

Copyright: The author/s  
This work is licensed under a CC-BY 4.0 license  
(\*) Corresponding author  
Peer review method: Double-blind  
Original research article  
DOI: 10.20544/HORIZONS.1.1.24.P01  
**Section A**



## PRIVACY AND PERSONAL INFORMATION PROTECTION IN KOSOVO: CHALLENGES AND PERSPECTIVES

**Berat Dërmaku**

University “Kadri Zeka”, Faculty of Law, Gjilan, Republic of Kosovo.

ORCID ID: <https://orcid.org/0000-0002-1744-5327>

Email: berat.dermaku@uni-gjilan.net

**Elena Temelkovska – Anevska**

University “St. Kliment Ohridski” - Bitola, Faculty of Law, Bitola, North Macedonia

ORCID ID: <https://orcid.org/0000-0003-1048-0848>

Email: e.temelkovska@gmail.com

### Abstract

*As a fundamental human right, privacy, and data protection are becoming increasingly important in the digital age. This study examines the challenges and opportunities for privacy and data protection in Kosovo, with a particular focus on the legal system, the impact of technology, and public awareness. A qualitative research approach was used, reviewing reports from relevant organizations, international treaties, and legal documents. While the findings show significant progress in aligning Kosovo's legal system with European standards, they also reveal gaps in implementation and knowledge. Rapid technological advances have outpaced legislative measures and exposed vulnerabilities in data security. The study comes to the conclusion that in order to address these issues, it is imperative to enhance the National Agency for Personal Data Protection, improve enforcement mechanisms, and advance public education. Establishing robust protections for personal data in Kosovo's changing digital environment requires cooperation between the public and commercial sectors.*

**Keywords:** Privacy, personal data protection, Kosovo, human rights, technology, legal framework, data security.

### INTRODUCTION

The right to the protection of personal data and privacy is a fundamental right within human rights. This right is essential for the functioning of a democratic society. The rapid development of information technology and telecommunications has complicated the personal data protection process. Now, modern technology devices, such as smartphones, computers, laptops, etc., have become the main tools for collecting and storing personal data. This

development of technology, on the one hand, made our lives easier, but on the other hand, it negatively affected our privacy.

The right to respect family life protects both the actual family life as well as the potential family life of an individual. But the right to privacy does not always allow all, sometimes it can even be confiscated if it is a question of abuses, terrorism, etc. The right to privacy is one of the main rights that is related to many other rights and that can be considered as a basis for the enjoyment of other rights.

The right to privacy implies the individual's right to live peacefully in his family and home independently from others, and the law guarantees him protection from unauthorized interference by other individuals. (Frank, 1972)

In contrast to this definition, the other author Robert B. Hallberg gives another definition where according to him the right to privacy or the right not to be seen or heard is subject to an essential limitation. So it does not waive the right not to be seen or heard when one goes public. The right to privacy is and must be subject to a substantial limitation. (Hallborg Jr, 1986)

The process of protecting personal data is a standard considered very important both at the local and international levels, the implementation of which is becoming part of the daily agenda for most democratic countries. The need for the protection of personal data has come as a result of the accelerated development of information technology. Taking as a comparison the traditional forms of collection and storage of personal data which were almost entirely archived in an analog way, the new technology has almost completely transformed the concept of collection and storage of these data. Modern technology devices such as computers, internet networks, audio and video recordings, etc., have become the main tools for collecting and storing personal data.

Favoring this development in the field of information technology was the continuous decrease in the market price of these devices as a result of the increase in market offers, making their possession possible for almost every individual. This easy access to the possession of these devices has increased the number of actors involved in the process of collecting, storing, or using personal data in both the public and private sectors. (Gottwald, 1996) In fact, nowadays with new technology, it has become very easy and extremely cheap that any natural or legal person can have access to personal data by creating databases to collect important personal data. In this context, given the constant increase in dynamics at work and therefore the acceleration of the exchange of information, it has become almost impossible to avoid the exposure of personal data. Exposure of personal data starts from the civil registration offices (birth registration, issuing of identity cards, passports, and birth certificates), business registration offices, filling out forms for various applications, submitting CVs, opening bank accounts or e-mail addresses, purchasing of telephone numbers, registration in various social networks, E-marketing, registration during entrances to buildings, during registration of participation in conferences, during border control, during police identification, surveillance with cameras and many others. Taking into account the variety of situations in which almost every citizen is obliged to expose personal data, it can be said that in addition to the positive aspects that the facilitation of communication has brought, especially in the efficiency of the use of time and the reduction of expenses, these developments have also negative impacts in the field of personal data protection. (Gierke, 2010) The negative part of this development has to do especially with the exposure of important private data, the disclosure of which may harm the personal interests of those individuals or companies.

