

Cyber-Security Regulation in Albania

Lecturer **Edvana TIRI**¹
Lecturer **Erjola ALIAJ**²

Abstract

The increasing access to cyberspace and its resources is having a significant impact on our societies and our daily lives, profoundly transforming the way we live, work and interact. The importance of cyber security converts into the need to keep information, data and devices private and secure. Cyber-security is an essential element for the flat functioning of all critical information infrastructures. In this context, the treatment of cyber-security in this paper is concrete, taking into account the cyberattack that our country went through, which was aimed at destroying critical structures and testing the capacities of Albania. It is worth noting that a secure cyber environment cannot function without giving it the opportunity to have the relevant mechanisms. Specifically, increasing cyber resilience in critical information infrastructures are flexible cyber security measures, which focus on the flat functioning of online public services keeping in focus the real threats and the risk management plan. Furthermore, within the framework of commitments as a candidate country of the European Union, Albania is meticulously implementing all European acts and international standards for the drafting of a consolidated and stable legal framework. In the present paper, through a legal assessment, special attention has been paid to the National Strategy for the period 2021-2023 and legal rules on cyber-security in the Albanian legislation, aiming to analyze the legal provisions, which regulate it in this regard. Also, an important objective of this paper is also the fact that it may serve as an important basis for further studies in this field. The analysis of the cyber-security legal regulation in Albania is based on the qualitative method, which contains also the research, analytical, descriptive, interpretive methods. The results of this paper, which treats an innovative topic, will stimulate debate in the academic level and contribute to the legal doctrine in Albania that lacks such.

Keywords: cyber-security, national strategy, legal regulation, Albania.

JEL Classification: F52, K24

1. Introduction

In the present paper, through a legal assessment, will be analyzed the National Strategy for the period 2021-2023 and legal rules on cyber-security in the Albanian legislation. This paper does not purport to serve as an exhaustive analysis of the above documents, but rather, aims to provide a general overview of the regulatory approach in relation to cyber-security in Albania.

The primary goal is the analysis of the abovementioned documents, focusing, initially on the conceptual assessment of cyber space and security, main goals, measures and principles defined in the National Strategy for the period 2021-2023, as well a general provision regulating cyber-security in Albania. The analysis of the cyber-security legal regulation in Albania is based on the qualitative method, which contains also the research, analytical, descriptive, interpretive methods.

As a result of the lack of doctrinal treatments and judicial practice in Albania in relation to cyber-security, we conclude that this paper is an attempt to make an important contribution to this specific topic, which constitutes innovation for Albanian topicality, as well as stimulates debate as a whole, especially in the academic level.

2. Cyber space and security conceptual assessment

Cyberspace offers countless opportunities for economic development, social interaction and political exchange³. It has provided the means to carry out illegal surveillance, collect personal data,

¹ Edvana Tiri - Faculty of Political and Legal Sciences, "Aleksander Moisiu" University, Albania, eda_tiri@yahoo.com.

² Erjola Aliaj - Faculty of Law, Mediterranean University of Albania, erjolaaliaj@umsh.edu.al.

³ 'In the context of the development of international economic law, a series of norms and principles inspired by the international law were promoted in the investment field, going as far as creating some bodies and institutions that guarantee or settle the disputes in this field.' Cristina Elena Popa Tache, *Individualization and development of international investment law as the third millennium law field*, "Juridical Tribune - Tribuna Juridică", Volume 9, Issue 3, December 2019, p. 587.

influence democratic processes, commit crimes and change the means and methods of warfare⁴. The nature of cyberspace as an abstract concept seemingly ungrounded in the physical world has led to a lack of clarity as to what is meant by the term.⁵

Often the organizations and nations define cyberspace in a way that best suits their purpose or use. Often these definitions focus on the security, militarization, or vulnerabilities present within cyberspace, with each organization, nation, and group emphasizing different aspects. However, there is a common theme found in most definitions: *cyberspace is an environment constituted by physical and virtual components, where data, information or communication are stored, modified or exchanged*.⁶

Although the Internet may be the most common and easily accessible form of cyberspace for the average citizen, it is far from its only aspect.⁷ Cyberspace includes any computer-based network system for the aforementioned purposes of storage, modification, or exchange,⁸ as can be found in the growing number of clocks, devices, and other connected items in cyberspace (also known as IoT). All these various flows of data and information constitute the "virtual" construct called cyberspace.

