Tinatin Lolomadze*

Personal Data Protection According to the "Three-step Test" of the European Court of Human Rights: Risks and Challenges

Data protection is a key aspect of the legislative space. Data protection protects personal information Privacy and security in the face of technological advances and increased data usage.

The article discusses the practice of the European Court of Human Rights and the "three-step" test, which is a widely recognized principle, and is used to assess the legality and validity of restrictions on fundamental rights. The "three-step" test requires that any limitation of a right, such as the right to data protection, must meet three criteria: legitimacy, necessity and proportionality. By following a three-step test, legislators and judges can strike a balance between protecting data privacy and a legitimate purpose or interest.

Keywords: *Data protection, Protection of human rights, Basic regulation of data protection, Right to private life, Legitimacy.*

1. Introduction

Every person has a personal life, it is the space that gives us the opportunity to develop as individuals and become a part of society. It is not surprising that we often want our private lives to be hidden from the public eye. This does not necessarily mean that, as if, by keeping the existing information, we are committing a crime. In fact, this is absolutely harmless information that concerns a person's religious, political or social views. Private life is the actual essence of privacy, and the disclosure of information should depend on the individual and his or her desire. It is the privacy and protection of personal life that gives people the opportunity and courage to be able to express their opinion. It also guarantees to the state that one's personal information, thoughts, views and opinions remain free from judgment. One aspect of the right to privacy is the protection of personal data, which is considered a basic human right in today's democratic states. To date, a number of important legislative and institutional reforms are being implemented to realize this right. The European Court of Human Rights explains that the right to the protection of personal data is not an autonomous right, but is included among various Convention rights and freedoms[1]. The court recognized that the protection of personal data is of fundamental importance for the enjoyment of the

* Master of Law, PhD student of the Faculty of Law at Ivane Javakhishvili Tbilisi State University.

[1] *Amann v. Switzerland,* Application №27798/95, European Court of Human Rights, February 16, 2000, §65.

right to respect for private and family life and correspondence, as guaranteed by Article 8[2] of the Convention. In the digital age, the safeguarding of personal data has become an urgent issue worldwide. For example, a robust data protection framework, such as the General Data Protection Regulation (GDPR), has been established. An essential aspect of understanding and implementing these regulations is compliance with human rights principles.

The article aims to explore the relationship between data protection regulations and the three-step test established by the European Court of Human Rights (ECtHR). By analyzing this test, we will explore how states should regulate database protection to ensure individual rights and protect people from potential risks. By examining the interplay of rights, risks and regulations, the importance of striking a delicate balance between privacy and legitimate public interests in the digital age will be assessed.

2. Protection of Personal Data by the European Court of Human Rights

Data protection plays an important role in protecting an individual's enjoyment of private and family life, as it prevents the public disclosure of personal information. The collection, storage and disclosure of data constitutes an invasion of privacy. Article 8 of the European Convention on Human Rights recognizes both the right to personal data and the right to private and family life, residence and correspondence. Although the protection of personal data and the protection of privacy are different concepts, both of them seek to protect human autonomy and dignity[3]. The right to protection of personal data is a modern and relevant aspect of privacy rights aimed at ensuring the proper processing and development of personal information. The privacy principle covers a wide range of subjects, including sensitive and personal details, and aims to prevent any arbitrary interference.[4]

According to Article 1 of the European Convention on Human Rights, states have an obligation to "ensure" Protection of rights and freedoms provided for by the Convention. This obligation implies not only the prevention of violations of rights and freedoms (negative obligation), but also the active protection of personal safety, even when violations are carried out by third parties (natural and legal entities) (positive obligation) [5]. Although the primary objective of many provisions of the European Convention is to prohibit unjustified restrictions on public human rights, there is no doubt that states are responsible for ensuring the effective protection of these rights. The European Court of Human Rights has held that a positive obligation derives from the provisions of the Convention, including Article 8, which protects personal and family rights. In the case of: Marx v. Belgium, the European Court emphasized that the essential purpose of this provision is to protect individuals against arbitrary interference by public authorities. The role of the state goes beyond merely refraining from intervention; It also requires "respect" for family life. Thus, the protection of personal data implies the intervention of the national state and the legal framework and the practical

[2] *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland,* Application №931/13, European Court of Human Rights, June 27, 2017, §137.