Bearing in mind that technological development in the field of information technology is a global concept that has not spared anyone, it can be said that Kosovo and its citizens have been and remain followers of these developments. Thus, even though our country still has many challenges to overcome in the journey of building the state and improving economic well-being, this does not mean at the same time that we dare to ignore the protection of those rights that can even be considered for each individual and that are related to the protection of personal data and privacy in general. In the end, because Kosovo has already adopted the relevant law that regulates this field, it is necessary that through analysis and research, the aim is to make the general public aware of the level of implementation of the protection of personal data, as well as the importance that this field presents. More concretely, from the contemporary perspective, the protection of personal data is as important as all other basic human rights. (Vrajolli & Kryeziu, 2011)

## **LITERATURE REVIEW**

The concept of privacy is deeply embedded in human relationships and is recognized as a fundamental right, both internationally and domestically. The protection of personal information has become increasingly challenging with the rapid evolution of information technology, particularly in countries like Kosovo. The importance of safeguarding personal data is underscored by the role it plays in upholding human rights and freedoms.

The digital age, marked by the prevalence of devices like smartphones and computers, has revolutionized the collection and storage of personal data. While technological advancements have undoubtedly improved efficiency, they have also raised concerns about privacy infringement. The right to privacy encompasses the individual's ability to live peacefully in their family and home, protected from unauthorized interference. However, with the proliferation of technology, exposure of personal data has become nearly unavoidable, posing risks to individuals' interests.

The protection of personal data is crucial, given the diverse situations in which individuals are obligated to disclose sensitive information. This includes civil registration processes, business transactions, social media activities, and more. The ease of access to technology has led to an exponential increase in the number of entities, both public and private, involved in collecting, storing, and using personal data. This development has both positive and negative implications, with the negative aspects primarily concerning the exposure of private data that may harm individuals or companies.

Kosovo, despite facing challenges in state-building and economic development, has recognized the importance of protecting personal data. The adoption of relevant legislation indicates a commitment to ensuring that the rights associated with personal data and privacy are not overlooked. However, public awareness remains a challenge, particularly in rural areas, where citizens may not be fully informed about their rights.

## **RESEARCH METHODOLOGY**

This research employs a qualitative approach, focusing on an analysis of the challenges and perspectives surrounding privacy and personal information protection in Kosovo. The study examines the current legal framework, technological advancements, and societal implications. Data collection involves a comprehensive review of existing literature, including legal documents, international agreements, and scholarly articles.

## **RESEARCH OBJECTIVES**

1. Evaluate the current legal framework for personal data protection in Kosovo.
2. Assess the impact of technological advancements on the privacy of individuals in Kosovo.
3. Examine societal perspectives and awareness regarding personal data protection.
4. Identify challenges faced by both public and private sectors in implementing and complying with data protection regulations.
5. Investigate the role of the State Agency for Personal Data Protection in monitoring and enforcing data protection laws.

## **PROTECTION OF PERSONAL DATA AND BREACH OF PRIVACY**

The bodies of the state power, in most cases, are presented in the capacity of the body in which the data are collected, recorded, processed, and use most of the citizens' data. This happens especially with the state administration bodies, which, while observing the situations in the territories for which they were created, keep various records and registers that are partially or completely related to citizens' data (e.g., mother records of born, married, deceased, and evidence for taxpayers, etc.). However, other state bodies, courts, and other legal entities authorized by law keep records and collections of various data that include the personal data of citizens (Central Registry, records in the field of work, health, defense social, personal evidence, etc.). Based on this, the protection of the personal data of citizens, as constitutionally guaranteed, but also by other international acts, appears as an important issue concerning the daily activity of a large number of public sector bodies. (Zeiller, 1998)

The legal protection of personal data also extends to cases where, in addition to state bodies and other legal, natural, or individual persons in the exercise of their profession or independent activity, they are presented as users with a summary of data based on legal authorization or written consent. of the person to whom the data relate. The purpose of personal data protection is to ensure the privacy and confidentiality of data relating to natural persons, while they are the object of collection, processing, storage, use, and exchange of data in the form of manual summaries of data. (Treschsel, 1980)