Some examples of cyberspace definitions currently in use:

Cyberspace, as per International Telecommunication Union, is the environment in which communication between computer networks takes place. And almost everyone in one way or another relates to it.

Referring to International Organization for Standardization, cyberspace is the compound environment resulting from the interaction of people, programs and services on the Internet by means of technological devices and related networks, which does not exist in any physical form.

*According to European Union, cyberspace is a set of tangible and intangible time-dependent assets that store and/or transfer electronic information.*⁹

*In South Africa, cyberspace means a physical and non-physical created terrain and/or consisting of some or all of the following: computers, computer systems, networks and their software, computer data, content data, traffic and user data.*¹⁰

With the expansion of cyberspace use by governments as well as individuals and companies, the amount of sensitive data and information within cyberspace is growing exponentially as the

⁴ Emerging technologies have been extensively used in the war in Ukraine. Both Russia and Ukraine have deployed a range of innovative military technologies, from armed drones and electronic warfare systems to cyberattacks and AI-enabled intelligence gathering. Marina Favaro & Heather Williams (2023) *False Sense of Supremacy: Emerging Technologies, the War in Ukraine, and the Risk of Nuclear Escalation*, Journal for Peace and Nuclear Disarmament, DOI: 10.1080/25751654.2023.2219437, available at: <https://www.tandfonline.com/doi/full/10.1080/25751654.2023.2219437>.

⁵ *Udhëzues për qeverisjen e mirë me sigurinë kibernetike*. Geneva Center for Security Sector Governance. 2019. p. 27. Available online at https://dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_AL_Jan2021_0.pdf. Last access on March 21st, 2023.

⁶ Ibid. p. 27.

⁷ Schreier F., Weekes B., Winkler Th., *Cyber security: The Road Forward*, "DCAF Horizon 2015". Working Paper No. 4, Geneva: Democratic Control of Armed Force, p. 8. Available online at <https://www.dcaf.ch/sites/default/files/publications/documents/Cyber2.pdf>. Last access on March 21st, 2023. See also *Udhëzues për qeverisjen e mirë me sigurinë kibernetike*. Geneva Center for Security Sector Governance. 2019. p. 27. Available online at https://dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_AL_Jan2021_0.pdf. Last access on March 21st, 2023.

⁸ Buckland B., Schreier F., Winkler Th., *Democratic Governance Challenges of Cybersecurity*, "DCAF Horizon 2015" Working Paper no. 1. Geneva: Democratic Control of Armed Forces, p. 9. Available online at https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf. Last access on March 21st, 2023. See also *Udhëzues për qeverisjen e mirë me sigurinë kibernetike*. Geneva Center for Security Sector Governance. 2019. p. 27. Available online at https://dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_AL_Jan2021_0.pdf. Last access on March 21st, 2023.

⁹ *Udhëzues për qeverisjen e mirë me sigurinë kibernetike*. Geneva Center for Security Sector Governance, 2019. p. 29. Available online at https://dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_AL_Jan2021_0.pdf. Last access on March 21st, 2023.

¹⁰ *ENISA overview of cybersecurity and related terminology*. ENISA. Version 1, September 2017. p. 7-8. Available online at <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology>. Last access on March 21st, 2023. See also *Udhëzues për qeverisjen e mirë me sigurinë kibernetike*. Geneva Center for Security Sector Governance. 2019. p. 29. Available online at https://dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_AL_Jan2021_0.pdf. Last access on March 21st, 2023.

number of new and ever-changing vulnerabilities increases.¹¹

Effective protection of this information is essential to creating a secure environment in and out of cyberspace. Cybersecurity, as the name would suggest, consists of the practices and methods of securing the data, information and integrity of the various components of cyberspace, including but not limited to the physical aspects of the medium.¹²

Although cyber security is often associated with national security strategies, to ensure a more secure cyberspace environment within their country, some norms are emerging regarding the extent of their power over cyberspace, as well as the way in which states can exercise power over cyberspace.¹³

In general, cybercrime¹⁴ is on the rise in both developed and developing countries. By its very nature, cybercrime is transnational, being beyond national borders. They mostly do not need to be in the same country as the victims or the police force pursuing them. This constitutes one of the main challenges in the fight against cybercrime, as differences in the legal systems and practices of the various countries involved can affect the efficiency and feasibility of cooperation, as well as the exchange of intelligence and evidences.¹⁵

