15 years ESJ
Special edition

Personal Data Protection: Cybersecurity Architecture in Georgia

Ekaterina Zakaradze, Academic Doctor of Public Administration
Associate Professor at Grigol Robakidze University, Georgia
Khatuna Muradishvili, Academic Doctor of Public Administration
Assistant Professor at Batumi Shota Rustaveli State University, Georgia

Doi:10.19044/esj.2025.v21n39p187

Submitted: 22 November 2024
Accepted: 27 February 2025
Published: 15 March 2025

Cite As:
Zakaradze E. & Muradishvili K. (2025). *Personal Data Protection: Cybersecurity Architecture in Georgia*. European Scientific Journal, ESJ, 21 (39), 187.
https://doi.org/10.19044/esj.2025.v21n39p187

Abstract

The modern world, with its growing dynamics, is becoming increasingly dependent on the digital realm. As a result of technological revolutions, digital technologies have become not only an integral part of daily human life but also one of the key instruments for regulating the relationship between the state and individuals. Against the backdrop of such changes, the need to develop mechanisms for protecting the digital world has emerged, in order to safeguard the essential data that is used for identifying individuals. Thus, the pace of technological development and the forms of personal data processing affect each of us in various ways on a daily basis. Consequently, a new challenge has arisen for the world: to develop a legal framework regarding the inviolability of private life and personal data protection. In Georgia, the protection of human rights and the processing of personal information is a top priority for the government. To achieve this, it is important to develop mechanisms that, on one hand, meet internationally recognized standards, and on the other hand, are precisely aligned with the current stage of Georgia's digital development. Another significant challenge facing the Georgian state is the analysis and monitoring of cybersecurity issues, as cyberattacks represent a serious threat to personal data protection.

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
1-2 November 2024, Tbilisi, Georgia

Keywords: Public Administration, Digital Technologies, Personal Data Protection, Cybersecurity

Introduction

The 20th century in world history could undoubtedly be called the "Leap of the Century." This is based on the rapid dynamics of civilization's development. The constant wars and processes of territorial formation of states were largely concluded by the Second World War, which also established human rights as a priority challenge. The individual and their legal relationship with the state became the main epicenter of governance. Despite the fact that legal conventions, acts, and international pacts regulated existing flawed approaches to the status of individuals within the state and created guarantees for their protection, it actually took several more decades for the full realization of these legislative achievements.

The creation of the global internet network set the stage for the world's rapid development, facilitating high-level communication and making information more accessible. All types of information, both personal and general, became available. As a result, the world developed further, and what was once regional in nature became global.

The 21st century introduces another giant in the digital industry: artificial intelligence. It is a product of the present, which, while simplifying life, also brings many challenges for both producers and consumers. One of the significant challenges concerns the boundary that lies between the benefits of artificial intelligence and personal data.

With all of the above-mentioned advances, threats have also emerged, presenting great challenges to the modern world. It should be noted that every innovation comes with side effects, and failing to address these could potentially turn the world into the epicenter of opposing phenomena. Thus, at the end of the 20th century, cybersecurity problems began to emerge, and the world started to fight against them, facing significant difficulties.

In the modern era, cybercrime has become quite widespread, with incidents such as online fraud, unauthorized access to computer systems, and unauthorized use of computer systems and data. Along with the state's dependence on critical infrastructure through information technologies, the challenges related to protecting Georgia's information space have increased.
Georgia actively collaborates with all international organizations to, on one hand, develop digital technologies and implement them fully into modern life, and on the other hand, ensure the protection of digital security to safeguard personal data to the greatest extent possible. The state also aims to control the potential misuse of political or commercial information in both the public and private sectors.

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
1-2 November 2024, Tbilisi, Georgia

Thus, personal data protection is one of the significant challenges of public administration in Georgia, and its effectiveness depends on the development of an effective and well-structured cybersecurity architecture. These elements must align to ensure the maximum protection of individual rights and the effective implementation of both domestic and foreign policies by the state.