Summary of data is multiple organized data that fully or partially contain personal data (registers, records, databases, and the like) that are recorded and used manually or with tools for automatic data processing. The protection of personal data is carried out through legal treatment and measures. The summary of data is established, maintained, and used by data users who may be legal and natural persons or individuals in the independent exercise of the activity or profession authorized by law or based on written consent from the person for whom they have to do the data. (Matscher, Petzold, & Wiarda, , 1988)

Users with data can transfer certain actions related to the collection, processing, storage, use, and delivery of data to the contracted executor – a legal entity or individual in the independent exercise of activity or profession or natural person authorized to the exercise of this activity. The holder of personal data can collect, process, store, use and submit them only for purposes specified by law or for purposes resulting from the written consent of the person to whom the data relate, and never use them contrary to legal purposes. The data provider can submit personal data only to the user who is authorized by law for their use, or based on a written request or written consent of the person or his authorized representative. The user of the data can use the obtained data only in a way that is by the law. Personal data that the user uses for scientific research, education, or for other similar purposes, the holder of the summary of the data is obliged to submit them in a manner and form that do not enable the identification of the person. (Henkel, 1958)

With the organized technological actions and measures that are undertaken due to the protection of personal data, the spaces, equipment, and programs through which personal data are processed are secured, the delivery and transfer of personal data are guaranteed and unauthorized access to equipment and devices is prevented. programs using which personal data are processed and summaries containing personal data. (Government, 2022)

## **CRIMINAL DEFENSE**

Privacy, as we understand it today, has its origins some 150 years ago. The origins of the right to privacy can be traced back to the nineteenth century. In 1890, Samuel D. Warren and Louis D. Brandeis published "The Right to Privacy," an influential article that assumed a general common law right to privacy. Before the publication of this article, no US court had recognized this legal right. Since the article was published, courts have relied on it in hundreds of cases presenting a variety of privacy issues. (Solove, 2006)

Unlawful invasion of privacy is a criminal offense. Anyone who uses personal data, transferring it illegally is punished. Even revealing official secrets is punishable. Not all acts are prohibited in terms of privacy because where the general interest of the state depends, it is not considered illegal.

## **CIVIL DEFENSE**

Illegal violation of private life means when a person's rights in personal and family life have been violated, that is, a violation of the most intimate rights, and thus for that person the right to seek compensation arises. In modern legal systems, a person does not need to be injured in his honor or authority to seek civil protection, but the violation of privacy provided by law is sufficient. Such protection, the person can seek through the courts. The person whose privacy rights have been violated is available to request the termination of this violation and the request for compensation for moral damage, etc. (Prof. dr. sc. Nikola Gavella- Osobna Prava I.dio, 2000)

## **PROTECTION OF PERSONAL DATA IN KOSOVO**

The protection of personal data in Kosovo is a fundamental right guaranteed by the Constitution of the Republic of Kosovo. The right to protection of personal data and privacy, as part of human rights and freedoms, based on Article 22, is guaranteed by the Constitution.

Human rights and freedoms guaranteed by international agreements and instruments apply directly in the Republic of Kosovo and have priority, in case of conflict, over the provisions of laws and other acts of public institutions. And, based on Article 53 of the Constitution of the Republic of Kosovo, the human rights and fundamental freedoms guaranteed by this Constitution are interpreted in harmony with the judicial decisions of the European Court of Human Rights.

Article 36 of the Constitution specifies that privacy and family life, inviolability of residence, the secrecy of correspondence, communication by telephone and other means, and protection of personal data are guaranteed for each individual. Thus, the Constitution and the Law guarantee the implementation of some of the main international and European conventions regarding data protection. These conventions are the Universal Declaration of Human Rights; European Convention for the Protection of Human Rights; Fundamental freedoms and protocols; Convention 108/EC and additional protocol (Europe, 2008); EU directives 95/46/EC (Protection, 2022) and directive 2006/24/EC (Për mbajtjen e të dhënave të gjeneruara ose përpunuara në lidhje me dispozitën e shërbimeve të komunikimit publik elektronik ose të rrjeteve të komunikimit publik dhe ndryshimit). Since Kosovo is not yet a member of the relevant international organizations and as a consequence is not a signatory party, then these conventions are applied unilaterally.

The Law on the Protection of Personal Data (Law No. 2010/03-L-172), regarding the protection of personal data, was adopted in April 2010, and as such was generally in harmony with the European Directive on the protection of personal data (Directive 95/46/EC). While great efforts are being made by the European Union to modify the existing directive to future circumstances, the existing law in Kosovo is advanced and the possible modifications of the EU directive do not require any major changes to the law of Kosovo. However, it was a request of the EU communication in the "Feasibility Study for the Stabilization Association Agreement between the European Union and Kosovo that the legislation for the protection of personal data should be further harmonized with EU standards."