Given the broad and competing definitions of cyberspace and cyber security, it is created the Global Cyber Security Index, which evaluates five different aspects of cybersecurity, legal, technological, organizational, capacity building and cooperation, in order to assess the commitment of a nation. Even though it is a good tool to evaluate the reaction and actions of a government to the cyberspace dominance, it neglects the role of the non-state actor in both cyberspace and cyber security. Since it evaluates policies and not practices, it does not take into account the practical impacts or effectiveness of these commitments.¹⁶

There has been much discussion and confusion about how legal frameworks can and do apply in cyberspace. Due to its cross-border nature, cyberspace poses a challenge to centralized state governance. On the one hand, the physical infrastructure that constitutes cyberspace is subject to national jurisdiction and authority. On the other hand, the flow of data and information across that infrastructure constantly crosses (multiple) territorial jurisdictions, making it difficult for a legal jurisdiction to exercise "effective control" over this flow of information.¹⁷

While some norms for safe practices in cyberspace and a general framework of legal expectations of rights within cyberspace have been established at the international and regional levels, there is now an increased focus on the need for coherent and holistic national approaches to the challenges of cyberspace. The continued reliance on cyberspace means that effective national legislation, policies and strategies are more than necessary to protect the data, information and knowledge transmitted and used in cyberspace, as well as to increase the security of citizens in it.¹⁸

Consequently, governments have a key role in ensuring good cyber security governance by:

¹¹ Buckland B., Schreier F., Winkler Th., *op. cit.*, p. 9. Available online at https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf. Last access on March 21st, 2023. See also *Udhëzues për qeverisjen e mirë me sigurinë kibernetike*. Geneva Center for Security Sector Governance, 2019, p. 30. Available online at https://dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_AL_Jan2021_0.pdf. Last access on March 21st, 2023.

¹² *Cfare eshte siguria kibernetike?* Drejtoria e Përgjithshme e Teknologjisë së Informacionit, Inovacionit dhe të Dhënave. 2023. Available online at <https://dptiidh.tirana.al/cfare-eshte-siguria-kibernetike/>. Last access on March 21st, 2023.

¹³ *International Cybersecurity Norms*, Microsoft Policy Papers. Digital Geneva Convention, 2019. Available online at <https://www.microsoft.com/en-us/cybersecurity/content-hub/international-cybersecurity-norms-overview>. Last access on March 21st, 2023. See also *Udhëzues për qeverisjen e mirë me sigurinë kibernetike*. Geneva Center for Security Sector Governance. 2019, p. 30. Available online at https://dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_AL_Jan2021_0.pdf. Last access on March 21st, 2023. See also *Guide to developing a National Cybersecurity Strategy*. ITU, 2018. Available online at https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf. Last access on March 21st, 2023.

¹⁴ "Cybercrime" is defined as a crime in which a computer is the object of a crime (hacking, phishing, spamming) or is used as a tool to commit a criminal offense. Cybercriminals can use computer technology to gain access to personal data or use the Internet for exploitative or malicious purposes.

¹⁵ *Udhëzues për qeverisjen e mirë me sigurinë kibernetike*. Geneva Center for Security Sector Governance, 2019, p. 31. Available online at https://dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_AL_Jan2021_0.pdf. Last access on March 21st, 2023.

¹⁶ *Ibid.*

¹⁷ *Ibid.*, p. 41.

¹⁸ *Ibid.*, p. 59.

1. developing, adopting and updating national laws, policies and strategies to regulate cyberspace and to meet current challenges in cyberspace, including the areas of privacy and protection of personal data, and protection of critical infrastructure.

2. increasing cyberspace expertise through education and knowledge sharing, especially through Public Private Partnerships.¹⁹

In this context, Albania has enriched its environment by adopting several laws and national strategies, which will be treated in the below sections of this paper.