[3] Guide to Article 8 of the Convention - Right to Respect for Private and Family Life, European Court of Human Rights, 2022.

[4] Guide to the Case Law of the European Court of Human Rights/Data Protection, Council of Europe/European Court of Human Rights, 2022, 7.

[5] *Korkelia K.,* Towards the integration of European standards: The European Convention on Human Rights and the Experience of Georgia, Tbilisi, 2007, 14-15 (in Georgian).

implementation of data protection measures. It is important to note that although Article 8 focuses primarily on the protection of private life, privacy as a fundamental element appears in private life itself. Confidentiality, in the context of personal data, is a crucial aspect of maintaining an individual's privacy. Ensuring the confidentiality of personal information through data protection mechanisms is a key factor in protecting the right to privacy and maintaining the necessary level of confidentiality and trust in personal relationships and transactions.

When assessing a potential violation of a person's right to data protection, it is crucial to refer to Article 8, paragraph 2, which outlines the prerequisites for legitimate interference. According to this provision, any interference must meet three criteria: it must be "necessary in a democratic society", "in accordance with the law", and must serve a "legitimate purpose". The requirement of interference, "in accordance with the law", implies that any limitation of the right to data protection must be based on clear and predictable legal provisions. This ensures that individuals have reasonable expectations of how their personal data will be processed and protected. In addition, the interference must have a “legitimate aim. This means that, through data processing, the invasion of a person's private life must have a justified purpose. Examples of legitimate purposes include national security, public safety, crime prevention, health protection, or the rights and freedoms of others. Finally, intervention must be considered "necessary in a democratic society." This criterion requires a balance between the competing interests of data protection and other public considerations. It requires that the interference be proportionate, meaning that it must be the least intrusive measure to achieve the legitimate aim pursued. of necessity the test also includes consideration of alternative means of achieving the same objective which would have less impact on the individual's right to data protection. Incorporating these criteria, Article 8(2) establishes a framework for assessing whether an interference with the right to data protection is justified and complies with human rights standards.

3. Compliance with the Law

Restrictions on the right to personal data protection must be regulated by law. This requirement implies that the restriction must have a legal basis that is accessible, foreseeable and formulated with sufficient clarity, which gives a person the opportunity to understand their duties and regulate their actions. The legal basis must clearly define the scope and form of exercise of authority by the relevant authority, which protects individuals from arbitrary interference.[6] In order for the intervention to be in accordance with the law, there are several prerequisites :

- There must be legislation in the state to process personal data;
- The legal basis requires that the processing of personal data is"necessary". If the State can reasonably achieve the same purpose without the processing, then the processing of the data is unlawful;
- The lawful basis for processing must be established prior to data collection;
- The purpose of data processing must not be changed to another legal basis at a later date, unless the reason for the change is justified;

[6] Necessity Toolkit - European Data Protection Supervisor, Necessity Toolkit, Brussels, 2017, 4.

- If a special category of data is subject to processing, both the legal basis for general processing and additional conditions for the processing of this type of data must be defined.[7]

The European Court of Human Rights considered whether personal data undergoing automatic processing must be received and processed fairly and lawfully, as provided for in the "Protection of Individuals with regard to Automatic Processing of Personal Data " (so-called Convention 108) of the Convention - in Article 5, then violation of Article 8 due to lack of legal basis. For example , in the case of Taylor-Sabor v. United Kingdom, the applicant was subject to police surveillance of his pager, and the legislative space did not provide for the control of information obtained as a result of the surveillance of pager messages[8]. The case of M.D. is similar. MD and others v. Spain, where the Court noted that, on the one hand, there was no domestic legal provision justifying the police action, and on the other hand, there were no guidelines. The court found that the police report of the judges and Magistrates' personal data, photos and political Disclosure of views was not provided for by the law and violated Article 8[9]. In other cases, the court found a violation of Article 8 because Domestic laws for the protection of personal data were either unavailable or confidential or not transparent. for example , in the cases of Vasil Vasilev v. Bulgaria and Nuh Uzun and others v. Turkey,[10] the Court established such issues as: Limited access to laws governing personal data or insufficient clarity of regulations[11]. In contrast, in Ben Faiza v. France, where the domestic law was clear, transparent and adequately safeguarded against potential Against violence, the court did not find a violation of Article 8[12]. In addition, the Court emphasizes that in cases involving covert surveillance measures, such as wiretapping, it is important to have clear and detailed rules to avoid arbitrary interference. The law should provide citizens with sufficient guidance on the circumstances and about the conditions under which state bodies can use the above measures. The Court noted that the law must indicate the scope of any discretion granted to the competent authorities and show the ways of its implementation with sufficient clarity so that subjects can adequately protect themselves from arbitrary interference.

