# BRITISH VIEW

MULTIDISCIPLINARY JOURNAL

www.britishview.co.uk

Anthropologie, Applied Linguistics, Applied Physics, Architecture, Artificial Intelligence, Astronomy, Biological Sciences, Botany, Chemistry, Communication studies, Computer Sciences, Computing technology, Cultural studies, Design, Earth Sciences, Ecology, Education, Electronics, Energy, Engineering Sciences, Environmental Sciences, Ethics, Ethnicity and Racism Studies, Fisheries, Forestry, Gender Studies, Geography, Health Sciences, History, Interdisciplinary Social Sciences, Labour studies, Languages and Linguistics, Law, Library Studies, Life sciences, Literature, Logic, Marine Sciences, Materials Engineering, Mathematics, Media Studies, Medical Sciences, Museum Studies, Music, Nanotechnology, Nuclear Physics, Optics, Philosophy, Physics, Political Science, Psychology, Publishing and editing, Religious Studies, Social Work, Sociology, Space Sciences, Statistics, Transportation, Visual and Performing Arts, Zoology and all other subject areas.



Manuscripts typed on our article template can be submitted through our website here. Alternatively, authors can send papers as an email attachment to editor@britishview.co.uk

Editor Multidisciplinary Journals

Website: http://britishview.co.uk
Email: editor@britishview.co.uk

British View ISSN 2041-3963 Volume 8 Issue 8 2023
Universal impact factor 8.528
SJIF 2022: 4.629

# Legal significance of consular protection during the development of digital relations

**Gafurova Sevara Alisherovna,**
Associate Professor at the University
World Economy and Diplomacy,
Doctor of Laws (DSc)
E-mail: sevaragafurova@mail.ru.
Blog: @dr.alisherovna_science

**Abstract*:*** Ensuring the security of mechanisms used in diplomatic and consular activities in cyberspace is essential. At the same time, digital development forms a system of new methods and means of implementing consular protection using the Internet and information and communication technologies and shows their influence in modern consular practice. The correct application of the rules relating to various branches of law used in the implementation of consular protection creates a solid legal basis for the stable development of relations between countries. The article comprehensively covers these aspects.

**Keywords:** consular law, consular protection, digital communication, cyberspace, digital legal relations, consular ralations, artificial intelligence, online application, email and valise, diplomatic post.

The importance of consular law in international legal relations, like other legal institutions, is evolving based on the nature of regulatory social relations and the requirements of the Internet era. Consular right is characterized by the systematic implementation of legal protection and its close connection with a number of legal branches. The norms necessary for the implementation of legal protection in consular practice are the basis for the formation of legal social and digital relations. The correct application of the norms related to various legal branches used in the implementation of consular protection creates a solid legal basis for the stable development of relations between countries [1].

The main task of consuls is to protect citizens living in foreign countries. The Internet has made consular duties easier. Most citizens can easily notify consulates of their address or concerns through consular websites and e-mails. In addition, the consulate can more conveniently find out about the requirements and service problems of its citizens through the consulate's website or e-mail that can be shared with other consulates. Often, e-mail is used as a method of quick communication with government officials[2]. In addition, in most countries, foreign ministries are equipped with an Intranet system, so that most of their employees can communicate with each other and share information. Quick responses and prompts allow consulates to take quick action to meet specific requests or existing problems[3].

Digital legal relations must create a model of legal regulation that fits this new technological reality. At the same time, special attention should be paid to its adaptation.

It is a necessary process for traditional law, law and administration to be quickly and formally assimilated into the new digital conditions of society. It is necessary to know the following:

- compliance with the specific features of the rules regulating communication on the Internet (customs, technical standards, etc.),
- the mechanism of legal regulation, the concept of legal relations and issues of legal responsibility in relation to them;
- digital achievements;
- the legal nature of the smart contract (smart-contract - self-executing contract);
- view artificial intelligence as an object or subject of law;
- cryptocurrencies (the object of rights and measures for the protection of virtual values);
- measures of legal responsibility in the digital law-order.

