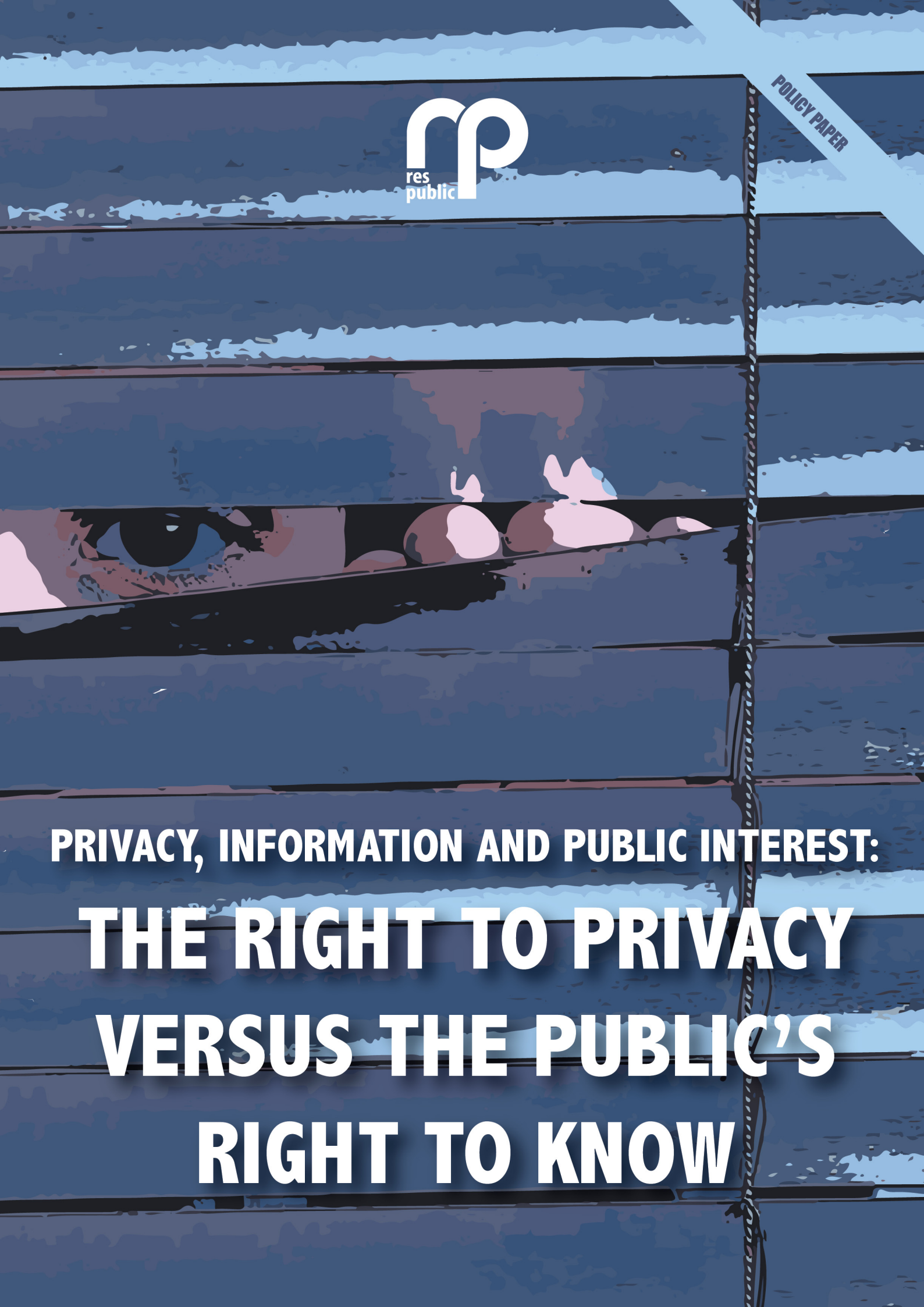


PRIVACY, INFORMATION AND PUBLIC INTEREST:

THE RIGHT TO PRIVACY VERSUS THE PUBLIC'S RIGHT TO KNOW

PRIVACY, INFORMATION AND PUBLIC INTEREST:
THE RIGHT TO PRIVACY VERSUS THE PUBLIC'S RIGHT TO KNOW

POLICY PAPER

PRIVACY, INFORMATION AND PUBLIC INTEREST:
THE RIGHT TO PRIVACY VERSUS THE PUBLIC'S RIGHT TO KNOW

Publishers: Institute of Communication Studies
School of Journalism and Public Relations
Jurij Gagarin no. 17/1-1, Skopje
www.iks.edu.mk
www.vs.edu.mk

For the publishers: Zaneta Trajkoska

Authors: Elena Stojanovska, Jovana Ananievska
Translation: Kalina Janeva
Editors: Zaneta Trajkoska, Bojan Georgievski
Cover and layout: Ljuben Dimanovski

British Embassy Skopje

The British Embassy Skopje supported the preparation of this publication, within the project "Voicing the Public Interest: Empowering Media and Citizens for Safeguarding the Public Policy in Macedonia". The content of this publication does not necessarily reflect the position or the opinions of the British Embassy in Skopje.

PRIVACY, INFORMATION AND PUBLIC INTEREST: THE RIGHT TO PRIVACY VERSUS THE PUBLIC'S RIGHT TO KNOW

Содржина

Executive Summary

The subject of this analysis is the issue of establishing balance between public and private interests, primarily in the sphere of the media's disclosing information containing personal data on the individuals subject to media reporting. The aim is, by analysing the European standards defined in the human rights protection legislation and in the national laws pertaining to the sphere of privacy protection, to assess the mechanisms guaranteeing the protection of privacy, but do not, in turn, restrict the right to information. As indicators for the importance of the subject matter, there are examples provided from the European Court of Human Rights (ECtHR) case law, which clearly show the relationship between privacy and public interest, as well as the position of the right to privacy against the public's right to information and public interest. The analysis also includes examples from the media reporting practice in the Republic of Macedonia, elucidating different situations in which the right to privacy and the right to information have not been put in the minimum balance required to respect both rights equally. Finally, the analysis devises conclusions and recommendations for the media, the institutions, but also for the public, conducive to fair implementation of the standards of respecting privacy.

The research has been conducted as part of the project *Expressing Public Interest: Increasing the Power of the Media and the Citizens in Safeguarding Public Policy in Macedonia.*

The project has been supported by the British Embassy Skopje.

Introduction

The analysis covers the right to privacy and the public's right to information, the challenges arising in the attempt to establish balance in enjoying these two rights and the shortcomings complicating the already existing entwinement of these two areas. It is unseldom the case that the right to privacy be violated under the guise of the public's right to information, even when it is baseless and unsubstantiated by well-argued reasons. On the other hand, individuals known to the public often 'abuse' the right to privacy, that is, even when subject to potential disclosure is public interest information, but concerning them personally, so they invoke the right to privacy as 'the right of all rights.'

This analysis proceeds from the fact that in the Republic of Macedonia there are shortcomings regarding the clarity and the enactment of legislation in this area. The key regulations from the field of privacy protection included in this analysis are primarily the Law on Personal Data Protection and the Law on Free Access to Public Information. However, subject to analysis are also the Law on Electronic Communications, the Law on Interception of Communications and the Law on the Protection of Privacy, as relevant legal acts in the area. Furthermore, the analysis portrays the situation by an overview of examples from the practice that clearly indicate that even the current legislative framework is not being implemented, but also that it requires changes that would affect the strengthening of the protection mechanisms and the improved balance between the right to information and the right to privacy.

Even though the analysis focuses on the balance between the right to privacy and the right to information, it attempts to offer a brief overview of the right to privacy from a different equally significant aspect as well, which is the ubiquity of contemporary communication technology and the manner in which citizens rely on this technology that helps transfer and manage sensitive personal data. Whereas before the 'boom' of technological progress, privacy and data were in complete control of the individual, that has radically changed in the last few decades. In the age we live in, our information may be intercepted and abused by various parties with great ease, and the line between the public and the private has been growing increasingly thinner. The paradox of the new developments and turmoil in the field of privacy is that, at the same time, people do not refrain from sharing personal data on the mass Internet services (Facebook, Twitter, etc.), where they practically disclose their whole eyes in full view of other individuals, i.e. 'friends' (oftentimes people they do not even know). So there are frequent cases of abuse of these data (for instance, posting photographs without their owner's permission).

Citizens do not pay sufficient attention to the fact that the intense use of tools that make everyday life easier (email, smartphones, online payment, social media and many other types of services offered by modern technology) comes with certain risks. Their negligence to protect their data leaves them exposed to abuse, and their privacy is constantly threatened. The media play an important part in this relationship, since

they are the ones that are obliged to inform the public in a transparent, truthful and ethically correct manner. This entails responsible handling the citizens' private data, and caution when publishing sensitive personal information. For this very reason, considering the great importance and the role of the media in protecting and advancing privacy, but also in responsible informing of the public, in the following text we will attempt to reflect on their role in this aspect as well.

Furthermore, in addition to the media, an important role is played by certain bodies responsible to intervene when there is abuse of personal data or unethical handling of sensitive information. In the Republic of Macedonia, this falls under the purview of the Directorate for Personal Data Protection (DPDP), which will be included in the analysis as well. Special emphasis will be placed on cases from the practice in the Republic of Macedonia where privacy has (unjustifiably) suffered in favour of public interest, as well as on analysing the role of some of the actors liable to raise the alarm and protect the privacy of the personal information of those who are in greatest need of such protection—the citizens.

1

Theoretical postulates and views

1.1. The Notion of Privacy

Summarising privacy in a single definition is practically impossible. Although numerous international authors, judges, lawyers, analysts, researchers, and others have written on privacy, there is still no consensus on what exactly constitutes as privacy. Part of the reasons for this situation is that the notion of privacy may entail different things, depending on the culture of the country in question. Privacy is problematic to define on an individual level as well, therefore what is privacy to one person is not necessarily to another. Seeing privacy as every human's protected right, one might say that it is a broad concept that establishes a link between protecting a person's privacy and their relationship to society. Privacy is considered crucial to the protection of an individual's ability to develop their own views and personal relationships. Although privacy is very often seen as a person's 'right to be let alone' (Warren and Brandeis, 1890), the legal concept of privacy protection involves a wider scope of rights, including protecting the privacy of the home and family.[1]

Part of the views on privacy focus on the control over a person's information (Parent, 1983), as the ability to define the individual based on when, where and to what extent the information related to said individual is shared with others.[2] One of the more contemporary definitions of privacy is William Parent's[3] definition according to which privacy is the condition of not having undocumented information on an individual, known to or possessed by others. He indicated that he defines privacy as a moral value of people who appreciate individuality and freedom, not as a moral or legal right to privacy. According to him, personal data are facts about a person that most people choose not to disclose to others (most often data related to one's health, level of income, sexual orientation, and so forth).

The argumentation on privacy often also relies on the link to human dignity (Bloustein, 1964), intimacy (Gerstein, 1978), and social relationships (Fried, 1970), or a combination of these categories (DeCew, 1997), creating a broad framework of positions on privacy.

When it comes to privacy and human dignity, Warren and Brandeis[4] start from defining the value—the inviolate personality that is the essence of human beings, which entails individual dignity and integrity, personal au-

1 Rovsek, Jernej, 2005, The Private and the Public in the Media, Ljubljana, Institute for Contemporary Social and Political Studies.
2 Westin, A., 1967, Privacy and Freedom, New York: Atheneum.
3 Parent, W., 1983, 'Privacy, Morality and the Law', Philosophy and Public Affairs.
4 Warren, S. and Brandeis, L., 1890, 'The Right to Privacy', Harvard Law Review.

tonomy and independence. The respect of these values is the foundation on which the concept of privacy is built. Violating a person's privacy by disclosing personal data or confidential information on them, by video surveillance, or gathering sensitive personal information, is not merely an invasion of the right to privacy, but also an offence to human dignity.

In addition to dignity, intimacy is oftentimes closely related to privacy. Privacy as an essential value that is inevitably related to a person's development, their moral and social features helping them establish intimate relationships to other, relationships founded on trust.[5] Should one characterise privacy as crucial to maintaining intimate trust relationships, then it might be easier to understand why the threat to the invasion of privacy also means a threat to a person's integrity. It is privacy that allows the individual to feel free to define their relationships to others and to decide what to share with them.

Although the link between privacy and intimacy is of paramount importance to most theoreticians, one cannot fail to consider another aspect of privacy, which is the aspect of establishing social relationships. Preserving privacy is necessary to maintaining social, as well as intimate, relationships. Privacy in this sense refers to the ability to control who knows what about us, who may come close to us and find something out, and thereby to our ability to assess how we should behave in front of others with the aim to maintain and control our social relationships.[6] In this context, one might add the view of privacy as an opportunity to limit another's access to personal data, regardless of whether it is a matter of another person or an institution. According to Ruth Gavison[7], privacy may be secured in three independent, but mutually related manners, that is to say: by securing secrecy, when nobody has the information on a certain person, through anonymity, when nobody pays attention to a certain individual, and through solitude, when nobody has physical access to a person. This concept is rather complex and it underscores an important function of privacy, which is promoting a person's freedom and autonomy and the freedom in society.

The different definitions on privacy and its relation to other human and social values raise the issue of the actual scope of privacy. On the one hand, privacy is seen as an opportunity to personally choose what one discloses of oneself, and on the other, this personal choice may be considered anonymous, and privacy may be secured only by limiting the access to personal data. Nevertheless, most theoreticians believe that privacy has an exceptionally broad scope, suggesting that the relationships among various private interests and their appreciation are important for one's ability to develop a concept of oneself and one's choices.[8] Although it is very difficult to give clear guidelines on how to understand privacy and why it is important, it could be said that there is a consensus regarding the justification of the meaning of privacy as an individual interest in protecting personal data, personal space and personal choices.[9] A well-known criticism of the right to privacy is that the right to privacy should not exist, that is, that any private interest may be protected equally well with the right to property (Thomson, 1975).