Literature review

In recent years, the modern world has faced a new challenge. Technological development is advancing rapidly, bringing both positive aspects and significant risks. It is the responsibility of each state to thoroughly examine these issues and, in particular, focus on risks such as cybersecurity and the protection of personal data. A number of international instruments have been adopted to strengthen the fight against cybercrime and enhance cybersecurity regulation. These instruments create a legal framework that ensures cooperation between states, reduces cybersecurity risks, and helps prevent cybercrime.

- ✓ In 2001, the **Budapest Convention on Cybercrime** was adopted. The Budapest Convention is the first international treaty aimed at establishing a legal framework for combating cybercrime. "Each party is required to adopt such legislative and other measures as may be necessary to criminalize unauthorized access to the whole or any part of a computer system, if the act is committed with intent." [Chapter II, Article 2]

The Budapest Convention provides for cooperation between member countries to protect computer systems and data, as well as the harmonization of legal procedures related to cybercrime. Many countries, including EU members, the United States, and others, have joined this convention (“Use of Artificial Intelligence Systems in Georgia,” 2021); (Georgian Research and Educational Networking Association, n.d.).

On June 1, 2012, in accordance with Article 18 of the Law of Georgia on "International Treaties of Georgia," the decree No. 450 of the President of Georgia was issued to enforce the Convention on Cybercrime of November 23, 2001. The decree approved the convention, with the conditions specified in the annex of the decree, and under this legal act, Georgia undertook the obligations stipulated by the convention (Decree No. 450 of the President of Georgia, 2012).

- ✓ The **United Nations** began discussing the potential critical impacts of information infrastructure in the 1980s. Later, the organization adopted a number of initiatives aimed at coordinated actions. To strengthen international information security in the global digital space, the UN

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
1-2 November 2024, Tbilisi, Georgia

Institute for Disarmament Research (UNIDIR[1]) organized several seminars.

In December 2000 and 2001, the UN General Assembly adopted resolutions No. 55/63 and No. 56/121 titled "Combating the Criminal Use of Information Technologies." In December 2002, the UN General Assembly's 57th session adopted Resolution No. 57/239 on "Creating a Global Culture of Cybersecurity." In December 2003, during the 58th session, the UN General Assembly adopted Resolution No. 58/199 on "Creating a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructure." The annex of this resolution formulates eleven principles for the protection of critical information infrastructure (Svanadze, 2015).

As for international instruments and regulations concerning the protection of personal data, these are relatively new in international legal space. As a parallel to the fight against cybercrime, the open internet space became vulnerable to the disclosure of personal data, which created a favorable ground for cybercrime. International instruments on personal data protection aim to safeguard individuals' data, ensure transparency in data processing, and establish universal standards for data protection.

- ✓ **The General Data Protection Regulation** (GDPR) of Europe is one of the European Union's most strictly regulated and influential data protection regulations, designed to protect the personal data of EU citizens. In terms of personal data protection, the regulation recognizes the fundamental right of individuals to have their personal data processed. According to Article 8(1) of the EU Charter of Fundamental Rights ("the Charter") and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU), everyone has the right to the protection of their personal data.
- ✓ **Directive 95/46/EC of the European Parliament and the Council** aims to harmonize the process of protecting the fundamental rights and freedoms of individuals in data processing and to ensure the free movement of personal data between member states (Directive 95/46/EC, 1995).
- ✓ **The OECD** published a very interesting report on manipulative business models. The report discusses the effectiveness and harm of manipulative business models and defines potential approaches that consumers and businesses can adopt to reduce them. The term "manipulative business models" refers to a variety of practices commonly found in online user interfaces. Manipulative business practices typically force consumers to spend more money, disclose less personal data, or devote less time and attention to issues than is

[1] UNIDIR1- The United Nations Institute for Disarmament Research

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
1-2 November 2024, Tbilisi, Georgia

desirable. The report proposes educational, technical, and business initiatives to address manipulative business models ("OECD Publishes a Report on Manipulative Business Models," 2022).

Thus, international practices in the fight against cybercrime and personal data protection reflect the modern world's latest challenges, with Georgia actively engaging in these efforts as a member of numerous international organizations. Georgia is gradually joining these legal instruments, which have led to the creation of various legislative acts. Of course, this process is still ongoing, and it is gradually taking shape and becoming more comprehensive.