Practical tools of digital legal relations are also used in consular activities, in particular, they are used in the processing and preparation of visa documents, direct communication with citizens

abroad, rapid communication in emergency situations and natural disasters. At the same time, taking into account all the objective advantages of digital technologies, the development of cyber relations in practice is close to risks and threats[4]. The Internet is perceived as a channel for the spread of extremism and terrorism, the implementation of foreign ideology and foreign policy propaganda, and a means of information warfare. Internet networks are used as a motivational force when most citizens leave for foreign countries[5].

There is no consensus on how to solve the problem when cyber operations targeting the buildings of diplomatic missions or consular institutions often come from abroad [6]. States have a duty to protect buildings on their territory. In accordance with the diplomatic and consular legislation, the receiving state does not have the obligation to ask for help in this regard, the obligation to take "appropriate measures" is determined by the measures that provide for the implementation of its sovereign powers.

It is also noteworthy that there is no state practice supporting the existence of such a right. There is also no obligation to take preventive measures to protect the premises of a diplomatic mission or consular post and its cyber infrastructure, unless the receiving State is aware of a specific threat. Accepting this position, in the event of a known security risk, it is the practice to receive only special personnel to protect mission or representative premises. mission or post. It should also be noted that the host country can rely on its own security measures to protect the cyber infrastructure in the office premises, not the sending country.

*Privileges and Immunities.* The cyber infrastructure on the territory of a diplomatic mission or consular institution is protected by the inviolability of this mission or institution. The receiving state must take all appropriate measures to protect the cyber infrastructure located on the territory of the diplomatic mission or consular institution of the sending state from intrusion or damage. For example, if receiving public services learn that the cyber infrastructure within the diplomatic mission of the sending state has been targeted by cyber operations, the receiving state must use all reasonable efforts to terminate the offending operations, including: informs about. Similarly, if a mission's cyber infrastructure is targeted by cyber operations, the host nation must take law enforcement or other measures proportionate and appropriate to the threat to deter the operations. This obligation is not absolute. The receiving state is only required to take "all appropriate measures" to protect the premises. The level of all appropriate measures is based on, inter alia, the magnitude of the threat to the premises, the receiving state's level of awareness of the specific threat, and the receiving state's ability to respond to the situation[7].

The receiving state has the right to choose certain measures to take to fulfill this obligation.

The inviolability of diplomatic mission premises is a basic principle of diplomatic law. According to him, it is not possible to enter the premises without permission. In addition, property in the premises of a diplomatic mission is protected from search, requisition, seizure or seizure by agents of the receiving state without the consent of the sending state.

Application of this provision also covers remote access to cyber infrastructure or otherwise tampering with or altering data therein, meaning that cyber operations manifesting in cyber infrastructure on these premises are tantamount to unauthorized access to premises. It is also confirmed by the special obligation of the receiving state to take all appropriate measures to protect the premises of the diplomatic mission from any invasion or damage and to assist in the full implementation of the mission.

Whether online applications to a diplomatic mission by e-mail or in person (for example, when the website of a diplomatic mission or consular institution allows citizens of the receiving country to submit online applications for visas to travel to the sending country) are classified as archives, documents or official correspondence protected by international norms, the issue is important.

Currently, international customary law does not include the practice of placing a seal of inviolability on electronic archives, documents or official correspondence of a diplomatic mission or consular institution[8].

Most of the experts of international law have expressed the opinion that immunity in such circumstances corresponds to the object and purpose of diplomatic and consular law, and since the information is presented for official purposes, it becomes at least a part of archives and documents. Some experts have argued that such private presentations are outside the scope of protection because diplomatic and consular rights are limited to relations between states. However, all experts agree that if, for example, a citizen of the host country posts a comment on a mission's latest post on a social networking Web site, that comment is not protected because it is publicly available.

Electronic archives, documents and official correspondence of a diplomatic mission or consular institution are inviolable. The receiving state must allow and protect free cyber communications of the diplomatic mission or consular post for all official purposes. Treaty and customary law norms ensure that official diplomatic and consular correspondence and other official communications from all States "in transit..." are accorded the same protection as the receiving State. Thus, receiving and third countries are prohibited from intercepting electronic messages in transit of diplomatic missions and consular institutions. They emphasized the importance of diplomatic and consular relations in defense and in the activities of the diplomatic mission or consular institution.