The law on the protection of personal data defines the rights, responsibilities, principles, and measures regarding the protection of personal data. The law also defines the institution responsible for monitoring the legitimacy of data processing. The law stipulates the establishment of the State Agency for Personal Data Protection (ASHMDHP), which is defined as an independent body under the direct supervision of the Assembly of Kosovo, which is responsible for supervising the implementation of data protection legislation. Therefore, the law specifies that the Agency will: provide advice to public and private bodies on issues related to data protection; decide on data-related complaints; made inspections and audits; inform the public about issues and developments in the field of data protection, and; promote and support fundamental data protection rights. (Qehaja)

## **PROTECTION OF PERSONAL DATA PROVIDED BY THE CRIMINAL CODE OF THE REPUBLIC OF KOSOVO**

The protection of privacy is also regulated by the Criminal Code of the Republic of Kosovo, respectively in article 199, paragraphs 1 and 2 of this Code, regulates the violation of the confidentiality of correspondence and computer databases, where further this article provides: "Anyone who without authorization opens a letter, telegram, facsimile or any other closed document or delivery or electronic communication of another person, or in any other way violates the confidentiality of such materials or without authorization retains, conceals, destroys

or delivers another person's letter, telegram, facsimile, electronic communication or any other closed document or delivery of the other person, shall be punished by a fine and imprisonment of up to six months. Anyone who without authorization intervenes in the computer database of another person or uses those data or makes them available to another person shall be punished by a fine and imprisonment for up to one year." (Official Gazette , 2019) So, as you can see in this provision of the Criminal Code, a prison sentence is provided if the confidentiality of data is violated and that the violation of this right constitutes a criminal offense.

In article 200, paragraph 1 of the Criminal Code, it is provided that "if the lawyer, defender, doctor or another person who without authorization discloses confidential information about which he was made aware during the exercise of his profession and which he is legally obliged to keep in secret, shall be punished by a fine or by imprisonment for up to one year". (Official Gazette , 2019) Article 201 paragraph 1 of this Code also states: "Anyone who, without authorization, eavesdrops on a conversation or statement or enables another person to be aware of the conversation or statement that was intercepted without authorization, is punished with imprisonment of one to three years(Official Gazette , 2019), while article 202 paragraph 1 provides: Anyone who without authorization photographs, films, videotapes or in any other way records another person in his residence or in any other place where the person has a reasonable expectation of privacy and in this way fundamentally infringes another's privacy, shall be punished with a fine or imprisonment of one to three years". (Official Gazette, 2019)

What is special in this aspect is that the protection of personal data has earned the epithet of their protection with the Criminal Code and the pursuit of potential violators of these rights is carried out according to the official duty, (Official Gazette , 2019) relate to data protection; decide on data related complaints; made inspections and audits; inform the public about issues and developments in the field of data protection, and; promote and support fundamental data protection rights. (Qehaja)

The installation of cameras in toilets can raise serious privacy concerns. Bathrooms and toilets are considered private spaces where people expect to have complete privacy. Cameras in these spaces can be a violation of privacy and can make people feel uncomfortable and insecure.

### **ACCESS TO DATA STORED BY THE STATE**

It is often more the individual's inability to access information held by the State on the subject of the complaint than the fact that such data is held by the State's archives. In the case of *Gaskin v United Kingdom*, the applicant, who had been taken into care at a very young age and remained there until he reached adulthood, wanted access to the entire file relating to his time in the care of the State. In contrast to the *Leander* case, the applicant in the *Gaskin* case did not complain that information about him had been collected and stored. He challenged the failure to give him access to that information as a failure to respect his privacy under Article 8, the Court had no difficulty in deciding that the information contained in the file belonged to the private and family life of the applicant, whose lack of access drew the attention of Article 8. It then went on to consider whether a fair balance had been struck between the general interest of the community – in keeping the system of social services records confidential – and the interests of the individual – in accessing information relating to his private life. Concerning the latter, the Court observed that persons like the applicant have a "vital interest" in obtaining information that is necessary to know and understand their childhood and early development. About the general

interest, however, the Court noted the important link that exists between obtaining objective and reliable information and maintaining a confidential system of public records.