Judicial practice also outlines specific elements that must be considered in the legislation regarding hearings, for example: defining the nature of offenses, specifying the categories of person's subject to hearing, establishing time limits and also data verification and storage procedures, and implementing security measures.

Regarding the collection and storage of personal data by the authorities for the purpose of preventing or punishing crime, case law emphasizes the need for clear and detailed rules, eg: in the case of Cathy v. United Kingdom, the Court explained that the collection of data was subject to the domestic legal framework, but the Court also distinguished that the data collection did not have a clearer and more understandable legal basis. The court noted that "domestic extremism " is interpreted differently by different agencies. Thus, it was unclear to the court, based on what criteria information about the citizen was collected. In the

[7] Guide to the General Data Protection Regulation (GDPR), Information Commissioner's Office, 2022, 19.
[8] *Taylor-Sabori v. the United Kingdom,* Application №47114/99, European Court of Human Rights, October 22, 2002, §19.
[9] *MD and Others v. Spain,* Application №36584/17, European Court of Human Rights, September 28, 2002, §§ 61-64.
[10] *Nuh Uzun and Others v. Turkey,* Application №49341/18, European Court of Human Rights, September 5, 2022, §§ 80-99.
[11] *Vasil Vasilev v. Bulgaria,* Application №7610/15, European Court of Human Rights - August 16, 2022, §§ 169-170.
[12] *Ben Faiza v. France,* Application №31446/12, European Court of Human Rights - May 8, 2021, §§ 58-61.

mentioned case, the court discussed not only the collection of data, but also their storage, the court pointed out that the domestic legislation did not provide for the maximum period of data storage. In addition, the applicant was not a threat to anyone (he was 95 years old), the records collected reflected the applicant's political views, which represented a special kind of data. Therefore, they were subject to high standards of protection. It was the sensitive nature of the data that represented the main essence of the case, on which the Court expressed its opinion: "When the powers granted to the state are vague, which creates a risk of arbitrariness, and when technologies are constantly developing and improving, it is important to check the compliance with the principles of Article 8 of the Convention." According to the court, the applicant had the right to request the erasure of the data, although there were no properly constituted procedural guarantees of data protection. The domestic legal framework stipulated that the data was kept for at least 6 years. Then the need to keep them was reviewed and evaluated. The case did not show whether the data was reclassified or not. The court noted that there should have been a maximum retention period for the data, in addition, the police had more information than was necessary, and the relevant agencies did not take into account the sensitive nature of the data.[13] In its decisions, the court emphasizes the importance of rules governing the duration, storage, use, access and destruction of such data, protecting their integrity and confidentiality.

4. Legitimate Purpose

In violation of Article 8, a legitimate purpose must also be established, which means that the personal data during the automatic processing must be collected for clear, specific and legitimate purposes. In these cases, the examination of legitimate aims that might justify interference with the exercise of Article 8 rights as enumerated in paragraph 2 is quite limited. The purposes of legitimate interference are: 1. National security, 2. Public safety and protection of the economic welfare of the country, 3. Prevention of disorder or crime, 4. Protection of health and morals or protection of the rights and liberties of others. The existence of one or more of these purposes, asserted by the Government, must also be shared by the Court under Article 8(2) to implement the objectives of the clause[14].

for example , the court found that the transfer of bank data to the authorities of another country based on a bilateral agreement served a legitimate purpose, as it contributed to the protection of the country's economic well-being[15].