Personal Data Protection Mechanisms in Georgia

According to Article 8 of the European Convention on Human Rights, the right to personal data protection is part of the right to respect for private and family life, home, and correspondence. Under EU legislation, data protection is recognized as an independent fundamental right. This is reinforced by the Treaty on the Functioning of the European Union, specifically Article 16, and by Article 8 of the Charter of Fundamental Rights of the European Union. Data protection in EU law was first regulated by the Data Protection Directive in 1995. Considering the rapid technological development, the EU adopted new legislation in 2016 to adapt data protection rules to the digital age. In May 2018, the General Data Protection Regulation (GDPR) came into force, which replaced the Data Protection Directive (Asvanua, 2023).

Along with the General Data Protection Regulation, the EU also adopted legislation to protect data processing by state authorities. Directive (EU) 2016/680 establishes the rules and principles of data protection concerning personal data processing, aiming to prevent, investigate, detect, prosecute, or enforce criminal penalties.

In line with EU legislation, the Parliament of Georgia adopted the **Law on Personal Data Protection** on June 14, 2023 (Document Number 3144-XI). The aim of this law is to protect the fundamental rights and freedoms of individuals, including the right to respect private and family life, personal space, and communication during personal data processing (European Union Agency for Fundamental Rights [FRA], 2018).

Personal data protection involves a range of procedural measures. First and foremost, it is essential to ensure that data protection complies with the law. Thus, the law specifically defines what constitutes legal data processing, which includes several basic principles that must be upheld during personal data processing. For example, data must be processed lawfully, fairly, and transparently, without infringing on the dignity of the data subject. Data

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
1-2 November 2024, Tbilisi, Georgia

should only be collected or obtained for specific, clearly defined, and legitimate purposes. It must be processed only to the extent necessary to achieve the relevant legitimate purpose. Furthermore, data must be accurate, complete, and, if necessary, kept up to date (The Law of Georgia on Personal Data Protection).

Data may only be retained for the period necessary to fulfill the legitimate purposes for which it was processed. Afterward, it should be deleted, destroyed, or stored in a depersonalized form. To ensure data security, technical and organizational measures must be taken during data processing to protect the data from unauthorized or unlawful processing, accidental loss, destruction, or damage.

Personal data processing without a valid legal basis is prohibited. It must be processed based on the subject's consent or in cases expressly provided by law. To implement the principles and conditions mentioned above, it is essential for organizations to appoint a **Data Protection Officer (DPO)** to develop and adapt personal data protection mechanisms within the legal framework.

Data protection also extends to biometric data processing, proper implementation of video and audio surveillance, and data processing for direct marketing purposes.

Main Text

Regarding the transfer of data to another state or international organization, it is permissible if the legal requirements for data processing are met and adequate safeguards for data protection and the protection of the data subject's rights are ensured in the receiving country or organization.

For effective personal data protection, the implementation of a comprehensive **Data Protection System** is essential. This procedural mechanism includes elements such as:

- **Approval of a list of persons** who are authorized to access personal data. It is necessary to establish a warning procedure to ensure these individuals are aware of their responsibility to protect data.
- **Approval of a list of personal data** being processed within the organization and ensuring employees are informed about these processes through confidentiality agreements.
- **Technical protection mechanisms** can include:
    - **Physical measures**, restrict access to the information storage system.
    - **Hardware-based security**, which includes active (e.g., electromagnetic noise generators, vibration acoustic protection) and passive (e.g., screens, filters, additional grounding systems) devices.

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
1-2 November 2024, Tbilisi, Georgia

- **Software-based security** tools, including antivirus programs and data encryption software (cryptographic programs) (Asvanua, 2023).

The main goal of each of these mechanisms is to ensure the correct processing, storage, access, and protection of personal data. The final goal is especially critical, as there is information that should not be stored for extended periods. For example, after data is used, it should be deleted. If long-term data storage is necessary, appropriate protection measures must be in place to prevent cyberattacks.

Cybersecurity and Its Necessity in Georgia

In the modern world, ensuring the security of cyberspace and the protection of electronic information has become increasingly important. With the rapid development of information technologies, the state's dependence on critical infrastructure has also grown. In this context, preventing unauthorized access to cyberspace and strengthening defensive measures has become crucial.