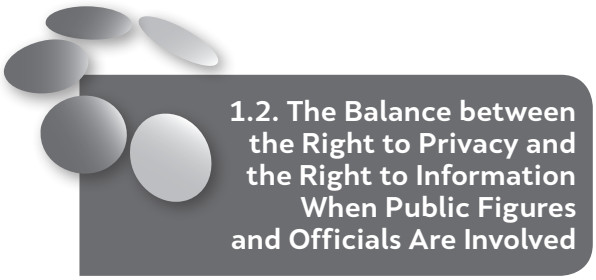
The scope of privacy is further expanded by the development of information technologies, the rise in the use of internet and the use of surveillance systems, placing in the focus of the debate the issues of individual privacy and privacy protection by the state and by society. The need to legally regulate the protection of privacy as one of the fundamental human rights stems from the fact that privacy remains a collective value conditioned by technological progress, which inevitably establishes that all individuals have the opportunity to a similar degree of privacy.[10]

In order to secure a minimal degree of protection, when creating the legislative framework on privacy protection, one must

5 Fried, C., 1970, An Anatomy of Values, Cambridge: Harvard University Press.
6 Rachels, J., 1975, 'Why Privacy is Important', Philosophy and Public Affairs.
7 Gavison, R., 1980, 'Privacy and the Limits of Law', Yale Law Journal.
8 Kupfer, J., 1987, 'Privacy, Autonomy and Self-Concept', American Philosophical Quarterly.
9 Allen, A., 2011, Unpopular Privacy: What Must We Hide?, Oxford: Oxford University Press.
10 Regan, P., 1995, Legislating Privacy, Chapel Hill, NC: University of North Carolina Press.

consider the cultural, moral and customary values of society. The relativity of privacy may be looked upon from two aspects: the first one raising the issue of whether privacy is equally valuable to all people or if its value depends on cultural differences, whereas the second aspect refers to whether certain facets of life are private by definition or not.[11] One of the difficulties when defining the field of privacy is the very idea that what privacy is is determined by the mentality in a society.

On European soil, the adopted legislative framework on privacy protection is the foundation for creating national laws regulating the area, but still, the features of every society define the principles of protecting the citizens' privacy.



1.2. The Balance between the Right to Privacy and the Right to Information When Public Figures and Officials Are Involved

When it comes to the right to privacy, as related to the right to information, as well as freedom of the media, it is very easy to conclude that they are mutually conflicting, that they stand on against the other and that one cannot exist without the other. Nevertheless, the main tendency should be towards establishing balance between these two rights.

On the one hand, there is the right to information, the citizens' interest into being informed, and the right of journalists to inform the public, which are among the postulates of any normal democratic society. On the other, there is the right to privacy protection, the right to personal data protection, and the protection of every individual's personal and moral integrity. The fact that there are numerous difficulties to finding balance between these two rights, and the manner in which they may be equally protected, suggests the need to achieve just that.

The fundamental features of democracy—the right to information, the freedom to communicate and the need for transparency—as crucial as they may be to the existence of an informed and quality debate on public policy affecting the citizens, should not eliminate the need for privacy, the right to develop one's own person, the right to develop one's own sphere of privacy and the right to the respect of one's dignity.[12]

1.2.1. The Role of the Media and Journalists in Balancing between Privacy and Informing the Public

Establishing balance between private and public interest is particularly necessary when it comes to the accessibility and public disclosure of personal data and information on the private lives of public figures, as opposed to others. The need to meet public interest oftentimes suffers from the need for exclusivity, so the media release personal, but also intimate data on public figures, as well as on individuals unknown to the public, but whose activities are in the public interest. It is the media and journalists that certainly play a key role in this process, and they sometimes have the difficult job of making sure they inform on important public interest matters without resorting to the violation of certain individual rights, such as the right to privacy. The media policy built on the concept of public interest focuses on strengthening the contribution of the media to good governance and accountability, to participatory communication, cultural pluralism and social activist. Good informedness of citizens, in turn, contributes to their active involvement in the social processes and to the democratisation of politics.[13]

Developing such media policy must rely on several fundamental prerequisites provided by the legislative and political framework of a democratic society and the general

11 Schoeman, F. (ed.), 1984, Philosophical Dimensions of Privacy: An Anthology, Cambridge: Cambridge University Press.
12 Mendell T., 1999, The Right of the Public to Know and Freedom of Entertainment, Strasbourg: Council of Europe.
13 Buckley, Duer, Mendel and O'Siochru, 2008, Broadcasting, Voice and Accountability, Washington: University of Michigan Press.

media environment, such as: freedom of expression, access to public information, media independence and pluralism, diversity of media content, media access to as broad an audience as possible, and sustainable sources of funding for the media.

Respecting the freedom of expression in a society is of fundamental significance to realising the potential of the media to contribute to good governance and to social development. Or, in other words, free media are the pillars of democracy and good governance. The right to free expression is closely related to the citizens' right to be informed, that is, the public's right 'to know.' Therefore, the role of the media is key to enabling the fulfilment of this right of the public to be informed, in order to create a comprehensive civil debate. Preventing journalists from investigating and reporting on public interest matters may seriously compromise their role in a democratic society. However, one must also bear in mind that freedom of expression is not unlimited. No country allows spreading malicious lies in order to ruin someone's reputation, and it is particularly impermissible to spread hatred based on religious, ethnic, gender or other grounds.

Journalists should differentiate between public figures 'par excellence,' that is, public figures holding political or public office, from public figures who are popular, but do not hold political or public office. If the personal data related to public figures who are not public 'par excellence' are not relevant to convey a certain piece of news and are not in the public interest, then they most often should not be released. It should be noted here that the public's curiosity might not be considered as public interest. In addition, protecting the personal data of an 'ordinary citizen' and of public figures is different. The condition to respect privacy is automatically reduced by the extent to which the individual is involved in public life or is in touch with other protected interests. In principle, the data on public figures may be released without their express consent. However, this rule is not absolute, and there are exceptions in which that should not be done.

According to one of the more exhaustive analyses of the media and the respect of privacy, conducted by the Slovenian body for protecting personal data and the free access to public information,[14] the practice differentiates between **absolute** and **relative** public figures. The former group (absolute public figures) includes individuals who are constantly in the public eye because of their function and role in society (politicians, actors, professional athletes, government representatives, etc.). The latter group of (relative) public figures consists of individuals of occasional interest to the public, on account of their association to a particular event (winners of certain events, lottery winners, criminals). The data on relative public figures may be disclosed only when there is justified public interest related to a specific event. The same goes for releasing information related to criminal offenders when the proceedings against them have been completed, or to facts that occurred long ago, since in such cases there is public interest. The sensationalism of disclosing unhelpful information may be tolerated in certain situations, both on absolute and relative public figures, but not for the purposes of violating their right to privacy, or invading their private lives.

The media's rights and responsibilities when informing the public depend on their authenticity. People have the right to be accurately informed, which will contribute to their building their own positions on social developments, thereby improving their participation in social processes and stimulating critical thinking. Although the speed of information is oftentimes very important to the media, information can be useful only if it can be trusted. This does not mean that only objective facts should be conveyed. However, in any case, the disclosed facts should be verified, and the information holder should fulfil the obligation of information accuracy. Timely verification of the information gathered—described in detail in the Code of Journalists—is not always necessary. Exceptions to the previously mentioned principle occur when the journalist discloses a certain piece of data from a state agency, for instance, at a

14 Lidija Koman Perenič and the Information Commissioner Slovenia, 2008, Media and the Protection of Personal Data, Ljubljana: Information Commissioner Slovenia.

press conference or in state agency bulletins. In such cases, the information is considered verified, and even if the information is inaccurate or if the protection of privacy has been violated, the journalist has partial responsibility to the state agency that released the information.

According the
Lidija Koman Perenič's analysis[15]:

The situation is different in the case of expressing an opinion or comment where strong subjective component is involved and it is hard to establish whether it is genuine or not. The right to express own opinion is winder [sic] than the right to information and an individual has a right to express his/her opinion even if he/she does not share it with others. However, limits exist also in this area. An opinion must not be offensive towards an individual. Each person needs to discuss in a manner fit for a civilised society and in line with good manners and behaviour. Rough discussion is not worth being protected since it is unproductive. However, a discussion may be emotional, in particularly [sic] as a response to a challenge. There is less tolerance in political discussions yet nondemocratic tone which leads to unwanted consequences cannot be supported. Politicians are no outlaws; consequently, a debate needs to be objective, cultured and needs to respect human dignity. Freedom of expression is thus limited, however, more [sic] it proves important for the public interest, fewer restrictions there are (valid also in the case of conveying facts and opinions). Adverse opinions interesting only to an individual and not the entire public yet they serve pure entertainment, contentment or pure curiosity, are not allowed. Therefore, media may publish news and opinions carefully checked and holding an objective interest even if they encroach upon individual's privacy. More [sic] these news and opinions encroach upon the right to privacy, less space they have for publishing.

15 Media and the Protection of Personal Data. Available at: http://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Media_and_the_Protection_of_Personal_Data.pdf

2

The European regulatory framework and standards

The individual rights and liberties guaranteed by the European legal documents are always described in general terms, which contributes to their broad interpretation and unclear definitions. So that there are no ambiguities in interpretation, national legislatures are obliged to further specify the provisions and offer clear implementation guidelines for the legal standards.

The right to privacy protection and the right to freedom of expression are guaranteed as individual rights in the European Convention on Human Rights and the EU Charter of Fundamental Rights.

2.1. The European Convention on Human Rights[16]

According to Article 8 of the European Convention on Human Rights:

Everyone has the right to respect for his private and family life, his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

As formulated, the article covers a broad spectrum of human rights, starting primarily with family life and the inviolability of the home, all the way to communication, and privacy is considered an integral and inseparable part of these rights.

Although not elaborated in this article in detail, the right to privacy, in accordance with the case law of the European Court of Human Rights, is interpreted quite broadly and includes: a person's physical and psychological integrity, including medical treatment, physical examinations and mental

16 http://www.echr.coe.int/Documents/Convention_ENG.pdf

health; aspects of a person's physical and social identity, including the confiscation of documents necessary to prove somebody's identity; a person's name and surname; the right to a person's image or photograph; a person's reputation; gender identity, including the right to legal recognition of post-operative transgender persons; sexual orientation; sex life; the right to establish and develop relationships with other human beings and the outside world; social relationships between settled migrants and the communities they live in, regardless of the existence of a 'family life,' or a lack thereof; emotional relationships between people of the same sex; the right to personal development and personal autonomy, even though this does not cover every public activity in which the person might want to get involved together with other people; the right to respect to the choice of becoming a parent (in genetic terms) or not; professional or business activities, and restrictions to certain professions and jobs; personal or public records or data collected or kept by security or other state agencies; information regarding a person's health and information on the risks to an individual's health; ethnic identity and the right to members of a national minority to preserve their identity and to lead private and family lives in accordance with their traditions; information on personal, religious and philosophical beliefs; search and seizure; stopping and frisking a person in a public place; intercepting communications and telephone conversations; video monitoring of public places; serious environmental pollution that may potentially affect the persons' wellbeing and prevent their enjoyment in their own homes, which might have an impact on their private and family lives, including unpleasant smells from landfills, in proximity of a prison and reaching the prison cell, which is considered the only living space available to the prisoner for years, as well as matters concerning the funerals of family members.

2.2. The Charter of Fundamental Rights of the European Union[17]

Article 8 of the EU Charter of Fundamental Rights concerns the protection of personal data and is a supplement of sorts to the European Convention on Human Rights by covering more broadly the right the privacy.

According to the EU Charter of Fundamental Rights:

Everyone has the right to the protection of personal data concerning him or her.

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. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

Compliance with these rules shall be subject to control by an independent authority.

Unlike the European Convention on Human Rights, the Charter also lays down the principles of protecting personal data aiming to establish conditions under which the processing of personal data is fair and legal. The principles of protecting personal data include: fair and legal gathering and processing; purpose limitation; necessity; reliability of personal data and their updating, and temporally limited keeping of personal data. As formulated, the article rendered in the national legislation on personal data protection compels those responsible to respect and implement the values of protecting this category of data and grants the citizens the right to personal data protection, should this right be abused. And finally, it provides oversight by independent personal data protection bodies.

17 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

2.3. Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data[18]

Directive 95/46/EC is a reference text that, on the European level, regulates the protection of personal data and lays down the regulatory framework aiming to establish balance between the high level of protection of an individual's privacy and the free movement of such data. In order to achieve that balance, the Directive imposes strict limitations on the collecting and use of personal data, and also requires that each EU country form an independent body responsible for the oversight of the personal data processing.

Generally, the Directive refers to personal data processed automatically, but also to data collected in hard copy. The Directive provisions do not cover the processing of personal data by natural persons, personal data collected for various activities in the home, as well as activities related to public safety.

As a key piece of regulation in the area, the Directive clearly specifies the principles of personal data protection that should form part of every national legislation on personal data protection.[19]

When it comes to the relationship between the right to information and the right to personal data protection, it is important to note that Directive 95/46/EC of the European Commission and the Council contains a special provision referring precisely to the media and journalists, which implies that the media and journalists are 'privileged' in terms of respecting the principles of personal data protection.

Namely, Article 9 of Directive 95/46/EC states that 'Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.'

The goal of the article, as formulated, is to provide greater protection of the privacy of the personal data subjects when their data are processed for the purposes of professional journalism.

Although extenuating, this exemption should in no way be abused by the media, but, on the contrary, they should develop media policy respectful of the fundamental rights. The media policy built on the concept of public interest focuses on strengthening the contribution of the media to good governance and accountability, to participatory communication, cultural pluralism and social activism.[20]

2.4. The Case Law of the European Court of Human Rights

In the case law of the European Court of Human Rights (ECtHR) one may come across interesting cases, that is, examples where a violation was found under Article 8 of the European Convention on Human Rights. At the same time, one may also find rulings where the ECtHR has decided that the disclosing or the storing of certain information that may be considered personal and private was legitimate. Throughout the case law of the ECtHR one may note that the Court has attempted to balance, on a case-by-case basis, between the individuals' right to privacy

18 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046&qid=1457547815346

19 Personal data must be: processed fairly and lawfully; collected for specific, explicit and legitimate purposes processed in a manner conducive to said purposes; adequate, relevant and not excessive to the purposes for which they are collected and processed; accurate, complete and updated where necessary, whereby all necessary steps must be taken to erase or correct data that are inaccurate or incomplete, with regard to the purposes for which they were collected or processed, and kept stored in such a form that allows the identification of the personal data subject, no longer than it is necessary to fulfil the purposes for which the data have been collected for further processing.