Referring to international instruments that emphasize fairness and equal opportunities in the fight against doping, the Court found that the protection of health and morals justified the obligation to locate athletes in order to combat doping. In sports, the court linked this kind of action to what the government called "morality" with the legitimate aim of protecting the rights and freedoms of others , since the presence of doping agents encouraged amateur athletes, especially young people, to follow them [16]. It was determined that listening to the

[13] *Catt v. United Kingdom,* Application №43514/15, European court of Human Rights, January 24, 2019.
[14] Guide to Article 8 of the Convention - Right to Respect for Private and Family Life, European Court of Human Rights, 2022, 12.
[15] *GSB v. Switzerland,* Application №28601/11, European Court of Human Rights December 22, 2015, § 83.
[16] *National Federation of Sportspersons' Associations and Unions (FNASS) and others v. France),* Application №48151/11, №77769/13, European Court of Human Rights January 18, 2018, §§ 164-166.

telephone conversations of the director of the prison suspected of corruption, saving this information and disclosing it was aimed at preventing corrupt actions, ensuring transparency and openness in the public service. Thus, the legitimate aims were to prevent disorder or crime and to protect the rights and liberties of others [17].

In each case, the Court has consistently recognized the existence of one or more legitimate goals pursued by governments. These findings highlight the Court's obligation to balance the protection of personal data with the need to protect the legitimate interests of society.

5. Necessary in a Democratic Society

In order for any measure that interferes with the protection of personal data under Article 8 to be considered necessary in a democratic society, it must meet the criteria of pressing social need and must not be disproportionate to the legitimate aims. The reasons given by the government must be relevant and sufficient. Although the initial assessment is made by the national authorities, the final assessment of the need for intervention is subject to judicial review to ensure compliance with the requirements of the Convention. When it comes to the violation of rights, the court considers whether the legislation adopted by the state provides adequate protection of these rights.

Overall, in order to determine whether a measure to interfere with the protection of personal data is justified under Article 8 in a democratic society, the matter must be considered by the Court in accordance with the requirements of Article 5 of Convention 108.

The Court emphasizes the need for measures to intervene in the protection of personal data in order to maintain proportionality in the face of pressing social needs. It is the role of the Court to consider and assess the necessity of such intervention in the light of national assessments of whether it is consistent with the requirements of the Convention.

5.1. Collected or Recorded Data Minimization Request

Only those data that are "relevant and the volume does not exceed the purpose for which they were collected and/or processed" must be processed. The categories of data selected for processing must be necessary to achieve the stated purpose of the processing operations, and the processor must be strictly limited to collecting only those data that directly fit a specific purpose. The processing of personal data must be proportionate to the legitimate purpose served by the processing. At all stages of data processing, there must be a fair balance between all relevant interests. This means that " adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')".[18]

For example, according to the EU General Data Protection Regulation, the data collected must be: Adequate-enough to properly fulfill the intended purpose; relevant - to have a rational connection with this goal; Be limited to what is necessary - no more information than necessary should be stored.

[17] *Adomaitis v. Lithuania,* Application №14833/18, European Court of Human Rights, January 18, 2022, § 84.
[18] General Data Protection Regulation, Article 5 (1) (c).

Therefore, the minimum amount of personal data necessary to fulfill the purpose should be determined. But the question arises, how to understand what is adequate, appropriate and limited? Legislation will not be able to define these terms. However, this will obviously depend on the purpose of collecting and using the personal data. It can also vary from one individual to another. So , in order to assess whether the " right amount " of personal data[19] is stored , it is first necessary to find out the relevant purpose and the nature of the data . in his own practice as well.

For example, the court found a violation of Article 8 after the retention of information obtained from electronic devices seized during the search was not relevant to the case. Also, it did not appear that any kind of selection procedure was performed to minimize the amount of these data [20]. The court considered whether the automatically processed personal data were suitable, relevant and not excessive for the purposes for which they were recorded in various instances. In some cases, the Court found a violation of Article 8 of the Convention. These violations occurred because no procedures were followed to minimize the amount of data seized from the applicants' electronic devices during searches. The court's decision to publicly identify a non-participant (involved in a case of sexual harassment at the workplace), without protecting confidentiality, was considered unnecessary and potentially stigmatizing. In addition, the disclosure of personal data captured without the journalist's consent in the progress report of the investigation was considered excessive and pointless.[21]