As a result, it held that a system that accesses records that are dependent on the consent of the contributor complies, at least in principle, with Article 8. However, difficulties arise in securing the interests of the individual seeking access to archives related to his private and family life, when the contributor of the information is either not available, or unreasonably refuses to give his consent. According to the Court, such a system will be compatible with the principle of proportionality only if it ensures that an independent authority decides definitively whether access should be granted in cases where the contributor does not respond or does not give his consent. (*Gaskin v. Great Britain*, 1989)

## **CONCLUSION**

The right to privacy for all persons must be guaranteed. Article 36 of the Constitution of the Republic of Kosovo protects the privacy and guarantees the protection of personal data. The right to private life, affirmed in the Constitution, includes the guarantee given to the individual not to incriminate himself, the right of the individual to make his data public when he wants, as well as the protection of this data, to the right to protect the privacy of the apartment from involuntary and unauthorized police interventions, as well as the privacy of correspondence.

Undoubtedly, the Strasbourg Court played and plays an irreplaceable role in the understanding and protection of this right, according to which, the right to respect for private and family life has, first of all, the purpose of protecting the individual from arbitrary interference by public authorities. This goal is achieved by protecting the four dimensions of personal autonomy of an individual which are private life, family life, housing, and correspondence. Privacy is precisely the right to maintain control over the information that belongs to us, to be aware that many of our daily actions leave traces in such a way that they reveal the details of our Personality, our inner belief, that we do not always want others know him. In the past, it was expensive to get someone under surveillance, but shortly, it will be expensive to get someone out of surveillance. Based on this, the majority of citizens in Kosovo continue to be uninformed about the existence of the Law on Personal Data Protection and the importance of the implementation of this law.

The exposure of citizens to the violation of privacy in Kosovo remains particularly high. Until now, there have been no criteria for verifying the cases of collection of personal data in an unauthorized manner, as well as there has been no adequate control for how the collected data is processed in cases where such authorization exists. In this regard, there is a lack of awareness regarding this field, both on the part of actors in the public or private sector who collect personal data in an authorized manner, as well as by ordinary citizens. Kosovo has made progress in terms of data protection personal and the right to privacy in the period from 2011-2013. Progress can be measured against the complete lack of public awareness of their rights before the adoption of the legislation (in 2010), and in particular before the establishment of the State Agency for the Protection of Personal Data (ASHMDHP).

Public awareness remains one of the challenges in the field of data protection. The agency has not managed to sensitize citizens in all regions, and in particular, these challenges remain more pronounced against the awareness of citizens in rural areas. The media was used as a means of raising awareness, but not at such a satisfactory level, knowing that the media have an extraordinary role in preserving and respecting private-family life.

## Recommendations

To effectively address the challenges and improve the protection of privacy and personal information in Kosovo, several key actions should be prioritized:

1. **Enhance Public Awareness:** It is crucial to implement widespread and targeted awareness campaigns, particularly focusing on educating citizens in rural and underserved areas. These campaigns should aim to inform individuals about their rights concerning personal data and emphasize the importance of data protection in everyday life. Awareness efforts should also include practical guidance on how citizens can safeguard their personal information in an increasingly digital world.
2. **Strengthen Legal Frameworks:** Kosovo's legal framework for data protection should be continuously reviewed and updated to keep pace with the rapid evolution of technology and international data protection standards. Legislators must ensure that the legal provisions offer robust protection for personal data, including clear guidelines for data collection, processing, and storage. Additionally, the law should impose stringent penalties for violations, ensuring deterrence and accountability among both public and private entities.
3. **Promote Collaboration and Coordination:** A coordinated approach involving government institutions, private sector organizations, and civil society is essential to effectively protect personal data. This collaboration should focus on sharing knowledge, resources, and best practices for data protection. By fostering open communication and cooperation among these stakeholders, Kosovo can create a more unified and effective system for safeguarding personal information.
4. **Conduct Regular Audits and Assessments:** To ensure compliance with data protection regulations, regular audits should be carried out, especially within the public sector, where large amounts of sensitive personal data are often processed. Continuous monitoring mechanisms must be established to detect potential breaches or non-compliance. These audits should be accompanied by assessments that identify areas for improvement and recommend corrective actions to enhance data security practices.
5. **Foster International Cooperation:** Given the global nature of data flows and digital technologies, Kosovo should strengthen its collaboration with international organizations and neighboring countries. By sharing best practices and aligning regional data protection efforts, Kosovo can bolster its capacity to address cross-border data protection challenges and stay informed about emerging global trends in privacy laws and regulations.