3. Albania National Strategy on Cyber-Security for the period 2021-2023

Cyber security is one of the latest aspects of national security policies, which is becoming increasingly important in all security sectors of European countries. Policymakers are still catching up to the pace of technological developments being exploited by a range of actors, both friendly and hostile. This requires new legal and policy frameworks to be developed quickly and comprehensively.²⁰

In addition to ensuring national security, protected and secure networks are also important for boosting the national economy and modernizing public sector governance in SEE countries (consider, for example, the critical importance of a secure network for good functioning of e-government services that are put into use). A safe cyberspace is also necessary to guarantee that citizens can exercise their rights, such as access to information and freedom of expression. Being aware of the opportunities, risks and threats, that cyberspace brings, are of vital importance.²¹

The Cyber Defense Strategies 2014-2020 of Albania aimed to ensure orientations, coherence and focus, for a comprehensive approach and to develop military capabilities in cyberspace.

Within the action plans, in implementation of these strategies, significant improvements have been made in increasing organizational skills against cyber security requirements. The operational capacities and awareness have been increased in various aspects of cyber security. Due to the high rate of technology change and rapid developments in the cyberspace threat environment, it is necessary to undertake continuous assessment and regular reviews of the adequacy of cyber security policies.²²

The goal should be technological progress, as well as cooperation and coordination with other countries, so that we are able to react faster than vulnerabilities and threats. A secure and resilient cyberspace allows us to build a strong foundation on the challenges of the complex cyberspace.²³

The Action Plan for the Implementation of the Albania Cyber Defense Strategy for the years 2021-2023 has defined as main goals, the following:

a) *Guaranteeing cyber security through the protection of information infrastructures, which may be achieved through:*²⁴

- Development of industrial and technological resources to ensure cyber security by guaranteeing that the hardware and software components used in services and critical infrastructures are reliable, secure for the protection of personal data, as well as addressing

¹⁹ Ibid., p. 67.

²⁰ *Strategjia per Mbrojtjen Kibernetike 2021-2023*. Ministria e Mbrojtjes, 2020. Available online at <https://www.mod.gov.al/images/PDF/2020/Strategjia-Mbrojtjen-Kibernetike-2021-2023.pdf>. Last access on March 21st, 2023. See also *Sfidat e sigurise kibernetike ne Shqiperi*. Ministria e Infrastrukturës dhe Energjisë. 2023. Available online at <https://www.infrastruktura.gov.al/sfidat-e-sigurise-kibernetike-ne-shqiperi/>. Last access on March 21st, 2023.

²¹ Ibid. See also *Siguria Kibernetike Kombëtare, Shqipëria në fund të Europës/ Jemi ndër 4 vendet me performancën më të dobët sa i përket sigurisë së qeverisjes elektronike*. SCAN Intel. 2022, available online at <https://siu.scan-tv.com/siguria-kibernetike-kombetare-shqiperia-ne-fund-te-europes-jemi-nder-4-vendet-me-performancen-me-te-dobet-sa-i-perket-sigurise-se-qeverisjes-elektronike/>. Last access on March 21st, 2023.

²² *Strategjia per Mbrojtjen Kibernetike 2014-2020*. Ministria e Mbrojtjes, 2014. Available online at <https://dokumen.tips/documents/strategjia-per-mbrojtjen-kibernetike-cyber-fusha-dixhitale-e-hapesires.html?page=3>. Last access on March 21st, 2023.

²³ *Strategjia per Mbrojtjen Kibernetike 2021-2023*. Ministria e Mbrojtjes, 2020. Available online at <https://www.mod.gov.al/images/PDF/2020/Strategjia-Mbrojtjen-Kibernetike-2021-2023.pdf>. Last access on March 21st, 2023.

²⁴ Ibid., p. 4.

the appropriate requirements for the performance of cyber security implemented throughout the chain.²⁵

- Putting in efficiency the capacities of detection, analysis, reduction and countermeasures to cyber threats, focusing in critical infrastructure, computer networks connected to the Internet and other systems, which includes the commitment of the Military Cyber Security Unit to build capacity for continuous maintenance and real-time monitoring of the threat environment, supported by established plans to respond to events that may occur.²⁶
- Strengthening cyber assets during missions focusing specifically on the further development of a cyber defense doctrine of offensive assets, the preparation of instructions for the preparation of cyber units and assets with a flexible model, the deployment of digital defense assets during missions, as well as the development of cyber assets and assets of cyber intelligence for tactical use and the integration of cyber aspects into the operational decision-making process, before and after operations.²⁷
- Implementation of complete organizational and technical cyber security measures in Communication and Information Systems, by taking measures for the protection of the critical and important information infrastructure to guarantee basic services, for the management of information and communication technology assets, the continuous control and evaluation of security measures, as well as the reflection of security requirements in the projects of new communication and information systems and for the implementation of defense technologies.²⁸
- Modeling best practices in protecting technology systems of information through partnership between all state structures that receive system services and revision of security policies, standards and procedures.²⁹

b) *Building a safe environment*, which may be attained via education and empowering of all individuals with information, confidence and practical tools, increasing the responsibility of state structures for cyber security, as well as developing the level and skills of cyber security specialists.³⁰

c) *Increasing national and international cooperation as member of NATO in the field of cybersecurity through* coordination and cooperation of all national actors, as the basic element for guaranteeing success and international cooperation for increasing the security of cyber space.³¹