20 Buckley, Duer, Mendel and O'Siochru, 2008, Broadcasting, Voice and Accountability, Washington: University of Michigan Press.

and the legitimacy of disregarding said right in the interest of the public. This means that the ECtHR does not recognise a trend or a rationale of decision-making whereby the ruling on a certain case may be predicted. The Court determines that public interest in disclosure must outweigh the individual right to privacy, taking into account the aim that is to be achieved and considering the limitations accompanying its use.[21]

As the most notable and relevant examples in the area of the right to privacy and public interest, we may divide the cases into two groups. On one hand, cases involving the right to public information and public informing, and on the other hand, cases involving the right of the state to use, and/or collect private information. This collection of personal information is justified as prevention of violations of national security, presented as higher than individual interest. Although the theory presents numerous dilemmas as to whether this principle is truly fair, or if it is merely left to free interpretation and human rights violations under the guise of national interest, legally the principle exists and is legitimate, that is, the ECtHR adheres to it.

The ECtHR decides whether the right to privacy has been violated based on whether:

1. The petitions falls within the domain of one of the protected interests—private life;
2. The intervention was in accordance with, and stipulated by law;
3. The need for intervention is for the purposes of fulfilling a certain legitimate goal;
4. The intervention made in the case in question was necessary in the democratic society.[22]

2.4.1. Important Concepts Regarding Privacy as Defined by the ECtHR through Its Case Law

2.4.1.1. Privacy versus Public Interest

When it comes to public interest as opposed to privacy, the ECtHR takes a firm stance towards national regulation of what public interest means and the unambiguity of situations in which public interest may give institutions the right to violate the individuals' right to privacy. The ECtHR that any regulation is not sufficient so that the tracking and gathering of data by the institutions are justified. Although the ECtHR recognises national interest as crucial, the European Court rulings indicate that national regulation must simultaneously provide prevention against abuses through protection mechanisms on multiple levels regarding interception of communications and gathering data on individuals.

In the case of **Weber and Saravia v. Germany**[23], the ECtHR indicates several important segments through which it attempts to prevent the possibility of the authorities' uncontrolled power of intercepting communication. That is to say, the secrecy of interception leaves room for arbitrariness, or unfairness,[24] so in this case it states that the national legislation must clearly define the nature of the punishable acts for which surveillance may be ordered, to define the

21 Marjana Popovska, 'The Right to Privacy in the Case Law of the European Court of Human Rights', 104-105.
22 Harris, O'Boyle and Warbrick, 2009, 363, 408 and 413.
23 Weber and Saravia v. Germany, December 2006.
24 Under the principle of subsidiarity, national bodies are the first that should enable the respect of the fundamental rights as stipulated by the Convention. For this reason, as a general rule, establishing the facts of the case and interpreting national legislation are matters that fall under the purview of national courts and other institutions, whose decisions and conclusions on the facts of the case and the interpretation of the legislation are legally binding for the Court. However, the principle of effectiveness of rights, in the overall system of the Convention, means that the Court can and should make sure that the decision-making process resulting in the act that the plaintiff is petitioning against was fair and non-arbitrary.

categories of people whose communications may be intercepted, the duration, the data storing procedure, precautionary measures when using the data, and the circumstances under which they may be erased. This is necessary for preventing abuses through protection mechanisms on several levels, and not just through an independent judge.

Furthermore, the law must have such a degree of clarity and specificity that the circumstances be predictable enough so that the citizens know when their communications may be intercepted.

On the other hand, in the case **Klass and Others v. Germany**[25], the ECtHR characterised the secret surveillance as invasion of privacy. The Court in this case too stressed that national laws must provide appropriate protection against uncontrolled state interference in the individuals' privacy and that any national regulation does not suffice. In **Malone v. the UK**[26] the ECtHR once again stressed that the quality of the laws must provide protection against arbitrariness. It is in this case that the ECtHR ascertained that acquiring details on the numbers dialled, the time and duration of the calls must be regulated by clear legal rules concerning the manner and the scope of practicing discretion by public authorities.

In the case of **Shimovolos v. Russia**[27], the ECtHR found a violation under Article 8 of the European Convention since Mr Shimovolos's name was registered in a database, which involved registering a human rights activist for secret surveillance in order to monitor his movements and possibly place him under arrest. The registration was based on a minister's order that was not disclosed and made available to the public. For this reason people could not know why individuals would be registered in the base, what was the scope of information contained and how long it was stored and used, or who had control over the database. The violation was found on account of the scope, the manner of gathering and use of the data, that is, their being ambiguous and unpredictable, thereby in contravention of the provisions of the ECHR.

2.4.1.2. The Right to Privacy versus the Right to Information and Public Interest

The ECtHR once again establishes balance between these two rights on a case-by-case basis, without adopting rigid stances and a practice leading to a trend towards prioritising any of these rights. The Court has also established case law regarding the ban on censorship and the importance of public interest on the one hand, and the right to privacy and the ban on unjustified invasion of privacy on the other. Since each case carries along its own distinctive features and terms, the Court has attempted to establish balance, on account of the complexity and entwinement of these two concepts.

In the case of the **Hungarian Civil Liberties Union (TASZ) v. Hungary**[28], the ECtHR found that a member of parliament's private life was not relevant to the release of a certain piece of information treated as the right to free expression, stating that it would be fatal if politicians were able to censor the media and public debate in favour of their own personal rights. The ECtHR, through this case, made an important ruling, recognising the right to access official documents. That is to say, when public bodies have information necessary for a public debate, it would be in contravention of Article 10 of the Convention to refuse the petitioners access to this information.

The Hungarian Civil Liberties Union submitted a petition to the Constitutional Court to grant it access to a complaint by a member of parliament. The complaint referred to the constitutionality of a provision from the criminal code regarding offences involving psychotropic substances. The Constitutional Court refused to release the complaint, explaining that it contained 'personal data.'

25 Klass and Others v. Germany, 6 September 1978.
26 Malone v. the United Kingdom, 1984.
27 Shimovolos v. Russia, 2011
28 Társaság a Szabadságjogokért (TASZ) v.Hungary, 2009.

The ECtHR determined that in this case the Constitutional Court's monopoly over the information constituted a type of censorship of public interest information.

In the case of **Axel Springer AG v. Germany**[29], however, subject to review was the violation of a German actor's right to privacy by releasing photographs of his arrest for unlawful possession of narcotics at a public event.

A German newspaper published photographs and on several occasions reported on this actor's drug connections. In one report, three photographs were placed on the front page. The actor complained to the court in Germany, which ruled that the actor's privacy had been violated with the publication of the images. The court banned the publication of the news and the photographs, whereby sanctioning the newspaper. Thereupon the newspaper petitioned the ECtHR, claiming there was a violation under Article 10 of the Convention. The ECtHR found that the actor was sufficiently well-known and a public figure, stressing that the arrest took place at a public event, therefore the ban on publishing the image was in contravention of the right to freedom of expression.

This ruling of the ECtHR is of utmost importance for the established principles of finding balance between freedom of expression and privacy, in terms of:

- The contribution to the debate of general interest;
- How well-known the person concerned is and the subject matter of the report;
- The prior conduct of the parties involved;
- The manner of obtaining information and its accuracy;
- The content, form and consequences of the publication, and
- The severity of the sanctions.

Nevertheless, in cases involving the publishing of photographs of the princess of Monaco, **Von Hannover v. Germany**, one might note the fact that the Court rules on a case-by-case basis and focuses on the specific terms and facts. On two separate occasions (in identical cases), on which the ECtHR deliberated, two different rulings were made. On one occasion, the princess's privacy was determined decisive, whereas on the other, public interest 'prevailed.'

In the first case[30], the princess contested two series of photographs published in the German press, arguing that her right to privacy had been violated. The German federal courts rejected her plea. ECtHR, on the other hand, found that the disputed court ruling violated Princess Caroline's right to respect of her private life, as guaranteed by Article 8 of the Convention.

The national courts deemed Princess Caroline a public figure 'par excellence' in modern society and, therefore, had no right to privacy, except in isolated places far from the public eye. The ECtHR court considered that this standard might be appropriate for politicians holding public office, but was not applicable to this case. That is to say, 'the interest of the general public and the press was based solely on the membership of the reigning family, whereas she herself did not exercise any official functions.'

The situation surrounding the second case[31] was similar, only the photographs in questions were accompanied by texts on the poor health of Prince Rainier of Monaco, as well as the manner in which his family cared for him during his illness. In this case, the ECtHR determined that 'the articles about the illness affecting Prince Rainier III, the reigning sovereign of the Principality of Monaco at the time, and the conduct of the members of his family during that illness' constituted a matter of public interest. The Court ruled in favour of freedom of expression, finding a different purpose to publishing the photographs in this case and in the previous, in which the photographs published were of the princess (while she was at the beach).

29 Axel Springer AG v. Germany, 7 February 2012
30 Von Hannover v. Germany (No. 1), 2004
31 Von Hannover v. Germany (No. 2), 2012

3

Analysis of Macedonian legislation and standards

Although privacy as a value and a human right is guaranteed by the Constitution of the Republic of Macedonia[32], the legislative framework on protecting personal data was first defined in 2005 by enacting the Law on Personal Data Protection.[33] Adopting this law established a new concept in the Republic of Macedonia, which involves including the right to privacy in our legal system, the protection of the citizens' right to privacy, more specifically, protection of their personal data. The Law on Personal Data Protection is completely harmonised with Directive 95/46/EC, and therefore considered a modern law in line with the European standards of protecting one of the fundamental human rights.

If one regards the implementation of the standards of personal data protection from the viewpoint of establishing balance between private and public interest, then one must inevitably take into account the Law on Free Access to Public Information,[34] the Law on Media,[35] as well as the Journalists' Code of Ethics,[36] as integral parts of the legislative framework on privacy protection.

What creates dilemmas in implementing the Law on Personal Data Protection is its harmonisation of the other laws with this one. Namely, each law that provides for the gathering and processing of personal data should also include clear and precise provisions on the manner in which said data are to be protected. Amending and supplementing all laws that provide for the processing of personal data is a process moving extremely slowly. The reasons for this is the organisation and functioning of the system according to the heretofore established standards, which complicates the course of the assessment of the needs for amendments and supplements to the laws. In addition to amending and supplementing existing laws, one should certainly consider adopting completely new laws covering the sphere of privacy, their justification, harmonisation with the standards of personal data protection, as well as their impact on the everyday functioning of society.

32 Article 18: 'The security and confidentiality 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.'
33 Article 25: 'Each citizen is guaranteed the respect and protection of the privacy of his/her personal and family life and of his/her dignity and repute.'
34 Official Gazette of the Republic of Macedonia, No. 7/2005, 103/2008, 124/2008, 124/2010, 135/2011, 43/2014 and 153/2015
35 Article 6 provides for an exemption according to which the information containing personal data, the disclosure of which would constitute a violation of the personal data protection, would not be considered public information.
36 Article 3 stipulates that the 'freedom of media shall include especially: The freedom of expression of opinions; the independence of the media; the freedom to collect, investigate, publish, select and transmit information for the purpose of informing the public; pluralism and diversity of the media; the free flow of information and openness of the media for different opinions, convictions and diverse contents; access to public information; respect for human individuality, privacy and dignity (...) the independence of editors, journalists, authors and creators of contents or programming collaborators and other persons, in accordance with the professional rules of journalism.'
32 Article 7 of the Code of the Journalists of the Republic of Macedonia states that the journalist shall respect a person's privacy, unless it is in contravention of public interest. The journalist is obliged to be respectful of personal pain and mourning

3.1. Law on Personal Data Protection

The debate on establishing a legislative framework on personal data protection in the Republic of Macedonia began in 1994, when it was first proposed to adopt a law that would provide standards for personal data protection. But this proposal was not accepted, so the first Law on Personal Data Protection was enacted as late as 2005, upon the recommendation of the European Union to legally regulate this area. The legislative framework on personal data protection in the Republic of Macedonia is supplemented by the Law on Ratification of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data,[37] as well as the Law on Ratification of Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows.[38]

The Law on Personal Data Protection also stipulated the forming of an independent supervisory body—the **Directorate for Personal Data Protection** (DPDP)[39] – responsible for overseeing the implementation of the law by conducting supervisory inspections, but also by responding to requests and petitions submitted by the citizens who believe their right to privacy has been violated.

Establishing a legislative and institutional framework on personal data protection is an extremely important moment in the history of human right protection in the Republic of Macedonia, as well as an enormous challenge. The fundamental principles provided in the Law should be easily implementable in practice, regardless of whether it is a matter of processing personal information by controllers, or of developing rules and work policies closely related to protecting the citizens' privacy.

Despite the existence of complex legal regulation on personal data protection, public information in all national and foreign provisions on personal data protection falls into the category of exemptions. For this very reason, for complete and successful implementation of the legal provisions guaranteeing personal data protection it is extremely important to know how public information is (legally) regulated.

The definition in the Law on Personal Data Protection stipulates that:

'Personal data' shall mean any information pertaining to an identified or identifiable natural person; and an identifiable person is one that can be identified, directly or indirectly, particularly by reference to a citizen's personal identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

Under the law, personal data must be processed fairly, collected for specific, explicit and legitimate purposes, and processed in a manner conducive to those purposes. One must also make sure that the personal data are adequate, relevant and not excessive to the purposes for which they are collected and processed; accurate, complete and updated where necessary, whereby all necessary steps must be taken to erase or correct data that are inaccurate or incomplete. Personal data should be stored in such a form that allows the identification of the personal data subject, no longer than it is necessary to fulfil the purposes for which the data have been collected for further processing. Adhering to these fundamental principles of personal data protection is obligatory for all companies, institutions and other subjects collecting and processing personal data.