It should be noted that not only the receiving country, but all countries must respect the inviolability of diplomatic and consular materials of the sending country. If the material is stored in the building of a diplomatic mission or consular institution, it is protected by the inviolability of the premises. When this material is off-premises, such as data stored on a private cloud server, it is protected by the privacy of official correspondence and other communications in transit consistent with the object and purpose of the privacy principle.

International law requires the receiving state to allow and protect "free communication" for all official purposes by the diplomatic mission or consular institution of the sending state. An international group of experts agreed that this provision reflects customary international law. The receiving State must permit and protect the cyber communications of the diplomatic mission or consular post for all official purposes.

As for consular institutions, the right of consular officials to communicate freely with citizens of the sending state deserves special attention. Therefore, the receiving state cannot, for example, interfere with e-mail communications between consular officials and citizens of the sending state on official consular matters.

The premises of a diplomatic mission or consular institution may not be used to carry out cyber activities that are incompatible with diplomatic or consular functions.

Diplomatic agents and consular officials may not engage in cyber activities that interfere with the internal affairs of the receiving state or that are inconsistent with the laws and regulations of that state.

As much as diplomatic agents and consular officials enjoy criminal, civil, and administrative jurisdiction, they also enjoy immunities for their cyber activities.

Due to immunity from criminal, civil and administrative proceedings of the receiving State, diplomatic agents cannot be subject to enforcement or judicial jurisdiction for activities that violate these rules. They can be declared persona non grata, which requires the sending country to take them back

While in the country, diplomatic agents are immune from the criminal jurisdiction of the host country for any activity that may be classified as cybercrime under the domestic law of the host country. This diplomatic immunity is absolute and unconditional. They are also immune from arrest and exempt from testifying as witnesses.

Diplomatic agents are also immune from the host nation's civil and administrative jurisdiction over their cyber activities. However, a diplomatic agent may not be immune from civil or administrative jurisdiction for selling goods online as a private business.

Both the Vienna Convention on Diplomatic Relations and the Vienna Convention on Consular Relations respectively state that a diplomatic mission and a consular post may install and

use wireless transmitters only with the consent of the receiving State. At the time of the development of the conventions, wireless transmitters were mainly used for radio transmission. According to an international panel of experts, the language of this treaty is somewhat outdated and its exact translation to cyber technologies is not complete and clear. In particular, experts generally agree that equipment that emits radio frequency signals only within the perimeter of a diplomatic mission or consular facility, such as a wireless router, is exempt from the rule. However, experts agree that as new forms of wireless technology emerge, this principle should continue to require the consent of the receiving state to install and operate equipment that allows a diplomatic mission or consular post to transmit communications outside its premises. This includes the installation of all types of wireless communication equipment (for example, for satellite communication) if their use could cause harmful interference to wireless communication in the receiving country[9].

If diplomatic or consular material is obtained by a third party (including another country) and then made available to the public by the third party (for example, as in the Wikileaks incident, the material is stolen or otherwise misappropriated ri is purchased and placed on the Internet) the issue of privacy is important. In such cases, immunity is lost, because the object and subject of immunity is considered to have been lost (the source has been made public and made public).

A separate issue is the protection of property of a diplomatic mission that is not on its premises, such as mobile phones or laptops outside the premises. As a general rule, such property is inviolable. Under the 1961 and 1963 Conventions, diplomatic and consular immunity in relation to property outside the premises is consistent with its object and purpose in this case. The Vienna Convention on Diplomatic Relations provides immunity to the movable personal property of diplomatic agents, subject only to exceptions for certain civil or administrative actions. Therefore, the property of a diplomatic mission is inviolable even if removed from the premises, while the private property of a diplomatic agent is inviolable regardless of where it is located.

The development of digital relations, the rapid penetration of high technologies into the daily consular practice requires the consuls to gain awareness, since the new technological social communication in the consular activity should be considered as the continuity and speed of communication with citizens [10].

In conclusion, it should be noted that since the beginning of the rapid development of information technologies, the concept of open government has spread throughout the world - the ideal issues of transparency and accountability in management have been emphasized. Citizens had to use state documents and procedures to create an effective inspection system. Over the past years, this concept has been inextricably linked with the concept of "e-government", and the common goals of "open" and "e-government" are to increase efficiency and transparency in providing legal assistance to citizens, as well as to simplify and improve legislation.