Moreover, this strategy is based on the following basic principles:³²

Shared responsibilities. All users of systems, while taking advantage of computer networks, must take reasonable steps to secure the systems they use, take care when communicating and storing information and data, and have an obligation to respect the information and systems of others.

Partnership. Based on shared responsibilities, an approach to cyber security, through partnership with all national and international actors in the field of cyber security, is fundamental to succeed.

Risk management. In a globalized world in which all Internet-connected systems are potentially vulnerable and cyber-attacks are difficult to detect, there is no such thing as absolute cyber security. A risk-based approach to systems must also be implemented to assess, prioritize, and support resourcing of cybersecurity activities.

Protecting the values of the Armed Forces. It is necessary to pursue cyber security policies that improve individual and collective security in the Armed Forces, while preserving the right of

²⁵ Ibid., p. 4. See also Daniel Kroening, Michael Tautschnig. *Automating Software Analysis at Large Scale*. In Mathematical and Engineering Methods in Computer Science, Springer 2014. pp. 30-39.

²⁶ *Strategija per Mbrojtjen Kibernetike 2021-2023*, op. cit., p. 4.

²⁷ Ibid., p. 5.

²⁸ Ibid., p. 6.

²⁹ Ibid., p. 6.

³⁰ Ibid., p. 7.

³¹ Ibid., p. 9.

³² Ibid., p.12.

individuals to privacy and other fundamental values. Maintaining this balance is a constant challenge to meet the complex challenges posed by cyber security in the country.³³

In conclusion, the main goal of this strategy should be technological progress, as well as cooperation and coordination with other countries in order to react faster than vulnerabilities and threats. Only a secure and resilient cyberspace allows Albania to build a strong foundation on the challenges of the complex cyberspace.³⁴

4. Legal regulation on cyber-security in Albania

Effective legal frameworks at the international, regional and national levels are one of the pillars of good governance and constitute a prerequisite for the law principles. In general, legal frameworks are essential to regulate the behavior of legal and to prohibit or penalize illegal activities. Legal frameworks in cybersecurity are also important to ensure compliance of human rights³⁵. That is the reason why many governments have developed new normative regimes to regulate cyberspace.

In Albania, the Law no. 2/2017 "On cyber security" aims to achieve a high level of cyber security, defining security measures, rights, obligations, as well as mutual cooperation between entities operating in the field of cyber security.³⁶

Article 1 of this law specifies that it applies to communication networks and information systems, the violation or destruction of which, would have an impact on the health, safety, economic well-being of citizens and the effective functioning of the economy in the Republic of Albania.³⁷

In articles 5-6 of the above mentioned law, the legislator has defined that the responsible subjects in the field of cybersecurity are: the Responsible Authority for Electronic Certification and Cyber Security and operators of critical and important information infrastructures. In addition to the above, in article 7, the legislator has also defined the computer security incident response team, which consists of specialists in the field of computer security near each operator that administers the critical information infrastructure.³⁸

In order to fulfill the aforementioned purpose, the legislator, based on Article 8 of the law, clearly determines that a series of actions must be undertaken in order to increase the security of information in information systems and the availability and reliability of services and communication networks in cyberspace. These actions, according to Article 9 of the aforementioned law, are divided into two categories: security measures of an organizational and technical nature.³⁹

Specifically, the organizational measures are those of: a) information security management; b) risk management; c) security policies; d) organizational security; e) security requirements for third parties; f) asset management; g) security of human resources and access of persons; h) security events and cyber security incident management; i) work continuity management; i) control and audit.⁴⁰

³³ Ibid., p.12.

³⁴ Ibid., p.11.