37 The Law on Ratification of the Convention 108/81 was published in the Official Gazette of the Republic of Macedonia No. 07/2005. The Convention was ratified on 14 March 2006, and it took effect on 1 July 2006.
38 The Law on Ratification of Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows was published in the Official Gazette of the Republic of Macedonia No. 103/08. The Additional Protocol took effect on 1 January 2009.
39 www.dzlp.mk

As any other law, so the Law on Personal Data Protection (Article 4-a) provides for exemptions, and one of them involves public interest as a determining factor when assessing the violation of the right to personal data protection:

The provisions of this Law shall not apply to the processing of personal data conducted for the purposes of professional journalism, only when public interest prevails over the private interest of the personal data subject.

This article further specifies the exemptions to implementing the provisions of the Law on Personal Data Protection when practicing professional journalism. Namely, the aim of the article, as formulated, is to provide greater protection of the privacy of personal data subjects when their data are being processed for the purposes of professional journalism.

The main objective of this provision is to secure prior consent from the personal data subject when processing their personal data for the purposes of professional journalism. This formulation shows that the journalists' 'privileged' position does not imply that they should not abide by the principles of personal data protection, particularly regarding Article 10 of the European Convention of Human Rights, which regulates freedom of expression and the restrictions to that freedom, and the Journalists' Code of Ethics that, in Article 7, which clearly stipulates that journalists shall respect a person's privacy, unless it is in contravention of public interest. This provision further specifies that journalists are obliged to be respectful of personal pain and mourning. The idea is to assess when public interest prevails, and when a person's private interest does so.

Generally, the balance depends on the journalist's or the editor's personal assessment of what is in the public interest when reporting on a certain issue. When making the assessment, one should take into account whether the subject reported on has legal legitimacy, or if the circumstances require the respect of privacy (Mendell, 1999). Although the Law on Personal Data Protection does not fully apply to the processing of personal data by journalists, it still does not absolve journalists from the responsibility to abide by the principles of personal data protection.

In an attempt to familiarise the media and to establish a practice of fair and impartial release of public data in the media, in 2008, the Directorate for Personal Data Protection of the Republic Macedonia put forwards specific recommendations containing the fundamental principles of protecting personal data when they are released by the media:

- Fair processing of personal data, that is, processing in accordance with the law or after obtaining prior consent from the personal data subject;
- Assessing the relevance of the information in relation to the scope of publishing personal data and establishing balance between the freedom of information and the right to privacy and personal data protection;
- Anonymising (obscuring) faces, licence plates and other personal data of the citizens;
- Mandatory (anonymisation) of the faces and other personal data of minors, and
- Publishing the initials instead of the full names of accident victims or of persons subject to criminal or administrative proceedings

These general recommendations are subject to general and special restriction. The fundamental concept is the 'relevance (importance) of the information.' Journalists must assess whether releasing personal data that form part of the news is relevant, that is, whether without releasing them the aim will be achieved and, finally, whether releasing the personal data is in the public interest or not.

Another general restriction referring to journalistic activities is the right of the personal data subject not to consent to the publication of their personal data. In cases when public interest does not prevail in disclosing a person's identity, and if said person is part of a feature story, the journalist must ask for consent to release their personal data.

Sensitive Data

According to the Law on Personal Data Protection, not all personal data enjoy equal protection. There is a category of special, sensitive data that are subject to special protection, and they are personal data revealing one's racial or ethnic background, one's political, religious, philosophical or other beliefs, membership to a trade union, and data regarding people's health, including genetic data, biometric data or data concerning one's sex life. The concept of 'information relevance' is particularly important in this case. Any mention of sensitive data should be avoided, particularly considering the fact that the Law on Personal Data Protection does not allow the processing of the special categories of personal data, barring extraordinary circumstances as stipulated by law.[40]

Protecting the Privacy of the Home or Residence

The journalist must not enter and record inside people's homes, or record hospital patients or prison inmates without their prior consent. The personal data subject's consent is a principle one must abide by. In cases when patients at healthcare facilities or prison inmates do not have full civil capacity, consent must be asked from their guardians or legal representatives.

Public Figures

Journalists should differentiate between public figures 'par excellence,' that is, public figures holding political office, and public figures who are popular, but do not hold public political office. If the personal data concerning public figures who are not public 'par excellence' are not relevant to conveying a certain piece of news and are not in the public interest, then they should not be disclosed. The condition to respect privacy is automatically reduced by the extent to which the individual is involved in public life or is in touch with other protected interests.

Persons with Illness

Medical data fall into the category of sensitive personal data, so their processing is prohibited. Data on the health of the citizens, but also of public figures, must not be disclosed publicly. The media may publish statistical information in case of an epidemic, without revealing personal data on the persons affected or deceased.

Minors

Personal data on minors must not be disclosed without proper safeguards, that is, obscuring the face, distorting the voice and using initials. Minors are persons with limited civil capacity, therefore they cannot personally give consent whether certain information on them is to be made public or not. The consent for publishing the personal data of minors must be asked from their parents, guardians or legal representatives, but even when it is obtained, one must take into account the future implications of disclosing the minor's personal data.

Persons Subject to Criminal or Administrative Proceedings

Recording and releasing information of data on persons subject to criminal or administrative proceedings is in contravention of the Law on Personal Data Protection, particularly if one also considers the failure to adhere to the principle of presumption of innocence. Public interest in investigative actions and court proceedings is great and justified, but in any case, the media must provide proper anonymisation of the persons directly involved in the ongoing proceedings.

3.2. Free Access to Public Information

The Law on Free Access to Public Information[41] in the Republic of Macedonia was adopted in 2006, and it guarantees the citizens' right to free access to the public information created and at the disposal of public and private institutions and companies. Undoubtedly, the very enactment of this law constitutes a contribution to opening the public information holders to the public, and through its implementation in the period since its enactment to this day a large amount of pub-

40 'Special categories of personal data' are data revealing one's racial or ethnic background, one's political, religious, philosophical or other beliefs, membership to a trade union and data regarding people's health, including genetic data, biometric data or data concerning one's sex life.
41 Official Gazette of the Republic of Macedonia No. 13/2006, 86/2008, 6/2010, 42/2014 and 148/2015

lic information has become available to the public. However, the assessment as to which information is public seems rather free and subjective, and the media's release of public information not always adheres to the principles guaranteed by the law.

Putting the right to free access to public information into correlation with the right to the protection of privacy perforce requires striking balance between public and private interest. Establishing this balance is difficult since it always must be done all over again, on a case-by-case basis. What is key is the assessment as to which information is of utmost importance to public interest. The Law on Free Access to Public Information also provides for exemptions to free access, one of them being the exemption concerning personal data:

Holders of information may reject a request for access to information under the law if the information concerns:

- Personal data the release of which would constitute a violation of personal data protection...

Under this provision, free access to public information is restricted wherever the release of public data would constitute a violation of the privacy of the person whose data is being disclosed. Furthermore, when it comes to free access of public information, the principle of partial access to information also applies, according to which publicly accessible are the data that do not threaten the interests of the legal and natural persons they regard.

A case from December 2015 may serve as a clear example of a type of abuse of the Law on Free Access to Public Information, that is, of a free interpretation of the exemption regarding personal data. It is a case of a media outlet, using this exemption, asking the Anti-Corruption Commission for the asset declarations of several former public officials, more precisely their first and final declarations. Upon this request, the Anti-Corruption Commission refused to disclose with how many assets the officials entered, and with how many they left the office, with the explanation that:

[t]he person under consideration no longer holds the office in question, that is, they no longer act in the capacity of an elected/appointed official, and the requested information contains personal data that are protected by law, so their disclosure constitutes a violation of personal data protection and an invasion of privacy.

This application of the exemption to free access to public information makes no sense primarily since, under the Law on Prevention of Corruption, any elected or appointed official is required to submit a declaration of their family's assets within 30 days of entering office, and then another declaration, within 30 days of leaving office. The Law stipulates that any change in assets occurring in the meantime should also be declared. Under the same law, the declaration is public, and there are no provisions for a change of status.

In addition to the legal provisions, it is of absolute importance to assess the public interest of disclosing the data on public officials' assets, whereby one could always anonymise personal data, such as addresses of real estate properties and the individuals' personal identification number.

The responsibility to ensure access to public information is shared. Primarily, the assessment of what is to be provided as public information is the responsibility of whoever initially provided the information (a public or private institution that has the status of information holder), and then of whoever releases it or delivers it to the general public. In order to strike a balance between public and private interest more easily, another mechanism has been established—the 'harmfulness test,' which is mandatory in cases when information holders allow access to information containing personal data. The harmfulness test is practically supposed to prove that releasing information containing personal data would have lesser consequences to the protected interest than on public interest, which would be satisfied by disclosing the information.

The three-step harmfulness test was introduced by the European Court of Human Rights as a guarantee of sorts of fair imple-

mentation of Article 10 of the European Convention on Human Rights. To correctly determine the restrictions to free access and the right to free expression, the Court provides a three-step test that primarily assesses: 1) Whether the restriction is provided by law; 2) Whether the restriction fulfils a legitimate purpose, and 3) Whether the restriction is necessary to justify a legitimate purpose. The three-step harmfulness test as a mechanism is included in numerous European laws on free access to public information, precisely for making establishing the balance between public and private interest easier.

3.3. The Right to Privacy versus Public Interest in Terms of Collecting Data and Intercepting Communications

Although the laws covered in this section do not directly affect the balance between these two rights, they are nevertheless extremely important to the practice and the interpretation of the notion of privacy and violating privacy in the name of public interest—even though in certain situations one might clearly establish the need to invade a person's privacy for these purposes. Despite the fact that this paper will not delve deeply into this aspect, we still believe it is of utmost importance to provide a brief overview of this facet of our legislation in the area.

In the contemporary world, intercepting communications, that is, wiretapping, by investigative bodies and the authorities is considered one of the most effective tools in fighting crime and protecting national security. This rationale leads to the belief that we should renounce our privacy for the sake of more security ('if you have nothing to hide, you have no reason to fear'). Formulated this way, the argument is difficult to dispute. At the end of the day, who would not renounce some privacy if they knew that would bring more security to themselves and the society they live in? The problem is that this distribution is hardly ever absolute, and renouncing one right does not lead to greater enjoyment of the other. That has, in fact, been demonstrated by the example of Edward Snowden, who sparked a worldwide debate on the invasive methods used by the world intelligence agencies to violate the citizens' privacy under the justification that they do it for 'national security.' Hence, this guiding formulation when adopting laws on intercepting communications is subject to controversial interpretations and abuses that unseldom violate individuals' human rights and privacy.

The laws covered in this section are: the **Law on Electronic Communications**[42], which focuses on multiple sectors, that is, regulates anything related to providing conditions for the development of electronic communications, competent supervisory bodies, operators' competences and responsibilities, etc.; the **Law on Interception of Communications**[43], regulating the terms under which the right to privacy may be ignored for higher purposes, that is, for national security, and the **Law on Protection of Privacy**[44] enacted in 2015, as a result of the scandal with releasing public officials' intercepted telephone conversations of public officials that revealed alleged crimes in contravention of public interest.

3.3.1. The Law on Electronic Communications (LEC)

Chapter 18 of this Law regulates the security and the integrity of public electronic communication network and services, as well as personal data protection. What is distinctive about the LEC is that it specifies a series of responsibilities for telecommunication operators regarding the providing of conditions to intercept users' communications and allowing access to users' data to the competent authorities.

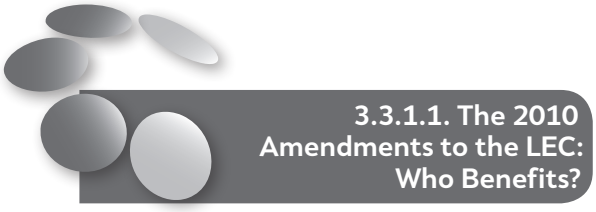
42 Official Gazette of the Republic of Macedonia No. 39/2014, 188/2014, 44/2015 and 193/2015.
43 Official Gazette of the Republic of Macedonia No. 121/2006; 110/2008 and 116/2012.
44 Official Gazette of the Republic of Macedonia No. 196/2015

Namely, under the Law on Electronic Communications operators are obliged to provide all necessary technical conditions enabling interception of communications in their networks. Operators are required, at their own expense, to supply and maintain equipment, appropriate interface and to set up electronic communication channels for transfer to the agency authorised to intercept communications, in order to enable interception of communications in their network.

The operators are obliged to provide the agency authorised to intercept communications with real-time interception of communications. The information on the intercepted communication should be made available immediately after the communication has ended, and the interception of the communication should be uninterrupted throughout the duration. The operators also have the responsibility to provide an accurate and unequivocal link of the information on the intercepted communication with the content of the communication being intercepted.

This law has recently been subject to criticism by the international community, for the excessive jurisdiction for intercepting communications provided to the security services. On piece of criticism formed part of the Recommendations of the Senior Experts' Group of the European Commission of June 2015, stating that:

Acting on the basis of Articles 175 and 176 of the Law on Electronic Communication, each of the three national telecommunications providers equips the UBK with the necessary technical apparatus, enabling it to mirror directly their entire operational centres. As a consequence, from a practical point of view, the UBK can intercept communications directly, autonomously and unimpeded, regardless of whether a court order has or has not been issued in accordance with the Law on Interception of Communications.[45]



3.3.1.1. The 2010 Amendments to the LEC: Who Benefits?

The above criticism of the LEC refers to several controversial provisions of the Law adopted in 2010, granting the competent authorities excessive jurisdiction and power to intercept communications. One of the articles in the 2010 amendments stated that public communication network operators and public communication service providers are obliged to provide the agency authorised to intercept communications **constant and direct access to their electronic communication networks, as well as conditions to autonomously download traffic data**.