Georgia's goal is to establish an information security system that minimizes the harmful consequences of any cyberattack and ensures the quick restoration of information infrastructure to full functionality after such an attack. Consequently, Georgia places great emphasis on ensuring the security of classified information and the protection of the state's information systems. The country is developing the necessary legislative infrastructure, which is essential for improving information technologies and ensuring the protection of information. Moreover, cooperation with friendly countries and the sharing of their experiences is crucial for ensuring cybersecurity (The Law of Georgia on Information Security).

It is widely recognized that the most vulnerable and sensitive sectors today are the banking sector, other financial institutions, stock exchanges, and key sectors where personal data is stored.

Over the past decade, the standards of cybersecurity and personal data protection in Georgia have significantly developed both at the legislative and practical implementation levels. In both areas, the country has established an organizational and institutional framework, enhanced the qualifications of specialists in these fields, and created the necessary strategic and legislative frameworks. These frameworks are expected to create favorable conditions for the development of cybersecurity and personal data protection, alongside regulatory measures.

Despite the development of cybersecurity and personal data protection standards, there remain significant challenges in these fields, given the global challenges and the dynamic nature of cybersecurity and data protection. These

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
1-2 November 2024, Tbilisi, Georgia

challenges persist in both private and public sectors. An illustrative example of this is the 2020 annual report of the State Inspector's Service, which highlighted that breaches related to data security measures increased by 10% compared to 2019.

As a country within the process of European legal culture development and European integration, Georgia is continuing to advance and align its national legislation with European regulatory standards. The adoption of European cybersecurity and personal data protection standards is another significant step toward Georgia's integration into the unified European digital market. Georgian citizens will benefit from high cybersecurity standards, with effective and operational mechanisms for the protection of human rights and freedoms, including the inviolability of private life, during the processing of personal data (Svanaze & Gotsiridze, 2015).

After the implementation of cybersecurity systems, several cases of cyberattacks have been recorded in Georgia, on which the cybersecurity program has worked quite effectively. All of this highlights the country's progress in this direction. Here are a few examples of such incidents:

- **2019 Cyberattack**: In July 2019, a large-scale cyberattack was carried out in Georgia, targeting various state and private sectors, including media companies, banks, and microfinance organizations. This incident was followed by a strong and rapid response from the country's cybersecurity program. Specifically, CERT.GE (the Computer Incident Response Team, established by the Georgian Scientific-Educational Computer Networks Association) was able to neutralize the hacker attacks and take necessary measures to protect critically important systems. Following the incident, the Georgian government announced that in the future, the private sector and government agencies would collaborate more closely on cybersecurity matters.
- **Cybersecurity Measures Before the 2020 Parliamentary Elections in Georgia**: In 2020, ahead of Georgia's parliamentary elections, the government strengthened its cybersecurity measures. The special operations carried out during this period successfully reinforced information security in the election process and prevented serious cyberattacks. CERT.GE and other relevant authorities played a significant role in this, constantly monitoring and identifying potential threats.

As a result of these specific incidents and actions, Georgia demonstrated that it has strong and rapid response systems for preventing and mitigating cyberattacks, which enhances the country's defense capabilities in

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
1-2 November 2024, Tbilisi, Georgia

the field of cybersecurity (Georgian Research and Educational Networking Association, n.d.).

In recent years, Georgia has been actively working on improving its cybersecurity systems, although there are still several gaps and challenges that require attention. These issues are primarily related to a shortage of human resources, as well as organizational and technological factors. Based on the materials we have studied, here are a few types of flaws and ways to address them:

- **Problems in the Private Sector Regarding Cybersecurity**
  Flaw: Despite the significant cybersecurity measures taken in Georgia's state and some private sectors, many companies and organizations still lack sufficient cybersecurity culture and systems. This is particularly evident in small and medium-sized businesses, which may not have the necessary security measures in place.
  Recommendation: It is essential to implement and expand educational programs on cybersecurity so that information security is adopted at all levels, starting from small businesses. The government should support small and medium-sized businesses to help them implement modern security systems within their organizations. CERT.GE's role in expanding its interactions with these organizations could also be significant.
- **Deficit of Professional Human Resources**
  Flaw: There is still a shortage of personnel in Georgia, especially in newer fields like cybersecurity. The number of cybersecurity specialists is insufficient to protect the country's critical infrastructure.
  Recommendation: There should be an increase in the training of cybersecurity specialists at the local level by creating relevant educational programs. Additionally, young people's interest in this field should be encouraged. To motivate this, scholarships, educational projects, international training programs, and other initiatives could be developed and implemented in collaboration between the government and the private sector.
- **Lack of Awareness About Cybersecurity Among Citizens**
  Flaw: Despite public services being prepared to respond, a significant portion of the population is still unaware of how to protect their personal information in cyberspace and how to prevent cyberattacks.
  Recommendation: It is necessary to raise public awareness about cybersecurity, which includes both the prevention of cyberattacks and the dissemination of information about safe online platforms. There should be campaigns designed to educate the public, such as advertising spots, informational messages displayed before accessing internet portals, and providing citizens with short text messages

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
1-2 November 2024, Tbilisi, Georgia

containing cybersecurity information. All of this would help promote greater awareness.

However, it is also important to note that before the 2008 Russo-Georgian War, Georgia's state websites were subjected to cyberattacks from 30 countries using DDOS (Distributed Denial of Service) techniques, including the President's website. As a result, a decision was made to protect the server in the United States (Tsatsanashvili & Zakaradze, 2018).

These key problems and their solutions will, to some extent, contribute to strengthening Georgia's cybersecurity system and, more broadly, to creating a safer environment for the country.

Conclusion

In conclusion, Georgia is actively engaged in all international processes related to the implementation and development of digital and electronic systems. Recent reforms in the Justice House and the Revenue Service have demonstrated that the country's economic development requires the digitization of services, which has led to faster service delivery, enhanced communication, and the rapid penetration of markets in neighboring countries. These reforms have also facilitated the inflow of investments and strengthened the export potential of the Georgian market. The digitization of services in the Justice House has simplified interactions between individuals and the state, making all the products offered by the state to citizens more accessible.

Alongside these achievements, Georgia's main objective remains ensuring cybersecurity, which involves strengthening personal data protection to prevent misuse and criminal exploitation of data. The Georgian Law on "Information Security" defines how, in the case of a personal data security breach or a cyberincident, competent cybersecurity authorities cooperate with the State Inspector's Office. An information exchange protocol and legal-procedural norms have been established.

While the laws of Georgia, namely the **Law on Personal Data Protection** and the **Law on Information Security**, have different objectives and scopes, they share significant legal and practical overlaps, particularly concerning personal data protection in cyberspace. Therefore, it is advisable for the responsible authorities in these areas to enhance cooperation, increase the intensity of their collaboration, and coordinate their actions more effectively.

Ultimately, Georgia's cybersecurity architecture is a system that incorporates strong cyber-defense mechanisms, and recently, a personal data protection structure has been added to this system to ensure the proper and effective realization of constitutional rights, serving as a guarantee of peace and security in the country.

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
1-2 November 2024, Tbilisi, Georgia

Georgia could strengthen its cybersecurity infrastructure by further refining its cybersecurity strategy, as there is a need to establish a strategy that defines objectives such as reliability, availability, confidentiality, and resilience. It is also important to further strengthen the National Cybersecurity Center and ensure an adequate response to modern challenges.

Enhancing international cooperation in the field of cybersecurity requires a multifaceted and long-term approach, based on common goals, shared experience, and strategic partnerships. In our view, as an associated country of the European Union and NATO, as well as in the context of deepening cooperation with other international organizations and partners, Georgia could strengthen itself in several key areas:

- A consistent process of developing cybersecurity standards and frameworks;
- Establishing a common mechanism for responding to cyberattacks (drawing on the examples of experienced countries);
- Introducing international educational and training programs in Georgia;
- Strengthening platforms for information exchange and partnerships.

The detailed discussion of the issues in the previous chapters has shown that Georgia is still facing challenges in the protection of cybersecurity. These challenges can generally be categorized as follows:

- Weaknesses in technological infrastructure;
- Increase in cyber-attacks;
- Protection of critical infrastructure;
- Shortage of skilled personnel;
- Lack of a centralized cybersecurity strategy.