³⁵ Working with its partners and allies, it commits Canada to advance its cyber security capabilities, defend the status quo in Taiwan, the South China Seas and the East China Sea, and to defend international norms, development standards and human rights concerning the Uighurs and democratic rights in Hong Kong. Paul Evans (2023) *Canada and Southeast Asia: entering through a different door*, Canadian Foreign Policy Journal, DOI: 10.1080/11926422.2023.2225201, available at <https://www.tandfonline.com/doi/full/10.1080/11926422.2023.2225201?src=>. See also Haraway, Donna (1991) "A Cyborg Manifesto." In Simians, Cyborgs, and Women: The Reinvention of Nature, 69–84. London: Routledge.

³⁶ Law no. 2/2017 "Per sigurine kibernetike". Fletore Zyrtare Nr.22, date 26.01.2017. Available online at <http://qbz.gov.al/eli/ligj/2017/01/26/2>. Last access on March 21st, 2023. This law is partially aligned with Directive (EU) 2016/1148 of the European Parliament and of the Council, dated July 6, 2016, "On measures for a common high level of security of networks and information systems in the European Union". CELEX number: 32016L1148, Official Journal of the European Union, Series L, no. 194, dated 19.7.2016, p. 1-30.

³⁷ Ibid., article 2.

³⁸ Ibid., articles 5-7.

³⁹ Ibid., articles 8-9.

⁴⁰ Ibid., article 9.

Whereas the technical measures are: a) physical security; b) protecting the integrity of communication networks; c) verifying the identity of users; d) management for access authorization; e) activity of administrators and users; f) detection of cyber security events; g) tools for tracking and evaluating cyber security events; h) application security; i) cryptographic devices; j) security of industrial systems.⁴¹

The operators of critical information infrastructure and operators of important information infrastructure, in accordance with articles 11 and 12 of the aforementioned law, in the framework of incident management, which must be reported immediately and reflected in the electronic incident register, should take into account the following parameters: a) the number of users affected by the incident; b) the duration of the incident; c) the geographical scope of the incident, if it can be determined; d) financial damage, if it can be determined.⁴²

Referring to Article 14, the measures in case of a cyber threat or incident are divided into:

a) warnings, which are published recommendations to the responsible entities for dealing with the threat, which is found or became aware, in the field of cyber security.⁴³

b) countermeasures, which are actions taken by public bodies, operators of critical information infrastructure and operators of important information infrastructure, aiming to defend against a cyber risk or a cyber security incident or solve a detected incident.⁴⁴

c) protective measures, which are general measures based on an analysis of cyber security incidents, already resolved, which are taken by the Operators of critical information infrastructure and operators of important information infrastructure in order to increase the protection of information systems, or services, or electronic communication networks.⁴⁵

It's important to emphasize that the legislator in article 19 has given the definition of the cyber crisis state, which is the situation, when the security of information in information systems or the security of electronic communications networks is seriously endangered, putting the public interest of the Republic of Albania at risk. The state of cyber crisis is announced by decision of the Council of Ministers for a period of up to seven days. The maximum period of declaring a state of cyber crisis should not exceed 30 days.⁴⁶

Also, the legislator has determined that the non-fulfillment of the aforementioned obligations, according to Article 21, constitutes an administrative offence, which is punishable by a fine of ALL 20,000 to ALL 800,000.⁴⁷

5. Conclusions

Within the analysis of National Strategy on Cyber-Security for the period 2021-2023 and Law on cybersecurity in Albania, we conclude that:

The use of cyberspace is increasing among people, governments and companies, both for the consumption of information, provision of public and private services, as well as for supporting work processes. This increase means that all these actors are potentially susceptible to violations and cyberattacks, a vulnerability that threatens human rights, as well as national and human securities.

Legislation and effective national strategies are necessary to protect the data, information, knowledge that are transmitted and used in cyberspace, as well as to increase the security of citizens in it. Specifically, the national strategy in Albania has included an international perspective in order that cyber regulation and cyber security not to be limited at national borders. Also, the Albanian legislation on cyber security is harmonized with the laws of other countries, aiming to allow international cooperation and its enforcement competences are subject to protective measures to

⁴¹ Ibid.

⁴² Ibid., articles 11-12.

⁴³ Ibid., article 15.

⁴⁴ Ibid., article 16.

⁴⁵ Ibid., article 17.

⁴⁶ Ibid., article 19.