According to the court, databases should not be designed to maximize the information to be stored in order to prevent and punish for a crime. The argument that storing more data leads to crime prevention does not justify storing information on the entire population, including deceased relatives, which is clearly excessive and inappropriate. The Court, in accordance with legitimate purposes, emphasizes the importance of adequate, appropriate and proportionate processing of personal data. Excessive retention and disclosure of data, without adequate safeguards, violates the rights and freedoms protected by Article 8 of the Convention. States need to strike a balance between the benefits of data retention and respect for individual privacy.[22]

5.2. Data Accuracy and Update Request

In accordance with EU and Council of Europe legislation, data subjects have the right to request the rectification of their personal data. Their accuracy is necessary to protect data subjects' personal information at a high level. [23]False or incomplete personal data collected and protected by the authorities may complicate the daily life of the subject of personal data protection, or may remove certain statutory procedural guarantees needed to protect the rights of the individual. Such data may be shared between different authorities, which may harm the personal or professional life of the data subject. It is the task of the authorities to verify the accuracy of the stored data. The Court of Human Rights has heard a number of

[19] Guide to the General Data Protection Regulation (GDPR), Information Commissioner's Office, 2022, 27.

[20] *Krugulov and others v. Russia,* Application №11264/04, European Court of Human Rights February 4, 2020, §123-138.

[21] *Khelili v. Switzerland,* Application №16188/07, European Court of Human Rights, October 18, 2011, § 62.

[22] Guide to European Data Protection Law, 2018, 144.

[23] General Data Protection Regulation, Article 16.

cases concerning the government's retention of data that was found to be inaccurate or whose accuracy was disputed by the data subject. Case law shows that data should be kept no longer than to fulfill the purpose for which they were obtained. In the case of S.And Marper v. United Kingdom[24], the Court noted that the permanent storage in a national database of the fingerprints, cellular samples and DNA profiles of persons accused but not convicted of a crime, regardless of the nature or seriousness of the crime of which the person was initially suspected, violates Article 8. for example, in the case of Anchev v. Bulgaria, where the applicant was subject to three investigations and, based on the archive, was "labeled" as a former employee of the security services. All this happened under a law aimed at exposing public officials who collaborated with the communist regime. However, the court dismissed the applicant's complaint, as he was given the right to access the archives and could later challenge the accuracy of the information. It is important to note that the court's decision in this case was specific to the circumstances presented. The Court recognized that providing the applicant with access to the archives and the opportunity to challenge the accuracy of the information was an appropriate remedy given the particular circumstances and the applicant's ability to present specific grounds for his appeal. Overall, this case highlights the importance of ensuring that people have the opportunity to review and challenge information held about them, particularly when it has the potential to affect their reputation and rights. Granting access to relevant archives enables authorized persons to present evidence to challenge the accuracy of such information, which is an important aspect of protecting their rights under the Convention.[25] Practice shows that the authorities must determine the accuracy of the stored data. Storing false or disputed information can have a detrimental effect on the data subject's daily life, reputation and procedural rights. It is very important that the authorities take care to ensure that data storage complies with the principles of accuracy and privacy of individuals, the latter of which is guaranteed by Article 8 of the Convention.

5.3. Limiting the Duration of Personal Data Storage (Requirement that Data Be Kept for No Longer than the Purpose for Which it Was Collected)

In several cases, the court considered the issue of limiting the duration of personal data storage. The court negatively evaluates the storage of data for an indefinite period, and, in addition, the period of data storage largely depends on the severity of the crime. The issue of permanent custody is particularly serious when it comes to minors because of their vulnerable situation, the importance of their development and integration into society [26]. for example , the court found a violation in the case of MK v. France, where the applicant was accused of book theft, but not convicted, and his prints were kept indefinitely [27], on the contrary, in the case - Martens v. Germany, the court declared the case, in which the personal