Addressing the privacy and personal information protection challenges in Kosovo requires a comprehensive, multi-stakeholder approach. By focusing on public awareness, legal reforms, inter-institutional cooperation, continuous assessments, and international collaboration, Kosovo can establish a robust data protection framework that ensures the privacy rights of individuals are respected in the digital age.

## REFERENCES

1. Europe, C. o. (2008, 11 08). Protokoli shtesë i konventës për mbrojtjen e individëve sa i përket përpunimit automatik të të dhënave personale në lidhje me autoritetet mbikëqyrëse dhe të qarkullimit të të dhënave përtej kufijve,. Retrieved from Details of Treaty No.181: <http://conventions.coe.int/Treaty/en>
2. Frank, R. (1972). Der Schutz der Personlichkeit in der Aivilrechtsordnung der Schweiz, Archiv fur die civilistische Praxis", p.8 1972. Archiv für die civilistische Praxis, 8.
3. Gaskin v. Great Britain,, Gaskin v. the United Kingdom (European Court of Human Rights July 07, 1989).
4. Gierke, O. V. (2010). Das deutsche Privatrecht, (Vol. 1). Leipzig: Ducker & Humblot.
5. Gottwald, S. (1996). Das allgemeine Persönlichkeitsrecht. Berlin, Baden-Baden: Berlin, Humboldt-University Press.
6. Government, N. M. (2022, March 10). Retrieved from [http://www.ads.gov.mk/WBStorage/Files/poglavje21\\_AL.pdf](http://www.ads.gov.mk/WBStorage/Files/poglavje21_AL.pdf)
7. Hallborg Jr, R. B. (1986). "Law and Philosophy" Principles of liberty and the right to privacy.Kluwer Academic Publishers.
8. Henkel, H. (1958). Der Strafschutz des Privatlebens gegen Indiskretion, gutachten und Leitsätze für den 42. Deutschen Juristentages , Bd II, (Sitzungsberichte), , (Vol. 1). Dusseldorf, Henkel, H. (1958). Der Strafschutz des Privatlebens gegen Indiskretion: Gutachten f.d.42. Dt. Juristentag. Germany: Mohr., Tübingen.: Mohr.
9. Matscher, F., Petzold, H., & Wiarda, , G. J. (1988). Expulsion and the right to respect for private and family life an introduction to the Commision's case-law, u:Matscher, F., Petzold, H.: Protecting Human Rights: The European Dimension- Protection des Droits de i'honneur de Gerard J. Wiard. In E. V. M, Protecting human rights : the European dimension : studies in honour of Gérard (p. 520). Koln: Villiger, M.E.:
10. Official Gazette , R. o. (2019, 01 14). Penal Code. Retrieved from Official Gazette of the Republic of Kosovo: <https://gzk.rks-gov.net/ActDetail.aspx?ActID=18413>
11. Për mbajtjen e të dhënave të gjeneruara ose përpunuara në lidhje me dispozitën e shërbimeve të komunikimit publik elektronik ose të rrjeteve të komunikimit publik dhe ndryshimit. . (n.d.).
12. Prof. dr. sc. Nikola Gavella- Osobna Prava I.dio, Z. 2.-2. (2000). Osobna Prava I.dio. Zagreb.
13. Protection, D. (2022, March 20). Direktiva për mbrojtjen e të dhënave. Retrieved from <https://www.dataprotection.ie/vieëdoc.asp?DocID=90&m=>
14. Qehaja, R. (n.d.). Material diskutimi për mbrojtjen e të dhënave personale.
15. Solove, D. J. (2006). " A brief History of Information Privacy Law". Retrieved from [https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2076&context=faculty\\_publicat](https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2076&context=faculty_publicat)
16. Treschsl, S. (1980). Die Garantie der persönlichen Freiheit (Art. 5 EMRK) in der Straßburger Rechtsprechung.
17. Vrajolli, M., & Kryeziu, S. (2011, August 22). Dokument i shkurtër i politikave u përgatit në kuadër të programit TRAIN (Think Tanks Providing Research and Advice through Interaction and Networking) të Këshillit Gjerman për Marrëdhënie me Jashtë. Retrieved January 2024, from Kosovar Center for security studies: [https://qkss.org/images/uploads/files/Mbrojtja\\_e\\_të\\_Dhënave\\_Personale\\_në\\_Kosovë\\_663963.pdf](https://qkss.org/images/uploads/files/Mbrojtja_e_të_Dhënave_Personale_në_Kosovë_663963.pdf)
18. Zeiller, G. (1998). Personlichkeitsschutz, . Wien.