⁴⁷ Ibid., article 31.

ensure the fulfillment of the requirements of the law and human rights.

Regardless of the above, this legislation is intended to deal with the advancement of innovation in cyberspace, with essential knowledge and expertise, which can be increased through education and knowledge shared with private partners, as well as with the international character of the issues, which complicate the implementation of this legislation.

In addition, private companies and non-governmental organizations in Albania should try to help by expanding the legal frameworks and norms to detail the prevailing cyber security approaches, as well as to create completed cyber space and cyber security governance that is based on the principles of good governance of the security sector.

Bibliography

1. Buckland B., Schreier F., Winkler Th., *Democratic Governance Challenges of Cybersecurity*, "DCAF Horizon 2015" Working Paper no. 1. Geneva: Democratic Control of Armed Forces.
2. *Cfare eshte siguria kibernetike?* Drejtoria e Përgjithshme e Teknologjisë së Informacionit, Inovacionit dhe të Dhënave.2023. Available online at <https://dptiidh.tirana.al/cfare-eshte-siguria-kibernetike/>.
3. Directive (EU) 2016/1148 of the European Parliament and of the Council, dated July 6, 2016, "On measures for a common high level of security of networks and information systems in the European Union". CELEX number: 32016L1148, Official Journal of the European Union, Series L, no. 194, dated 19.7.2016.
4. *ENISA overview of cybersecurity and related terminology*. ENISA. Version 1, September 2017. Available online at <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology>.
5. Evans, Paul (2023) *Canada and Southeast Asia: entering through a different door*, Canadian Foreign Policy Journal, available at <https://www.tandfonline.com/doi/full/10.1080/11926422.2023.2225201?src=>.
6. Favaro, Marina & Williams, Heather, (2023) *False Sense of Supremacy: Emerging Technologies, the War in Ukraine, and the Risk of Nuclear Escalation*, Journal for Peace and Nuclear Disarmament, available at: <https://www.tandfonline.com/doi/full/10.1080/25751654.2023.2219437>.
7. *Guide to developing a National Cybersecurity Strategy*. ITU, 2018. Available online at https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf.
8. Haraway, Donna (1991), *Simians, Cyborgs, and Women: The Reinvention of Nature* London: Routledge.
9. *International Cybersecurity Norms*, Microsoft Policy Papers. Digital Geneva Convention, 2019. Available online at <https://www.microsoft.com/en-us/cybersecurity/content-hub/international-cybersecurity-norms-overview>.
10. Kroening, Daniel & Tautschnig, Michael, *Automating Software Analysis at Large Scale*. In Mathematical and Engineering Methods in Computer Science, Springer 2014. pp. 30-39.
11. Law No. 2 dt.26.01.2017 "Për sigurinë kibernetike". Fletore Zyrtare Nr.22, datë 26.01.2017.
12. Popa Tache, Cristina Elena, *Individualization and development of international investment law as the third millennium law field*, "Juridical Tribune - Tribuna Juridică", Volume 9, Issue 3, December 2019, 583-588.
13. Schreier F., Weekes B., Winkler Th., *Cyber security: The Road Forward*, "DCAF Horizon 2015". Working Paper No. 4. Geneva: Democratic Control of Armed Force.
14. Sfidat e sigurisë kibernetike ne Shqipëri. Ministria e Infrastrukturës dhe Energjisë, 2023 <https://www.infrastruktura.gov.al/sfidat-e-sigurise-kibernetike-ne-shqiperi/>.
15. *Siguria Kibernetike Kombëtare, Shqipëria në fund të Europës/ Jemi ndër 4 vendet me performancën më të dobët sa i përket sigurisë së qeverisjes elektronike*. SCAN Intel.2022, <https://siu.scan-tv.com/siguria-kibernetike-kombetare-shqiperia-ne-fund-te-europes-jemi-nder-4-vendet-me-performancen-me-te-dobet-sa-i-perket-sigurise-se-qeverisjes-elektronike/>.
16. Strategjia për Mbrojtjen Kibernetike 2014-2020, Ministria e Mbrojtjes.2014.
17. Strategjia për Mbrojtjen Kibernetike 2021-2023. Ministria e Mbrojtjes, 2020.
18. *Udhëzues për qeverisjen e mirë me sigurinë kibernetike*. Geneva Center for Security Sector Governance, 2019, Available online at https://dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_AL_Jan2021_0.pdf.