After the enactment of these amendments proposed by the Government of the Republic of Macedonia, the Constitutional Court ruled that this paragraph constituted a violation of the right to privacy, since the competent authority is not obliged to respect procedure, that is, obtain a court order, by the very fact that it has direct access to users' communications. Paragraphs 7 and 8 of Article 112 of the amendments granting the competent authority direct access was declared unconstitutional on 15 December 2010.[46]

The LEC saw comprehensive reform in 2014 (Official Gazette of the Republic of Macedonia No. 39/2014). Part of the new provisions of the law once again grant jurisdiction to the competent authority to directly intercept communications, whereby the **operators are obliged to provide transfer**. Although the language (as compared to the 2010 amendments) was modified, it is nevertheless troubling that the Law provides for transfer of communications by the operators **to the competent authority without prior**

45 Recommendations of the Senior Experts' Group of the European Commission, 8 June 2015, 5-6. See:
http://ec.europa.eu/enlargement/news_corner/news/news-files/20150619_recommendations_of_the_senior_experts_group.pdf

46 Constitutional Court ruling (C. No. 139.2010) on the 2010 amendments to the LEC: The Court found that the contested provisions of the Law do not include sufficient safeguards against possible abuse by the competent authority with the provided technical capability to continually and autonomously intercept the content of the communication, as well as when collecting the necessary data regarding the communication in question. In addition, the provisions regulating the area of surveillance must be sufficiently precise and predictable, not to be subject to improvisation and interpretation, so that they do not constitute a threat of surveillance to anyone to whom the law may apply, and not to violate, in an unconstitutional and unlawful manner, the respect of the citizens' right to correspondence and freedom of communication. (...) Therefore, according to the Court, the contested provisious of the Law, on account of the imprecision of the wording used, the insufficient regulation of the terms and the procedure during which there might occur a departure from the constitutionally guaranteed right to privacy, constitute a real threat of willful and arbitrary interference of state agencies in the citizens' private lives and correspondence, which may negatively reflect on the citizens' honour and reputation, without real foundation in the Constitution and the laws. For these reasons, the contested provisions cannot be interpreted as provisions guaranteeing the fundamental human rights and liberties of the citizens recognised by international law and specified in the Constitution as a fundamental value of the constitutional order of the Republic of Macedonia.

obtaining a court order. That is to say, the amendments that had provoked enormous backlash in 2010 and were declared unconstitutional, in the new LEC were reintroduced in a new form and allowed the same, if not greater invasiveness as the unconstitutional amendments.

It is unknown whether the repealed amendments have affected practice, that is, whether the already installed technology allowing the competent authority direct access to communications has been removed after the Constitutional Court's ruling that the measure is unconstitutional, or if in the period since the measure was rescinded—between 2011 and 2014—the competent authority has still had direct access. In his newspaper column 'Occam's Razor on the Wiretapping,' Novica Nakov remarked that:

Articles 175 and 176 of the Law on Electronic Communications have been in effect since February of 2014, when the cited Law on Electronic Communications (Official Gazette of the Republic of Macedonia No. 39/2014) was adopted. However, as we could hear from the recordings and learn from journalistic analyses, the conversations were conducted in different periods, and there are recordings dating back to 2011. How could these recordings be made if the DSC at that time was not allow to 'directly mirror their entire operational centres'?[47]

On the other hand, there is also problem with the oversight of the legality of implementing the measure. That is to say, the operators are not obliged to request and establish the existence of a competent court order allowing the competent authority to implement the measure, nor are the operators obliged to check or control the interception of communications. Their only obligation is to provide technical condition for its implementation.

Although the Agency for Electronic Communications (AEC) should be largely competent of the oversight of implementing the measure of intercepting communications, the Law provides that the AEC intervene only in one specific situation. Vladimir Ristovski, advisor to the AEC director, once stated that, under the law on the Agency's remit and under Article 175 of the LEC, the Agency is obliged to and may intervene with the authorised body or with the telecommunication operator in Macedonia only if there are problems with their cooperation. This cooperation refers to whether, for instance, the operator has provided the appropriate interface (interconnecting the technology on both ends) and the necessary equipment. 'The Agency performs oversight only if one of the parties involved informs us that cooperation is lacking. Otherwise, we do not perform oversight.'[48]

According to Article 6 of the Law on Interception of Communications: 'The person whose communication was intercepted has the right to challenge the authenticity of the data collected and the legality of the procedure of interception of their communications, in a procedure determined by the Law on Criminal Procedure.'

However, this too is problematic, since the interception of communications is conducted in secret and operators under the LEC are obliged to ensure that the person does not notice that their communication has been intercepted. Then how could said person contest the authenticity? Of course, it is provided that the person contest them if they are used in proceedings against them, but problems arise when the suspicions that would justify intercepting somebody's communications turn out to be wrong. In that case the competent authority is under no obligation to inform the person of the surveillance, whereby the individual will not be aware that their privacy has been violated.

There is no real control over the secret security services anywhere in the world. Name one

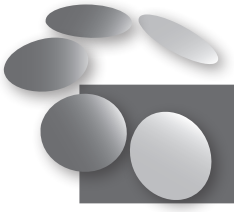
47 Novica Nakov, 'Occam's Razor on the Wiretapping' (newspaper column), 4 July 2015. Available at: http://www.makdenes.org/content/article/27108823.html
48 Goran Naumovski, PlusInfo, 'AEC: We Intervene If There Is a Problem between the Ministry of the Interior and the Operator, We Do Not Control If There Is Unauthorised Wiretapping', 13 February 2015.

example of a parliament that has such control. Yes, based on their constitution and the legislation, numerous countries have established mechanisms of civil control over the work of the security services, but in practice, such control is implemented either very little or not at all. Particularly in the area of violating human rights through implementing interception of communications. That is why I believe that this control acts merely as democratic décor.[49]

Another segment worthy of attention is the retention period of the personal data that operators are obliged to store. These data include the identity of the caller, the registration list, name and address of the telephone number's owner, the PIN or password when a SIM card is used, the Internet connection, IP address, date and time of the calls, the location at the moment of the call, etc. According to the law (under Article 178, Paragraph 1 and 3 of the LEC), operators are obliged to retain these data up to 12 months. In comparison, most countries of the European Union most often adopt the minimal data retention period of 6 months, in order to respect the safety and secrecy of personal data.

Also troubling is the obligation under the Law (Article 176) to store electronic communication data that have not been obtained as a direct result of a surveillance order, but from the everyday communication of the users' telephones, that is, call lists, location, and so for. Although this measure is provided for the prevention of crimes and safeguarding the country's security, it nevertheless veers into the domain of mass surveillance, which is subject to abuses regarding the individuals' privacy.

The only reaction from operators about this problem concerns the increased costs for the necessary technical preparation to meet the particular specifications needed for these measures. There has been no voicing of concern about this measure and the excessive invasion of the individuals' privacy.



3.4. The Law on Interception of Communications[50]

Although it is a fact that intercepting communications is one of the most effective methods the authorities may use to uncover or prevent crime, or to protect national security, this method is also the most invasive of individuals' privacy. It is required that, if this method is used, it must be under safe and clear supervision, in order to prevent abuses and excessive use, which would constitute a human rights violation.

The Law on Interception of Communication regulates, as stated in Article 1: the procedure of intercepting and recording telephone and other electronic communications, as well as the manner of handling, storing and using the data obtained by interception. That means that this law regulates the cases in which the right to privacy, that is, to private communication is not exclusive, i.e. the cases in which it may be disregarded. The law regulates the capabilities of the competent authorities for intercepting communications to secretly learn the content of a specific communication and to create a record, that is, store the communication in a base with the possibility to reproduce it.

All this suggests that under this law, the public prosecutor, the Ministry of the Interior, the Financial Police Office, the Customs Administration and the Ministry of Defence, under certain conditions are allowed to disregard the individuals' right to privacy and secretly learn the content of the information they share. Of course, competent authorities do not have the exclusive right to invoke this Law, that is, as stated above, certain conditions must be met for this procedure to be legitimate.

49 Pavle Trajanov's statement, Katerina Blaževska's news article, 'Control of Wiretapping Equals—Zero!', Deutsche Welle, DW, 13 October 2014.
50 The notion of communication implies any type of telephone or electronic communication, that is, any process that involves the use of a device to transfer or receive information between two or multiple parties. It is not limited to two or more individuals communicating, but also includes the communication between an individual and a certain web page. That is to say, the very web page visit constitutes communication using an Internet protocol.

The Law specifies two areas in which competent authorities may use the right to intercept communications, those being: (1) detection or prosecution of perpetrators of criminal offences, or (2) safeguarding the country's security and defence interests.

Under the Law, the court may authorise the interception of communications in the following cases: preparing a crime against the government, against the armed forces or against international law and humanity. It may also authorise it if someone prepares, initiates, organises and participates in an armed attack against the Republic of Macedonia, or in incapacitating the defence system and preventing it from performing its function—when the data on such activities cannot be obtained in another way, or their obtaining would involve great difficulty to prevent the carrying out of the armed attack or the incapacitating of the defence system.

What is problematic in this law is the possibility for the court to grant an oral order for intercepting communications. Under Article 11-a, in emergencies, when there is danger for causing irreparable harm to the successful conducting of the criminal proceedings, the judge in a prior proceeding may grant an oral order whereby authorising interception of communications for a period of 48 hours, based on an oral request for intercepting communications submitted by the competent public prosecutor. This article merely expands the communication surveillance jurisdictions, where the competent authorities may be authorised without a written court order.

It is a troubling fact that the only mechanism, supposed to be protective against abuses of this measure, in certain cases is reduced to an oral order. Particularly if one considers the sensitivity of this measure and the need for a clear and concise procedure and oversight of said procedure. Would the judge who would grant the oral order be able to exercise any real control over the legitimacy of the measure?

This possibility provided by the LIC was troubling as early as 2010, when the LEC was amended, and the lack of control over the interception of communication was also noted by Prof. Gordan Kalajdžiev, PhD (2010):

As it stands, for the time being there is absolutely no possibility for anyone, not even the courts, the prosecutor's office, and the parliamentary committees, to exercise any real, regular and effective control over the actual scope of the wiretapping.[51]

The fear articulated in the very reactions to the amendments to the Law on Electronic Communications that were declared unconstitutional may be reflected in the current Law on Interception of Communications.

So there are no guarantees that someone controls how the procedure is conducted, how authorisation is granted and, subsequently, how one stores the information that law enforcement obtained during the interception of communications.[52]

Apart from the emergency measure of oral court order, in order for competent authorities to be granted authorisation to intercept communications, the procedure is as follows: The public prosecutor submits a request to a competent court, on the prosecutor's own initiative or on the initiative of the other competent authorities. Upon receiving approval, the competent authority may proceed to intercepting the communications. And all this only if there are **indications**, i.e. findings and evidence on which suspicions are based, but also an explanation of the reasons for which the data or evidence **cannot** be collected in another manner of detecting or prosecuting a perpetrator of a criminal offence or of safeguarding the country's security and defence interests.

In the chain of control and oversight over the implementation of the measures of intercepting communications, what is also alarming is the rate of approved requests for intercepting communications submitted by the com-

51 Gordan Kalajdžiev, 'The Erosion of Privacy in the Republic of Macedonia', On the Amendments and Supplements to the Law on Electronic Communications, 2010.
52 Statement by Uranija Pirovska, Helsinki Committee for Human Rights, Slaǵana Božinovska, 'The Law on Interception of Communication Breeds Fear', Radio Free Europe, 8 June 2012.

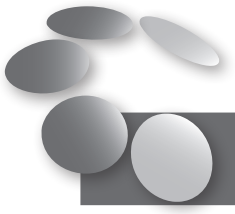
petent authorities. The court of first instance has never rejected such requests, regardless of their nature, which is a troubling fact in itself. The research entitled *Communications Interception Oversight in Macedonia* conducted by the Analytica Thinking Laboratory notes:

Statistical data reveals a worrying trend that the courts are completely aligned with the Ministry of Interior, when interceptions of communications are requested. With a rate of 100% approvals, Primary Court Skopje 1 has not found any request for interceptions to be inadequate. Questions are raised regarding the expertise of the judges to assess potential security threats and grounds for suspicions, but there are also concerns about the independence and impartiality of the judicial power.[53]

This research by Analytica has concluded that the court has granted an interception order to every request submitted by the competent authority. If the courts are completely aligned with law enforcement and the communication interception requests, one must ask whose interests are being safeguarded by this manner of decision-making, and whether the authorities competent to protect the citizens' rights really consider public interest when making a decision. What is the role of the court if it does not conduct a proper assessment of the need for intercepting communication, but only issues orders upon every request? How many of these requests have been truly legitimate, and how many have been approved only because of the court's incompetence (or bias to other interests)?

The lack of protection mechanisms when implementing the measure of interception of communications may also be noted in another ludicrousness of the Law.

The legislator provided for ongoing control and oversight over the practical implementation of the measures by the competent public prosecutor, which is not a functional solution, considering that the public prosecutor has broad jurisdiction in the procedure of proposing and extending the implementation of the measure. That gives rise to a founded suspicion that the public prosecutor is subject to a conflict of interest of sorts, and in this situation does not constitute an impartial subject for exercising control and oversight over the practical implementation of the measure. In addition, the Public Prosecutor's Office has developed not merely a partner, but a subservient relationship with the Ministry of Internal Affairs, and shows no great enthusiasm about controlling law enforcement.[54]



3.5. Law on the Protection of Privacy

This Law was adopted in November 2015, in a calm atmosphere, without much reaction, even though it had been preceded by rather controversial circumstances related to the political developments in the Republic of Macedonia at the time, concerning the audio materials released as 'bombs' by the opposition, through which the issue was raised of the unlawful wiretapping of telephone conversations and the invasion of privacy of, allegedly, thousands of people, including members of non-governmental organisations, journalists and public officials.