In relation to the personal data protection issues we discussed, which are also contemporary developments in Georgia's legal space, several key challenges have emerged:

- Compliance with data processing regulations;
- Data breaches and their harmful use;
- Low public awareness;
- Challenges related to the enforcement of legislation;
- Intersection of cyber defense and data protection.

As noted above, Georgia is actively cooperating with all international organizations to address these challenges and overcome them in the shortest possible time. We have developed several recommendations that we believe will help the relevant institutions better tackle these challenges:

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
1-2 November 2024, Tbilisi, Georgia

Regarding cybersecurity:

- **Strengthening infrastructure**: Implementing modern technologies to protect critical systems.
- **Cybersecurity strategy**: Refining the national cybersecurity strategy and improving regulations.
- **Education and qualification**: Training specialists and raising public awareness about the importance of cybersecurity.
- **International partnerships**: Participating in cybersecurity programs with the support of NATO and the EU.

Regarding personal data protection:

- **Integration of GDPR standards**: Harmonizing legislation with European regulations.
- **Strengthening oversight**: Enhancing the resources of the Personal Data Protection Inspector's office.
- **Regular awareness campaigns**: Raising public awareness about data processing rules.
- **Openness and transparency**: Ensuring transparency in data processing by the public and private sectors.

As for international relations and support, the following is recommended:

- Collaboration and strengthening of strong international institutions (such as the UN, NATO).
- Developing common strategies and sharing information;
- Taking specific measures against any changes;
- Using innovations and technologies to enhance security.

Ultimately, Georgia's cybersecurity architecture is a system that incorporates strong mechanisms for cyber defense, and recently, a structure for personal data protection has been added to this system to ensure the proper and effective realization of constitutional rights, which serves as a guarantee of peace and security in the country. Security issues require an interdisciplinary approach, where all sectors actively participate in addressing them.

Conflict of Interest: The authors reported no conflict of interest.

Data Availability: All data are included in the content of the paper.

Funding Statement: The authors did not obtain any funding for this research.

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
1-2 November 2024, Tbilisi, Georgia

References:

1. Asvanua, N. (2023). *"Personal Data Protection Mechanisms"* . 1st edition, Tbilisi: Universal Publishing House. ISBN 978-9941-33
2. European Union Agency for Fundamental Rights (FRA). (2018). *"Handbook on European Data Protection Law".* Luxembourg: EU Publishing House. ISBN 978-9941-9658-9-0
3. The Law of Georgia on "*Personal Data Protection".*
4. The Law of Georgia on *"Information Security".*
5. Svanaze, V.; Gotsiridze, A. (2015). *"Cyber Defense: Key Actors in Cyberspace. Cybersecurity Policy, Strategy, and Challenges"* (Collection of Works and Articles), Ministry of Defense of Georgia, State Cybersecurity Bureau. Tbilisi.
6. Article *"Use of Artificial Intelligence Systems in Georgia - Legislation and Practice".* (2021). Available at: https://idfi.ge/ge/artificial%20intelligence_international_tendencies_and_georgia
7. Geogian Research and Educational Networking Associaliton.
8. Decree No. 450 of the President of Georgia, June 1, 2012, "On the Approval of the Convention on Cybercrime". Available at: https://www.matsne.gov.ge/ka/document/view/1665167?publication=0
9. Svanadze, V. (2015). "Cyberspace and Cybersecurity Challenges (Collection)". Available at: https://gipa.ge/uploads/files/Cyber_Protection.pdf
10. Directive 95/46/EC of the European Parliament and Council, October 24, 1995, on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (OJ L 281, 23.11.1995, p. 31). Available at: https://eur-lex.europa.eu/eli/dir/1995/46/oj/eng
11. Article: "OECD Publishes a Report on Manipulative Business Models" (2022).
    Journal "World Practice" Personal Data Protection Service. Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/the-intersection-between-competition-and-data-privacy_b5ac1ae6/0dd065a3-en.pdf
12. Tsatsanashvili, M.; Zakaradze E. (2018). "*Homo Informaticus and Information Safety in Georgia".* Tangible and Intangible Impact of Information and Communication in the Digital Age. Khanty-Mansiysk. Siberia.