[24] *SS. and Marper v. the United Kingdom,* Application № 30562/04 and 30566/04, European Court of Human Rights, December 4, 2008, §§ 70-75.
[25] *Anchev v. Bulgaria,* Application №38334/08 - 68242/16, European court of Human Rights, December 5, 2017, §§ 112-115.
[26] Guide to the Case Law of the European Court of Human Rights/Data Protection, Council of Europe/European Court of Human Rights, 2022, 29.
[27] *MK v France,* Application № 19522/09, European Court of Human Rights, April 18, 2013.

data of the applicant was kept indefinitely, clearly unfounded, but the legislation called for reviews at regular intervals of no more than ten years to determine whether data was being retained. The duration is not necessarily decisive in relation to the retention period of the biometric data of convicts, the Court stated that the absence of a maximum period of data retention does not automatically violate Article 8. However, in such cases, procedural safeguards become crucial to ensure that the duration of data retention remains proportionate. Diligence by authorities in assessing and periodically reviewing the need to retain personal data becomes essential to maintain a balance between legitimate objectives and individuals' right to privacy. The duration of storage should depend on the degree of severity of the crime, the past actions of the accused, the strength of the suspicion that exists against the subject, these factors should be evaluated by the state and the proportionality of the storage should be determined in each case, taking into account the purpose of data storage and the nature and severity of the circumstances .[28]

The Court of Justice recognizes that there may be justified reasons for retaining personal data beyond a certain period, especially in cases involving serious crimes , however, the permanent retention of data relating to persons who have not been convicted of any crime, regardless of their age or suspicious nature, is incompatible with Art. 8 at the knee. Procedural safeguards and diligent oversight must be put in place to secure data.

5.4. Request to Restrict the Use of Data for the Purpose for Which They Were Recorded

Importantly, the requirement to limit the use of data to the purpose for which it was recorded is a recurring theme in court practice. The court emphasized the need for strict adherence to this principle in order to protect an individual's right to privacy. A few notable cases provide additional information on this requirement [29]:

For example, in the case of Karabeoglu v. Turkey, the Court found a violation of Article 8 because data obtained from wiretapping during a criminal investigation was used for another purpose, in a subsequent disciplinary investigation. The court emphasized that the use of data for purposes other than those that justified their collection may be a violation of the right to privacy [30]. The case of Surikov v. Ukraine concerned the long-term storage, dissemination and use of data about an individual's mental health for purposes unrelated to the original case. The court concluded that such practices constituted a disproportionate interference with the data subject's right to respect for private life. This case highlights the importance of ensuring that personal data is used only for the purposes for which it was originally collected [31].

Any deviation from this principle, e.g., using data for different purposes or improper disclosure, may violate an individual's right to privacy. The implementation of appropriate safeguards and access control is of crucial importance to ensure the protection of personal data and the protection of the rights of individuals under Article 8 of the Convention.

[28] *Peruzzo and Martens v. Germany,* Application №7841/08 and 57900/12, European Court of Human Rights, June 4, 2013, §§ 44-49.
[29] General Data Protection Regulation, Article 5 (1) (c).
[30] *Karabeyoğlu v. Turkey,* Application №30083/10, European Court of Human Rights June 7, 2016, §111-124.
[31] *Surikov v. Ukraine,* Application №42788/06, European Court of Human Rights, January 26, 2017, § 80-96.

5.5. Data Processing Procedures Transparency Request

In a number of cases related to personal data collected and stored by public authorities, the Court held that the authorities had a positive obligation to provide interested parties with an "effective and accessible procedure"[32] so that they could have access to "all relevant information." The subject of personal data has the right to request information about personal identity for discovery, of course, this requirement of transparency has little effect when the other side of the scale is national security information. The practice shows how important it is to make the legislation transparent and concrete in order not to exceed the discretion of the state bodies. In addition, it is emphasized that despite the powers of the state, the collection of personal data, the final assessment is the prerogative of the court, therefore, the court should be familiar with this issue in order not to allow misinterpretation of the law.