Before the enactment of the privacy law as a result of an agreement among the political parties, another bill was submitted to the Assembly of the Republic of Macedonia, namely, the Bill Prohibiting the Possession, Processing, Releasing and Handling of Materials Resulting from Unlawfully Intercepted Communications. Although these two laws are seemingly different, upon comparison, one might conclude that the context is rather similar, even if one bill was met with fierce backlash, whereas the other was enacted in a calmer atmosphere.[55]

53 Bogdanovski, A., Lembovska, M., 2015, Communication Interception Oversight in Macedonia: Making the Impossible Possible, Skopje: Analytica Thinking Laboratory.
54 Helsinki Committee for Human Rights of the Republic of Macedonia, 'Control over Wiretapping—Who Will Guard Us from the Guards?', Quarterly report, December 2011-February 2012.
55 Mirjana Najčevska, a column published on the Okno web portal, 'The Law on the Protection of Privacy—When the Constitution Turns into "Toilet Paper"':
'Some of the media conveyed positions that the overall Pržino Agreement might be called into question on account of this bill, and withdrawing the bill from parliamentary proceedings is linked, among other things, to the need for its harmonisation with European standards.'

What is most critical about this Law is Article 1, Paragraph 3, stating:

The possession, processing, public disclosure and disposal in any way, shape or form of material arising from the unlawful interception of communication carried out in the period between 2008 and 2015, including the usage and disposal thereof in the electoral process and for political and other purposes and procedures shall also be banned under this Law.

It is difficult to find solid argumentation for the existence and the enactment of this law, considering that it provides for measures valid only in a specific time period. Why this particular period, and was the possession, processing and releasing of materials resulting from unlawful interception of communication tacitly allowed, that is, not expressly prohibited? These are just some of the questions deserving an answer, but the answer has not been provided (yet).

Under the law, the restrictions only pertain to recordings in the private domain, but the law does not specify what 'private domain' means. Furthermore, although the law regulates matters in the public interest, at no point does it take into account the explanation of what it constitutes, or where the public interest is in this context.

3.6. Whistleblowers and Public Interest

When discussing the public's right to be informed, it is inevitable in this context to reflect on the relevance of the so-called 'whistleblowers' (or 'disclosers' under Macedonian law) in contemporary democratic societies. Although there is no generally accepted definition of whistleblowers, the term most often refers to persons believing that public interest is more important than the interests of a certain organisation or institution. Hence, they 'disclose' cases of serious corruption in the private or the public sector (most often in the organisation or institution where they work), or other abuses harmful to the public interest or in violation of human rights. Whistleblowers are particularly important in societies that do not foster appropriate safeguarding of the right to free expression and societies with oppressive government structures. Still, even in certain societies deemed more democratic, whistleblowers enjoy a reputation of 'informants' or traitors who are disloyal to their employers, institutions, or their country. The most renowned 'whistleblowing' example was the 2013 case of Edward Snowden, who exposed the methods of the intelligence services in the US and Europe, through which they (unlawfully and unconstitutionally) invaded the citizens' privacy (under the guise of public interest).

It is because of the importance of whistleblowers to public debate and of ensuring greater accountability from public and private institutions that it is crucial to provide effective legal protection for these individuals. Moreover, it is necessary to properly educate the companies and state institutions on the importance of whistleblowers, to provide an environment where they could speak freely, without risking negative work-related consequences (such as getting fired or having their salaries or remunerations reduced).

Macedonia does not have a wealth of experience with cases of disclosed corruption by concerned employees of an organisation. This is partly due to the fact that citizens hesitate to speak publicly about such phenomena for fear of repercussions. One of the findings of the research[56] conducted by the Foundation Open Society-Macedonia was that over a quarter (28%) of citizens (surveyed) do not request information from public institutions, believing that they would not get the information requested and that state institutions are generally closed to the citizens.

It is particularly important to stress the need for protecting whistleblowers in the public sector, considering the lack of openness and transparency of state institutions in our country. The Freedom House freedom of the press country report on Macedonia (Freedom House: 2015) notes that the

56 http://www.soros.org.mk/CMS/Files/Documents/istrazuvanje-tajnnost-vo-rabotenjeto-mkd-1.pdf

Law on Free Access to Public Information 'is unevenly and selectively enforced, with officials delaying responses and shunning independent or critical media outlets.' The research on the transparency and accountability of public institutions in Macedonia,[57] spearheaded by Transparency International Macedonia (2012), has been indicative in this aspect. As part of the research, a survey was conducted, according to which over 70% of citizens surveyed believe that corruption is most common in those sectors of the administration closest to the 'power holders.' One of the conclusions in the report is that in all likelihood 'people will decide not to report corruption because of fear and lack of trust in the institutions which [sic] should protect them in such cases.'

In November of 2015, the Assembly of the Republic of Macedonia enacted the **Law on the Protection of Whistleblowers** (Official Gazette of the Republic of Macedonia No. 196/2015) as part of the reform package stipulated by the Pržino Agreement reached in June 2015. The Law provides protection in cases of disclosing unlawful activities threatening public interest in state institutions, as well as in private companies, and its implementation was to start four months after its enactments. Under the Law, a 'whistleblower' may be any employee, job applicant, intern or individual hired on any grounds.

Despite the well-regulated whistleblower protection, the Law contains several provisions whose practical implementation might be problematic. In particular, there are three areas where there is room for further improvement.

Protection in Cases of Public Disclosure: Although the Law provides for protected public disclosure (Article 6), protection is afforded only when the 'whistleblower' has already made internal disclosure (inside the employer organisation) or external disclosure (in certain state institutions), but there is no protection provided for public disclosure in the media. If the whistleblower reveals information directly (publicly) without making the above types of disclosure, they have no right to protection against repercussions in the institution in which the disclosure was made, nor right to protection before a competent court.

Under the principles for whistleblower protection specified by Transparency International[58], whistleblowers should enjoy protection (judicial, and protection against negative workplace consequences) even when they disclose criminal offences or unlawful activities directly in the media, civil society and other organisations.

In the case of **Guja v. Moldova**[59], the ECtHR noted that government actions or oversights must by subject to direct supervision by the media and the public, whereas in the case of **Heinisch v. Germany**[60], it stressed that 'the public interest in being informed about the quality of public services outweighs the interests of protecting the reputation of any organization.'

Independence of Internal Disclosure Channels: In its current form, the Law stipulates that the whistleblower discloses to the person authorised to receive such complaints within the organisation where the disclosure is made, or, if no such person exists, to the managing officer of the organisation. As a result, institutions may use this to identify whistleblowers and to attempt to discourage them from disclosing, or to press charges against them before they make the disclosure. The individuals and bodies authorised to receive whistleblower complaints should be independent and have the power and resources to act on the information received, and not be appointed 'pro forma.'

57 http://www.osce.org/mk/skopje/104549?download=true
58 https://www.transparency.org/files/content/activity/2009_PrinciplesForWhistleblowingLegislation_EN.pdf
59 Application No. 14277/04
60 Application No. 28274/08

4

The role of the media in balancing privacy with the public interest

What makes the relationship between the right to privacy and the public's right to information particular is that these two concepts are intertwined and often contradict one another, depending whose interests are on the line. On the one hand is the citizens' interest to be supplied with true and clear information, whereas on the other is the protection of privacy, that is, of personal data and the individuals' integrity.

The media/journalists are obliged to inform the public, to present the real and accurate information concerning the environment in which their readers and viewers live. In theory, it is the reporters who, through investigative journalism, are required to reveal to the citizens the truth on public interest matters. However, in order to do their job, the media must not disregard the right to privacy. What makes the journalists' job more difficult is the intricacy of striking a balance between informing the public and the privacy of the concerned parties subject to media reporting.

The right to privacy is quite disregarded in the Republic of Macedonia. Although there are quality and extensive legal provisions for personal data protection, we have nonetheless witnessed numerous recordings used in the media that clearly disclosed information that is defined as the concerned parties' personal data, and the same information, if obscured, would not undermine the purpose of the reporting and the bottom line of the news. The media often do not consider the effect they exert on the public with this informing practice, and one example of this is the failure to obscure the faces of persons under arrest and the use of their full names before they are convicted—even though they are not public figures—whereby violating the principle of presumption of innocence and giving the public misleading impressions.

The governing concept for journalists should be the importance and relevance of the information they release; that is to say, whether the information that might invade an individual's privacy is necessary, or if it will affect the informing purposes. If the information constituting personal data or part of the individual's privacy does not affect the fulfilment of the purpose of the news, then it should be omitted. However, another significant factor is the balance between the information whose release invades an individual's privacy and the public interest in releasing said information.

In theory, there is a dilemma when it comes to the privacy of public figures and the information that is part of their privacy, but is in the public interest. That is to say, whether, if certain information that is part of a politician's privacy, but contradicts certain views that he has been advocating publicly and that helped him win the people's votes, it is part of the public interest or remains protected as part of his privacy. A simple hypothetical example would be the following: A health minister has publicly stood against abortion and promoted pro-life views, but the information has surfaced that she had once had an abortion. Is this event from her private life in the public interest? And will the journalist who has obtained the information from their own sources act unlawfully is they release it?

Or, if we consider another hypothetical example: Does a journalist, if they learn that a politician who has initiated the enactment of a law prohibiting the public promotion of homosexuality, and has won the people's support partially for his statements against homosexuality, and is himself homosexual in his private life, have the right to disclose this information?[61]

In truth, there is no specific and clear definition of what public interest is, nor is there a uniform conclusion as to when the interest of a larger number of people should be placed above an individual's privacy interests. Is sensationalism rousing the interest of a large number of citizens justified, or does the information play no part in improving or affecting the interest of most intrigued parties? That is to say, the curiosity of an actor's fans about their private life is not a legally justified reason to release to the public information from that person's privacy. If, however, the information pertaining to said actor's life is in the public domain—for instance, involving lobbying on certain social or political inclusion issues—and yet is private in nature, then it would be treated differently, that is, as public interest information.

Technological progress and the digitalisation of personal information have complicated the situation further in this respect. The sharing of personal data by public figures on their social media profiles is a new conundrum for the balance between the right to information and the right to privacy. That is to say, there is a trend with celebrities promoting certain facets of their private lives on social media, while at the same time fighting for protecting other parts of their privacy in the courts.

As stated in a research conducted in the United Kingdom,[62] while most people regard 'what happens on blogs or social network sites such as Facebook as semi-private, journalists see it as information in the public domain.' The authors argue that it is not entirely clear in which situations the emphasis is on privacy, as the courts have become stricter, and in which on the right the information, so they recommend a device called an 'impact test,' that is, a tool that is to help journalists make a decision on releasing information pertaining to the individuals' privacy. The tool involves asking oneself whether by disclosing the information one would be 'exposing issues which have the potential to impact the lives of a number of people rather than simply being interesting to the prurient.'

Another dilemma is to what extent the information that people post on their social media profile is public and accessible to usage and release by third parties. If a post has a 'public' setting, could it be considered acceptable to (re)post it without obtaining prior permission from the person that originally posted it on their profile?

When it comes to posting photographs on Facebook, it is a common belief (by reason of ignorance of legislative regulations) that every user, by posting the photographs, has given consent to have them publicly shared on the Internet. However, a photograph constitutes a piece of biometric personal data that fall into the category sensitive personal data, and enjoying a special degree of protection, so it cannot be process without the personal data subject's consent or without legal grounds. The user's consent to post their own photographs on their private profile, regardless of their user reach, does not imply the consent to have them reposted on other web pages or media. However, if they are posted using the 'public' setting, there are different interpretations on the legality and legitimacy of posting the photograph without prior consent.

On the other hand, the question arises of how much the law can protect the individuals' privacy in a situation of 'playing catch-up' with technological progress and the rise of the number of tools allowing for instant sharing of personal information that might threaten the individuals' dignity and integrity. The rapid development of certain services that pay too little attention to actually protecting their users' privacy is a subject matter that is not sufficiently prominent in public debate in general, and even less so in the Republic of Macedonia.

61 An Australian transport minister who created a public image of a family man invested in his home life, after the information surfaced that he had attended a gay club, resigned from office with a public apology to his family.
http://www.theaustralian.com.au/national-affairs/state-politics/minister-caught-at-gay-club-david-campbell-resigns/story-e6frgczx-1225869390970
http://stephanieleewilliams.blogspot.mk/2011/09/privacy-vs-public-interest-publics.html

62 Stephen Whittle, Glenda Cooper, Reuters Institute at Oxford University, 'Privacy, Probity and the Public Interest', 8 July 2009.

5

Cases from Macedonian practice

In order to assess whether the media in the Republic of Macedonia are mindful of the manner of releasing public data on the individuals subject to media reporting, the following questions should be answered: 1) Are the personal data on the individuals subject to media reporting crucial to the news, and is the scope of disclosed public data appropriate to achieving the effect of the news? 2) When releasing personal data, has it been made sure to anonymise the individuals, particularly when they are minors, accident victims or persons subject to criminal or administrative proceedings?

Unfortunately, for the sake of exclusivity, the media often happen to release data that are not only irrelevant to the news, but also reveal details of the private lives of the persons subject to media reporting. Furthermore, it has become increasingly common to use social media as sources of information, so it is very easy for someone's private life to become part of a media feature story. In addition, the media have not established clear rules on the technical processing—anonymisation—of the materials they release, if they contain personal data.

Moreover, there is a general problem about releasing information that the media have obtained from the institutions, such as information on suspected or arrested individuals, the disclosure of which not only violates privacy, but also the principle of presumption of innocence. It is also important to note the reporting during coverage of court proceedings, which may often reveal data on the private lives of the persona involved in the proceedings that are not of vital importance, considering the fact that the reporting takes place in the course of the proceedings themselves.

The media's responsibility to fairly process personal data should not merely be an obligation imposed by law, but a responsibility to abide by the rules that every media outlet should establish in order to assess more easily which information is in the public interest, and which one crosses the line and constitutes a violation of the right to privacy. In the interest of comprehensive and accurate informing on events involving human suffering and disasters, the media are obliged to strike a balance between public interest and the privacy of the citizens, as well as respect their human dignity.