The Internet is becoming an indispensable tool for diplomatic negotiations and communication with various interest groups. In this new environment, the traditional law of diplomacy and consular affairs must also evolve through a new interpretation of existing rules. If some of these rules are insufficient or insufficient to regulate cyber relationships, new rules must be created. International rules on inviolability of premises, inviolability of documents and archives, freedom of official correspondence, tax exemptions, and immunity from judicial jurisdiction must be reinterpreted and applied to reflect the cyber diplomacy environment.

## References:

**1.** Gafurova S.A. Konsullik himoyasini amalga oshirishda xalqaro huquqning rivojlanib borayotgan tarmoqlarining ahamiyati // Huquqiy tadqiqotlar. 2022. 7-jild, №3. – B. 93-100.
**2.** Birahayu D. Maritime Digital Diplomacy: Legal Revitalization and Reform of Modern and Solutive Diplomacy //Audito Comparative Law Journal (ACLJ). – 2023. – T. 4. – №. 3. – C. 170-184.: 3. *Qarang:* Kapeller D/ Websites as a instrument of diplomacy // Malt. Second

conference on Web menegment of diplomacy. 2002.; GLuša, Đana & Jakopović, Hrvoje. (2017). Websites as a government tool of public diplomacy: Framing the issue of unemployment. Teorija in Praksa. 54. 284-306.
**3.** Kapeller D/ Websites as a instrument of diplomacy // Malt. Second conference on Web menegment of diplomacy. 2002.; *Qarang:* GLuša, Đana & Jakopović, Hrvoje. (2017). Websites as a government tool of public diplomacy: Framing the issue of unemployment. Teorija in Praksa. 54. 284-306.
**4.** Gafurova S. Implementation of consular protection and data protection law //British View. – 2022. – Т.: 7. – №. 1. *Qarang:* Mihai S. et al. On Digital Diplomacy. Key Issues //International Conference on Cybersecurity and Cybercrime. – 2022. – Т.: 9. – С. 23-28.; Cornut J., Manor I., Blumenthal C. WhatsApp with Diplomatic Practices in Geneva? Diplomats, Digital Technologies, and Adaptation in Practice //International Studies Review. – 2022. – Т.: 24. – №. 4. – С. viac047.
**5.** Ровинская Т. Роль новых цифровых технологий в период кризиса. Мировая экономика и международные отношения, 2021, т. 65, № 6.
**6.** Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.). Cambridge: Cambridge University Press. doi:10.1017/9781316822524 Diplomatic and consular law. https://www.cambridge.org/core Harvard University. https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781316822524.013 https://www.cambridge.org/core. Harvard University, on 06 Dec 2017 at 15:30:41, subject
**7.** Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.). Cambridge: Cambridge University Press. doi:10.1017/9781316822524 Diplomatic and consular law. https://www.cambridge.org/core Harvard University. https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781316822524.013 https://www.cambridge.org/core. Harvard University, on 06 Dec 2017 at 15:30:41, subject
**8.** Von Heinegg, W. (2012). Chapter 1: The Tallinn Manual and International Cyber Security Law. Yearbook of International Humanitarian Law, 15, 3-18. doi:10.1007/978-90-6704-924-5_1; *Qarang:*Birahayu D. Maritime Digital Diplomacy: Legal Revitalization and Reform of Modern and Solutive Diplomacy //Audito Comparative Law Journal (ACLJ). – 2023. – Т. 4. – №. 3. – С. 170-184.
**9.** Masalani chuqurroq o'rganish uchun "zararli shovqin" haqidagi ma'lumotlarni o'rganib chiqing.
**10.** Синюков В. Н. Цифровое право и проблемы этапной трансформации российской правовой системы //Lex russica. – 2019. – №. 9 (154). – С. 9-18.; *Qarang:* Солдаткина О. Л. Цифровое право: особенности цифровой среды и субъекты //Государство и право. – 2019. – №. 12. – С. 113 – 123.; Конобеевская И. М. Л. Цифровые права как новый объект гражданских прав //Известия Саратовского университета. Новая серия. Серия Экономика. Управление. Право. – 2019. – Т.: 19. – №. 3. – С. 330-334.; Агибалова Е. Н. Цифровые права в системе объектов гражданских прав //Юридический вестник Дагестанского государственного университета. – 2020. – Т.: 33. – №. 1. – С. 90 – 99.