6. Conclusion

Respecting the private life of each person is one of the obligations of a democratic state, as it creates the basis for personal growth and development. Privacy is a haven for citizens where they can freely express their opinions, beliefs and identities without any judgment or fear. Respecting an individual's privacy helps to create an environment conducive to self-expression, creativity and the pursuit of individuality. In the context of data protection, the concept of privacy takes on additional importance. Our personal information is constantly collected, processed and shared with other authorities for companies, from online activities to financial transactions. Our digital footprints leave a wealth of data that can reveal details about our lives. Protecting the privacy of individuals in the digital realm is paramount. It ensures that individuals retain control over their personal information and have the freedom to decide how to use, share and store it. Respect for privacy allows individuals to make informed choices and maintain autonomy over their personal data. Furthermore, privacy is not just a matter of individual rights; It is the fundamental pillar of a democratic society. When individuals feel secure in their private lives, they are more likely to engage in open discourse, express diverse opinions, and contribute to the cultural, social, and intellectual fabric of society. States are obliged, first of all, to create such a legal framework that will be able to protect the data of their citizens, in addition, the problem is that the definition of personal data is changing and becoming more multifaceted. That is why there is a need for more involvement of judicial authorities in the aspect of personal data protection.

Data privacy protection is one of the most important issues. By protecting data, you protect individuals from unwarranted intrusions and surveillance. By valuing and protecting privacy, we create an environment that fosters individuality, self-expression, and the pursuit of personal growth.

[32] *Gaskin v. the United Kingdom,* Application №10454/83, European Court of Human Rights, July 7, 1989, § 40-60.

Bibliography:

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
2. Guide to European Data Protection Law, 2018, 144.
3. Guide to the Case Law of the European Court of Human Rights/Data Protection, Council of Europe/European Court of Human Rights, 2022, 7.
4. Guide to Article 8 of the Convention - Right to Respect for Private and Family Life, European Court of Human Rights, 2022.
5. *Korkelia K.,* Towards the integration of European standards: the European Convention on Human Rights and the experience of Georgia, Tbilisi, 2007, 14-15 (in Georgian).
6. Necessity Toolkit - European Data Protection Supervisor, Necessity Toolkit, Brussels, 2017.
7. *Adomaitis v. Lithuania*, Application №14833/18, European Court of Human Rights, January 18, 2022.
8. *Amann v. Switzerland*, Application №27798/95, Human Rights European the court big of the Chamber of February 16, 2000.
9. *Anchev v. Bulgaria,* Application №38334/08 - 68242/16, European Court of Human Rights, December 5, 2017.
10. *Ben Faiza v. France*, Application №31446/12, European Court of Human Rights, May 8, 2021.
11. *Catt v. United Kingdom,* Application №43514/15, European Court of Human Rights, January 24, 2019.
12. *Gaskin v. the United Kingdom*, Application №10454/83, European Court of Human Rights, July 7, 1989.
13. GSB v. Switzerland, Application №28601/11, European Court of Human Rights, December 22, 2015.
14. *Karabeyoğlu v. Turkey,* Application №30083/10, European Court of Human Rights, June 7, 2016.
15. *Krugulov and others v. Russia*, Application №11264/04, European Court of Human Rights, February 4, 2020.
16. *Khelili v. Switzerland,* Application №16188/07, European Court of Human Rights, October 18, 2011.
17. *MD and Others v. Spain*, Application №36584/17, European Court of Human Rights, September 28, 2002.
18. *MK v France,* Application №19522/09, European Court of Human Rights, April 18, 2013.
19. *National Federation of Sportspersons' Associations and Unions (FNASS) and others v. France,* Application №48151/11, №77769/ 13, European Court of Human Rights, January 18, 2018.
20. *Nuh Uzun and Others v. Turkey,* Application №49341/18, European Court of Human Rights, September 5, 2022.
21. *Peruzzo and Martens v. Germany,* Application №7841/08 and 57900/12, European Court of Human Rights, June 4, 2013.
22. *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland,* Application №931/13, European court of Human Rights, June 27, 2017.

23. *S. and Marper v. the United Kingdom,* Application №30562/04 and 30566/04, European Court of Human Rights, December 4, 2008.
24. *Surikov v. Ukraine,* Application №42788/06, European court of Human Rights of the Court on January 26, 2017.
25. Taylor-Sabori v. the United Kingdom, Application №47114/99, European Court of Human Rights, October 22, 2002.
26. *Vasil Vasilev v. Bulgaria*, Application №7610/15, European Court of Human Rights, August 16, 2022.