5.1. Case Study: 'Sex Workers'

In 2008, the media released the news that, in consultation with the prosecution and the courts, pursuant to a court order, there was a medical examination conducted of 22 individuals—sex works—in order to confirm, or dismiss, the suspicions that they were carriers of venereal or viral infections, which they were intentionally transmitting to the persons they engaged in sexual contact with.

The news appeared on all the media, supported by photographs and video footage of the police raid itself. Apart from not com-

pletely focusing on the importance of the information, these feature stories did not take appropriate measures to protect the sex workers' personal data. In the features, the sex workers' faces were clearly visible and their voices recognisable, allowing for their direct identification. The face and the voice are biometric personal data, whereby they fall into the category of sensitive personal data enjoying a special degree of protection. Revealing the faces and voices without their obscuring and distorting constitutes disclosing personal data in a scope excessive to the purposes of the information.

Moreover, medical data fall into the category of sensitive personal data, so their processing is prohibited. Data on the citizens' health cannot be released to the public. The media may publish statistical information in case of an epidemic, without revealing personal data on the persons affected or deceased.

The news of the arrest would not lose any substance and would have the same effect if the faces of the arrested individuals had been obscured.

5.2. Case Study: 'Serial Killer'

The case with the serial killer compared to Raskolnikov received enormous media attention, and there was unquestionable public interest in the institutional resolution to the case. Following the suspect's arrest, a media outlet—in an attempt to profile the individual—aired an 'exclusive' feature story in which, in addition to reporting on the arrest of the serial murder suspect, they filmed his home and tried taking a statement from his mother who, as is clearly visible on the footage, refused to make a statement, or even allow the television crew in her home. The address of residence in this case is considered a piece of personal data, since, correlated with the other data released in the feature, it directly identifies the suspect, and indirectly his mother. Entering the yard of the house and filming without the mother's consent constitutes an invasion of privacy, particularly since the video clearly shows the suspect's mother expressly refusing to be filmed.

Obtaining the personal data subject's consent is among the fundamental principles of personal data protection, which must be adhered to during every release of personal data by the media. Moreover, the segment of the story featuring the footage of the suspect's home and of his mother's current situation does not contribute to the quality of the information and does not pertain to its substance, or relevance, therefore it may be treated as excessive disclosure of personal data.

5.3. Case Study: 'Snake Eye'

One of the largest mass arrest police operations is the 'Snake Eyes' case, in which approximately 70 toll booth attendants suspected of receiving bribes, handcuffed, were filmed in the course of the raid, and the footage was integrally broadcast by the media.

The feature stories might be said to focus on the relevance of the information, but no appropriate measures were taken to protect the arrestees' personal data, that is, their faces were not obscured, allowing for their direct identification. The face is a biometric piece of personal data subject to a special degree of protection. Revealing some of the arrested individuals' faces constitutes disclosure of personal data in excess of what is necessary to the purposes of the information. The news of the arrest would not lose any substance and would have the same effect if the faces had been obscured. In this case, the principles of personal data protection were not applied.

Fighting corruption is a matter of considerable public interest and the public has the right to be informed on how the state deals with such cases. However, revealing personal data before guilt is proven cannot be justified by public interest. When deciding on the acceptable level of encroaching on individual rights, public interest is the main criterion.

This case is particularly important, considering the fact that in the course of the criminal proceedings over half of the individuals arrested were cleared of suspicions of receiving bribes, but remained publicly tainted by revealing their faces in the media.

5.4. Case Study: 'Daughter of a Politician'

Using Facebook as their primary source of information, several web portals published the photographs of a politician's daughter, as well as the location and the date they were taken. The context in which these data were disclosed is political, but if one considers the actual conduct of the media releasing and sharing the news with reference to the principles of respecting an individual's privacy, it must be analysed from several angles.

In this particular case, the published photographs, the full name, the location, as well as the connection to her parent who is a public figure, all constitute personal data. Journalists should distinguish between the relevance of the information they release on public figures holding political or public office, and the data on their family members. Protecting the personal data of the politician's daughter and protecting his privacy as a public figure are diametrically opposed.

The discussion on the protection privacy is all the more important if one takes into account that the data in question related to a minor. Personal data on minors must not be released without proper safeguards, that is, obscuring the face and using initials. Minors are persons with limited civil capacity, therefore they cannot personally give consent whether certain information on them is to be made public or not. The consent for publishing the personal data of minors must be asked from their parents, guardians or legal representatives, but even when it is obtained, one must take into account the future implications of disclosing the minor's personal data. That the media outlet was not mindful of protecting the privacy of the politician's daughter is evident from the two published photographs, which were obviously reposted and unprocessed: on one, the full name was visible and the face obscured, whereas on the other only the name was anonymised, and the face visible.

In furtherance of the above findings, one should also consider the legal restrictions to processing sensitive personal data: in this case, political convictions.

5.5. Case Study: 'Media Owner'

In an attempt to prove the ownership of a company and of foreign bank accounts, the media released data from the Central Registry, whereby on one of the forms one could clearly see the personal identification number of the manager of one of the trading companies subject to media reporting, who is also the owner of a well-known media outlet.

In this particular case, the personal data disclosed included the individual's full name, his personal identification number and his address of residence. Considering the fact that these data are also mandatory in the form section requiring the data on the managing officer of the legal entity, the piece of data that under all circumstances must be completely obscured when reporting is the citizen's personal identification number.

The Law on Personal Data Protection specifies that the citizen's personal identification number be considered a particularly sensitive piece of data. Processing the citizen's personal identification number is specially regulated, that is to say, it can only be processed upon the personal data subject's prior consent, for the purposes of realising the subject's legal rights and responsibilities. In any case, under the law, one should make sure that the citizen's personal identification number not be needlessly visible, reprinted or downloaded from a personal data collection.

In this particular case, the release of the manager's full address of residence is also questionable. Namely, the purpose of the

news was to show that two legal entities had the same address, whereas the address of residence of the manager linked to these legal entities did not pertain to the substance of the information. In such cases, partial anonymisation (of the building and flat number) should be applied. The manager's address would not be subject to anonymisation if it matched the legal entity's registration address.

The responsibility for the release of non-anonymised personal data in this case was shared. Initially, anonymisation should be performed by whoever releases the information, and if that has not been done, it is the media that, upon publication, should protect the personal data on the individuals subject to reporting, if the data do not affect the relevance of the information.

5.6. Case Study: 'Voter Registry'

One of the most vigorous debates conducted in the public over the last few election cycles is the electronic availability of the voter registry, that is, the publicly accessible personal data on the citizens with the right to vote.

It is unquestionably in the citizens' interest to be able to check the accuracy of their personal data in the voter registry in an easily accessible, fast and free manner. What is also unquestionable is the extent of personal data collected in the voter registry. Under the Electoral Code, the voter registry contains the citizen's personal identification number, the surname, a parent's name and first name, the sex, a personal photograph (in an ID or passport format), address of residence (municipality, geographic area, street name, house number, block and flat number), the date of entry and removal from the registry, and the date and type of data amendments.

What has sparked the debate, in fact, is the use of the citizen's personal identification number as the password the access the electronic voter registry. Namely, the citizen's personal identification number, under the Law on Personal Data Protection, is a sensitive piece of personal data, enjoying higher degree of protection than other types of personal data. Any processing or use of the citizen's personal identification number should be specified by law, and such ground are not provided either in the Electoral Code, or in the Law on Personal Data Protection.

Furthermore, in contravention of the principles of personal data protection is the possibility through a simple name search to arrive at the specific address of residence, that is, at data on the municipality, geographic area, street name, house number, block and flat number, and polling station.

In order to accommodate the principles of personal data protection, a sufficient protective measure would be for every citizen to access the voter registry with a password they create themselves, but also to provide anonymisation of part of the data (block, building and flat numbers) publicly available after a simple name search.

5.7. Case Study: 'City Parking Services Director'

One of the news that was in the public interest focus in November 2015—an example of inaccurate assessment of where to draw the line between public and private interest—was the news on the level of income of a public enterprise director.

The media, chiefly web portals, released a photograph of the calculation of the director's salary, which clearly showed that his monthly earnings amounted to nearly EUR 2,000. On the photograph one could clearly see the data on the month the salary had been received, the director's full name, employment longevity, gross income, years of service, allowances, social security contributions, and salary deductions.

The news became even more interesting when the director filed a petition against the media, claiming that releasing the calcula-

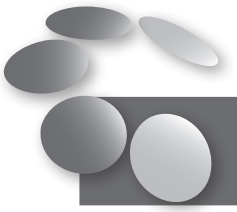
tion and his level of income had invaded his privacy, that is, they had disclosed his personal data in a scope excessive to the purposes of informing the public. Furthermore, the director invoked the fact that his data had been released without his consent. The Council of Media Ethics responded to his petition by issuing a ruling, finding that his privacy had been violated, but not specifying which data are considered excessive.

Judging from the provisions of the Law on Free Access to Public Information, it is clear that the salaries of elected and appointed officials paid from 'public funds' constitute public information. Should this information be requested, it should be released by the employer, and not upon the consent of the person it pertains to. Of course, considering the exemption to the law regarding personal data protection, it could be debated that anonymisation should be performed where necessary, but in this case it should be specified precisely where the exemption would apply.

The years of service may be considered as the individual's overall work experience, which should be a criterion for his appointment to the position, but considering the fact that the Law on Public Enterprises does not clearly specify this criterion, the data on the years of service in this particular case are not crucial to the news, the purpose of which was to show the level of income.

The salary deductions are data that absolutely reveal part of a person's privacy, and for this reason, they should be anonymised. In this particular case, the deduction referred to a collective insurance premium payment, but this part of the calculation also includes data on loan payments, sick leave deduction, and so forth. For these reasons, the data on salary deductions are considered excessive.

In this case, one might conclude that part of the data do not serve the purposes of the information and are excessive, and that the media, when reporting, should have employed technical measures for anonymisation, thereby abiding by the principles of personal data protection.



5.8. Case Study: 'Secret Lists with Publicly Available Data'

The lists of citizens' personal data used in various partisan activities always seem to be a current topic, regardless of what exactly they refer to. In December 2015, a web portal released the news of a

cracked VMRO-DPMNE survey carried out by party members using a filtered voter registry of only young people from the Centar Municipality, conducting a poll with the question: In the next elections, would you vote for VMRO-DPMNE if the party offers you a guarantee of post-election employment?

The news was further supported by photographs of lists, on which on could easily read the citizens' personal data, including: full name, specific address of residence, full phone number and information on whether the citizen had voted or not. The news in itself does not include sufficient concrete facts that would make it reliable and true, but what is subject to this analysis is the disclosure of the citizens' personal data, in context of their political affiliation.

The Law on Personal Data Protection is decisive in defining which data are considered personal:

'Personal data' shall mean any information pertaining to a natural person or a person identifiable by reference to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

Under this law, there are exemptions pertaining to professional journalism:

The provisions of this Law shall not apply to the processing of personal data conducted for the purposes of professional journalism, only when public interest prevails over the private interest of the personal data subject.

The public interest in this case is undisputable, but the manner in which the data were released should absolutely be disputed, considering that what was disclosed were personal data allowing for the citizens' direct identification. What the media outlet is obliged to do in such cases is to assess which personal data are released, to what extent and how much their disclosure supports the substance of the information.

An additional argument in favour of contesting the manner in which these lists were released is the fact that under the Law on Personal Data Protection not all personal data enjoy the same degree of protection. There is a category of special, sensitive personal data that are under special protection, and they are data

revealing one's racial or ethnic background, one's political, religious, philosophical or other beliefs, membership to a trade union and data regarding people's health, including genetic data, biometric data or data concerning one's sex life.

The concept of 'relevance of the information' is particularly important in this case. Any mention of sensitive data should be avoided, considering the fact that the Law on Personal Data Protection prohibits the processing of special categories of personal data, barring extraordinary circumstances as stipulated by law.

In addition to all of the above, one of the principles of fair processing of personal data that must not be disregarded is the consent of the citizens whose personal data are on the lists to have the data processed. We cannot guess whether the citizens consented to be on the list, but we can certainly assume that they did not consent to have their personal data released to the public.

This information would not lose any of its substance if the media outlet that released it first had employed minimum technical measures for anonymisation, that is, if it had obscured the citizens' full names, specific addresses and telephone numbers.

6

Conclusions

Based on the findings from the theory and practice in the sphere of privacy and informing the public in Macedonia, and the analysis of the legislation and the cases from the practice, one might draw several conclusions on the situation and the relationship between the right to privacy and the public's right to know in the Republic of Macedonia:

- Privacy as a notion is still on a low and insufficiently understandable level in terms of executing policies and media reporting. Although there is a relatively good legislative framework on personal data protection, the notion of privacy is still abstract in implementing the regulations by the media. For the sake of exclusivity, data are disclosed that are not relevant to the news and violate the right to privacy of the person subject to media reporting. Furthermore, not enough measures are taken to anonymise the released materials in which personal data are revealed. There are data disclosed that not only violate the right the privacy, but also the principle of presumption of innocence.
- The Directorate for Personal Data Protection as a supervisory body is not sufficiently involved in mapping the shortcomings, in capacity building and in a suggestive approach to the media and other institutions to align with the laws on personal data protection and on free access to public information.
- The media do not have their own internal rules for fair release of the personal data on the persons subject to media reporting, and for privacy protection in general.
- Privacy as a notion is very complicated to define and to establish specific measures and norms for its protection. It is questionable how much the law can protect the individuals' privacy in a situation when with the progress of technology there is a rise in the number of tools allowing for instant sharing of personal information that might threaten the individuals' dignity and integrity. The rapid development of technology offering services that do not pay enough attention to really protecting their users' privacy is a subject matter that is not sufficiently prominent in public debate in the Republic of Macedonia.
- The legislative framework in the area of communication interception and the regulation of electronic communication is not specified clearly enough, and leaves room for abuses and for invasion the citizens' right to privacy. Oversight of the special investigative measures, including the interception of communications, is regulated poorly or not at all, whereby the institutions authorised to implement these measures have the opportunity for abuses, selective approach, arbitrariness, and human rights violations on account of the uncontrolled power of the institutions in the area.

