/2015, 192/2015, 27/2016, 163/2017, 21/2018 and 198/2018 and "Official Gazette of the Republic of North Macedonia" No. 104/2019, 146/2019, 275/2019, 311/2020 and 294/2021)

Law on Electronic Communications ("Official Gazette of the Republic of Macedonia" No. 39/2014, 188/2014, 44/2015, 193/2015, 11/2018 and 21/2018 and "Official Gazette of the Republic of North Macedonia" No. 98/2019 and 153/2019)

Law on Electronic Trade ("Official Gazette of the Republic of Macedonia" No. 133/2007, 17/2011, 104/2015 and 192/2015 and "Official Gazette of the Republic of North Macedonia" No. 31/2020).

Law on Obligations (“Official Gazette of the Republic of Macedonia” No. 18/2001, 4/2002, 5/2003, 84/2008, 81/2009, 161/2009 and 123/2013 and “Official Gazette of the Republic of North Macedonia” No. 215/2021)

Law on Secondary Education (“Official Gazette of the Republic of Macedonia” No. 44/1995, 24/1996, 34/1996, 35/1997, 82/1999, 29/2002, 40/2003, 42/2003, 67/2004, 55/2005, 113/2005, 35/2006, 30/2007, 49/2007, 81/2008, 92/2008, 33/2010, 116/2010, 156/2010, 18/2011, 42/2011, 51/2011, 6/2012, 100/2012, 24/2013, 41/2014, 116/2014, 135/2014, 10/2015, 98/2015, 145/2015, 30/2016, 127/2016, 67/2017 and 64/2018 and “Official Gazette of the Republic of North Macedonia” No. 29/2020)

<https://makfax.com.mk/top/40-%D0%B8%D0%BB%D1%98%D0%B0%D0%B4%D0%B8-%D0%B4%D0%B5%D1%86%D0%B0-%D0%BD%D0%B5%D0%BC%D0%B0%D0%B0%D1%82-%D0%BA%D0%BE%D0%BC%D0%BF%D1%98%D1%83%D1%82%D0%B5%D1%80%D0%B8-%D0%B7%D0%B0-%D0%B4%D0%B0-%D1%81/>

<https://www.novamakedonija.com.mk/makedonija/%D1%87%D0%B5%D1%82%D0%B8%D1%80%D0%B8%D0%B5%D1%81%D0%B5%D1%82-%D0%B8%D0%B8%D1%98%D0%B0%D0%B4%D0%B8-%D0%B4%D0%B5%D1%86%D0%B0-%D0%BD%D0%B5%D0%BC%D0%B0%D0%B0%D1%82-%D0%BA%D0%BE%D0%BC%D0%BF%D1%98%D1%83/>

www.dzlp.mk