7

Recommendations

Establishing balance between private and public interest is more than necessary, in order to simultaneously respect the right to privacy and the right to information, or the public's right 'to know.' Considering the fact that there is no single formula according to which one could make a general assessment what is public and what is private interest, striking the balance is particular and should be done on a case-by-case basis. The responsibility for establishing balance is shared among the media and the supervisory bodies implementing the laws on personal data protection and on free access to public information. Hence, the following recommendations may be made:

Recommendations for the Media and Journalists

- Adopting internal privacy policies—internally focused tools that will aim to clarify how the media will abide by the principles for personal data protection in cases when the reports contain personal data on the individuals subject to media reporting;
- Establishing codes of conduct—self-regulatory tools defining the common rules for the media in cases when private information should be released;
- Specifying standards for employing technical measures in the processing of information—obscuring faces and other personal data on the individuals subject to media reporting, distorting voices, using initials instead of full names;
- Obtaining consent to release personal data from the individuals subject to media reporting or their guardians any times it is possible;
- Journalists should not arbitrarily take and repost content from users' social media and personal profiles, but be particularly mindful of how they use such data, if the invade the private lives of the individuals whose data they are releasing, if they have the necessary consent, and be careful when reusing such data, particularly if the events in question are tragic or distressing.

Recommendations for the Directorate for Personal Data Protection and the Commission for Protection of the Right to Free Access to Public Information

- Acting in favour of amending and supplementing the Code of Journalists and the Law on Media. It is the supervisory bodies that should indicate shortcomings and propose harmonisation with the laws on personal data protection and on free access to public information;
- Mounting targeted informative campaigns to raise the awareness of editors, journalists and other media professionals as a support of sorts for easier establishing balance between public and private interest, and
- Regular educational meetings with the media, as well as with journalism students, considering the fact that no journalism and communication studies curriculum includes material on personal data protection.

Bibliography

Literature

- Jernej Rovsek, 2005, The Private and the Public in the Media, Ljubljana: Institute for Contemporary Social and Political Studies.
- Parent, W., 1983, 'Privacy, Morality and the Law', Philosophy and Public Affairs.
- Westin, A., 1967, Privacy and Freedom, New York: Atheneum.
- Warren, S. and Brandeis, L., 1890, 'The Right to Privacy', Harvard Law Review.
- Fried, C., 1970, An Anatomy of Values, Cambridge: Harvard University Press.
- Gavison, R., 1980, 'Privacy and the Limits of Law', Yale Law Journal.
- Rachels, J., 1975, 'Why Privacy is Important', Philosophy and Public Affairs.
- Kupfer, J., 1987, 'Privacy, Autonomy and Self-Concept', American Philosophical Quarterly.
- Allen, A., 2011, Unpopular Privacy: What Must We Hide?, Oxford: Oxford University Press.
- Regan, P., 1995, Legislating Privacy, Chapel Hill, NC: University of North Carolina Press.
- Schoeman, F., (ed.), 1984, Philosophical Dimensions of Privacy: An Anthology, Cambridge: Cambridge University Press.
- Buckley, Duer, Mendel and O'Siochru, 2008, Broadcasting, Voice and Accountability, Washington: University of Michigan Press.
- Lidija Koman Perenič and the Information Commissioner Slovenia, 2008, Media and the Protection of Personal Data, Ljubljana: Information Commissioner Slovenia.
- Mendell T., 1999, The Right of the Public to Know and Freedom of Entertainment, Strasbourg, Council of Europe.
- Верица Трајкова, „Истражување за свеста кај медиумите за подобра имплементација на правото за заштита на личните податоци" ['Research on the Awareness of the Media for Better Implementation of the Right to Personal Data Protection'].
- Олга Ѓуркова, „Правото на приватен живот и правото на заштита на лични податоци во Европското законодавсрво во судир со националната безбедност" ['The Right to a Private Life and the Right to Personal Data Protection in European Legilsation in Conflict with National Security'].
- Марјана Поповска, „Правото на приватност низ практиката на Европскиот суд за човекови права", 104-105 ['The Right to Privacy in the Case Law of the European Court of Human Rights'].
- О'Бојл, Варбрик, Харис, 2009, 363, 408, 413.
- Stephen Whittle, Glenda Cooper, Reuters Institute at Oxford University, 'Privacy, Probity and the Public Interest', 8 July 2009.
- Новица Наков, „Окамовиот меч за прислушувањето", 4 July 2015 ['Occam's Razor on the Wiretapping' (newspaper column)].
- Мирјана Најчевска, „Закон за заштита на приватноста – Кога Уставот ќе стане 'тоалетна хартија'" [The Law on the Protection of Privacy—When the Constitution Turns into "Toilet Paper"'].
- Горан Наумовски, ПлусИнфо, „АЕК: Ние реагираме ако има проблем помеѓу МВР и операторот, не контролираме дали има неовластено прислушување", 13 February 2015 ['AEC: We Intervene If There Is a Problem between the Ministry of the Interior and the Operator, We Do Not Control If There Is Unauthorised Wiretapping'].
- Изјава на Павле Трајанов, вест на Катерина Блажевска „Контролата на прислушкувањето еднаква на – нула!", DW, 13 October 2014 [Pavle Trajanov's statement, Katerina Blaževska's news article, 'Control of Wiretapping Equals—Zero!'].
- Гордан Калајџиев, „Ерозија на приватноста во Република Македонија", Кон измените и дополнувањата на Законот за електронски комуникации, 2010 ['The Erosion of Privacy in the Republic of Macedonia', On the Amendments and Supplements to the Law on Electronic Communications].

- Изјава на Уранија Пировска, Хелсиншки Комитет за човекови права, Слаѓана Божиновска, „Законот за следење комуникации раѓа страв“, Radio Free Europe, 8 June 2012 [Statement by Uranija Pirovska, Helsinki Committee for Human Rights, Slaǵana Božinovska, ‘The Law on Interception of Communication Breeds Fear’].
- Andreja Bogdanovski, Magdalena Lembovska, 2015, Communication Interception Oversight in Macedonia: Making the Impossible Possible, Skopje: Analytica Thinking Laboratory.
- Helsinki Committee for Human Rights of the Republic of Macedonia, ‘Control over Wiretapping—Who Will Guard Us from the Guards?’, Quarterly report, December 2011-February 2012.
- Metamorphosis Guide Privacy as a Fundamental Human Right.
- Danilovska-Bajdevska, D. et al (eds), 2013, Overcoming the Principles of Secrecy in the Public Admnistration’s Operation, Skopje: Foundation Open Society-Macedonia.
- Promoting Transparency and Accountability in Public Institutions, Skopje: Transparency International Macedonia, 2012.
- International Principles for Whistleblowing Legislation, Transparency International, 2009 https://www.transparency.org/files/content/activity/2009_PrinciplesForWhistleblowingLegislation_EN.pdf

European Court of Human Rights Cases

- Weber and Saravia v. Germany, December 2006.
- Klass and Others v. Germany, 6 September 1978.
- Malone v. the United Kingdom, 2 August 1984.
- Shimovolos v. Russia, 21 June 2011.
- Társaság a Szabadságjogokért (TASZ) v.Hungary, 14 April 2009.
- Axel Springer AG v. Germany, 7 February 2012.
- Von Hannover v. Germany (No. 1), 2004.
- Von Hannover v. Germany (No. 2), 2012.

Regulations

- Constitution of the Republic of Macedonia, Official Gazette of the Republic of Macedonia No. 52/1991.
- Law on Personal Data Protection, Official Gazette of the Republic of Macedonia No. 7/2005, 103/2008, 124/2008, 124/2010, 135/2011, 43/2014 and 153/2015.
- Law on Ratification of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Official Gazette of the Republic of Macedonia No. 7/2005.
- Law on Ratification of Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, Official Gazette of the Republic of Macedonia No.103/2008.
- Law on Free Access to Public Information, Official Gazette of the Republic of Macedonia No. 13/2006, 86/2008, 6/2010, 42/2014 and 148/2015.
- Law on Electronic Communications, Official Gazette of the Republic of Macedonia No. 39/2014, 188/2014, 44/2015 and 193/2015
- Law on Amendments and Supplements to the Law on Electronic Communications, Official Gazette of the Republic of Macedonia No. 83/2010.
- Law on Interception of Communications, Official Gazette of the Republic of Macedonia No. 121/2006, 110/2008 and 116/2012.
- Law on Protection of Privacy, Official Gazette of the Republic of Macedonia No. 196/2015.
- Law on Media, Official Gazette of the Republic of Macedonia No. 184/2013 and 13/2014.
- Constitutional Court ruling, Law on Electronic Communications, C. No. 139/2010, 15 December 2010.
- European Convention on Human Rights.
- EU Charter of Fundamental Rights.
- Code of the Journalists of the Republic of Macedonia.

Online Sources

- http://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Media_and_the_Protection_of_Personal_Data.pdf
- http://www.echr.coe.int/Documents/Convention_ENG.pdf
- http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT
- www.dzlp.mk
- www.coe.int/dataprotection
- http://mediawatch.mirovni-institut.si/eng/mw16.htm
- https://freedomhouse.org/report/freedom-press/2015/macedonia

About the Publisher

The Institute of Communication Studies (ICS) was established by the School of Journalism and Public Relations in 2013. ICS is a leading scientific research organization in the field of journalism studies, media, public relations, political communication and corporate communication. ICS in Reublic Macedonia has a dual focus: through academic and applied research to advance science and to be supportive of practitioners; through post-graduate studies to build a network of young researchers who will strengthen the pillars of these disciplines.

The Institute is accredited to provide graduate (master) studies in two areas: Management of Strategic Communications and Management of Media and Multimedia. Using the procedure of binding the teaching process and learning through research, the ICS fosters the development of young people in research and promotes the process of creation and dissemination of knowledge.

The ICS has the following main objectives:

- Developing academic and applied research that will increase the knowledge in the fields of communication, media and public relations;
- Creating a thorough research base that will be used in the education process in the fields of communication, media and public relations;
- Promoting innovative ideas in research related to the industry needs;
- Encouraging the development of young professionals in research by engaging students and young researchers in this field;
- Publishing research results on current affairs and issues in order to contribute to the public debate and to the process of creating policies in the fields of interest to ICS.

About the Project

The Institute of Communication Studies (ICS) implements the project **"Voicing the Public Interest: Empowering Media and Citizens for Safeguarding the Public Policy in Macedonia"**. Within the Project, ICS will (1) prepare analysis and policy papers and will organize discussions around them, (2) develop newsroom editorial guidelines for safeguarding the public interest, including the public interest test and, (3) impel citizens and experts to actively participate in the public sphere through the Res Publica blog.

Through analysis, policy papers, and discussions, ICS will provide a clear overview of the key aspects of public interest, i.e. how can citizens influence the policy-making process; how journalists cover public interest topics; the delicate balance between the public interest and other human rights (e.g. privacy, free speech); the role of the judiciary and the Government in safeguarding the public interest.

In collaboration with newsrooms, ICS will develop a Guideline for Public Interest Journalism (incorporating the public interest test) in order to protect the public from negligent journalism and unlawful media practices, and restore the trust of citizens in media. The Guideline will set out the standards for producing or presenting the newsroom products, and will provide advice for media professionals on how to deal with editorial issues, and on how to produce content on the highest ethical level when covering public affairs. The public interest test will improve the skills of journalists to decide how best to proceed when they are reporting about the welfare and safety of the public. ICS will work with fi ve national and regional media in order to develop the Guideline.

In order to reach a broader audience, ICS will utilize the newly developed web platform *Res Publica* (www.respublica.edu.mk) that will impel citizens, journalists, and experts to write articles and debate issues of public interest. This way, ICS will create a professional network that will continually analyze and introduce the public with current issues of public interest in the Republic of Macedonia.

The Project is supported by the British Embassy Skopje.

VOICING THE PUBLIC INTEREST

Empowering media and citizens for safeguarding the public policy in Macedonia

About the Authors

ELENA STOJANOVSKA has an MA in Communication and years of experience in the field of privacy protection. Between 2005 and 2014 she worked as an international cooperation and public relations advisor at the Directorate for Personal Data Protection. She completed her undergraduate studies at the Faculty of Law of the Ss. Cyril and Methodius University in Skopje, and received her masters from the Institute for Sociological, Political and Juridical Research in Skopje, with a dissertation entitled *The Impact of Recordings of Investigative Operations Broadcast in the Media on Realising the Right to Privacy in the Republic of Macedonia.* She has authored and co-authored numerous professional papers on personal data protection in various fields, analyses and research pertaining to the implementation of the personal data protection regulation. In addition to the right to privacy, her field of interest also includes media regulation and information and communication theories.

JOVANA ANANIEVSKA graduated from the Iustinianus Primus Faculty of Law of the Ss. Cyril and Methodius University. She continued her education with the Erasmus Mundus Master's Programme in the field of International and European Law at the Louis Pasteur Faculty of Law at the University of Rouen, France, and the Faculty of Law at the Catholic University of Portugal in Lisbon. She received her master's with a dissertation entitled *European Legislation and Protection against Discrimination Based on Disability.* She joined the civil sector as a volunteer in numerous organisations working in the field of discrimination against persons with disabilities. From 2012 to 2014 she worked as a coordinator and legal advisor at the LGBTI Support Centre, a subsidiary of the Helsinki Committee for Human Rights. In 2013 she began working in the field of privacy as pertaining to marginalised communities. Her field of interest includes digital security, sensitive data protection and tools for increasing online privacy.

PRIVACY, INFORMATION AND PUBLIC INTEREST:
THE RIGHT TO PRIVACY VERSUS THE PUBLIC'S RIGHT TO KNOW

POLICY PAPER

VOICING THE PUBLIC INTEREST

Empowering media and citizens for
safeguarding the public policy in Macedonia

British Embassy
Skopje

INSTITUTE
OF COMMUNICATION STUDIES

Jurij Gagarin 17-1/1
1000 Skopje, Macedonia
T: +389 2 3090 004
info@iks.edu.mk I www.iks.edu.mk