Article

УДК: 341

THE FIRST "BLOCKING" STATUTE AGAINST UNLAWFUL FOREIGN LAW ENFORCEMENT AND JUDICIAL ACTIVITIES IN CYBERSPACE

Pyotr A. Litvishko*

DOI 10.24833/2073-8420-2026-1-78-40-50

Introduction. *Federal Law No. 282-FZ of 31 July 2025 added a new article – 294[1] ("Unlawful performance of investigative, other procedural actions and operational search measures in the territory of the Russian Federation") to the RF Criminal Code. This publication represents a commentary thereon, with an emphasis on its application to activities in cyberspace. It highlights the circumstances of the enactment and international legal aspects of the novel norm, analyzes the elements of the criminal offence, specificities of proceedings on it, as well as its effect in the context of the UN Convention against Cybercrime[1].*

Materials and methods. *The article explores the relevant treaties and customary international law, soft law, as well as domestic and foreign laws and regulations. It is also sourced from jurisprudence and legal practices of interstate, domestic and foreign law enforcement authorities, as well as scholarly literature. The applied methodology includes the formal legal and comparative methods, methods of systemic and structural analysis, and synthesis of social and legal phenomena.*

Results of the study. *The new legal norm constitutes a blocking statute aimed at precluding application in the territory of the enacting state of a law made by a foreign jurisdiction, and proceeds from the legal fiction of the "territorialization" of cyberspace. The spotlight on the problem of extraneous law enforcement on Russian soil was turned due to the special military operation and concomitant risks of the adversaries illegitimately exfiltrating evidence from its territory, for understandable reasons primarily in a remote virtual mode with no boots on the ground. The Russian law as a trailblazer goes beyond what its foreign counterparts have managed to regulate so far, which in the long term can be expected to contribute to the progressive development of international law as well.*

* **Pyotr A. Litvishko**, Candidate of Sciences (Law), Deputy Head of the General Department of International Legal Cooperation – Head of the Department of Legal and Law Enforcement Assistance, Senior Assistant to the Prosecutor General of the Russian Federation, Prosecutor General's Office of the Russian Federation, Moscow, Russia
e-mail: petrlitvishko@yandex.ru
ORCID ID: 0009-0001-3424-7031

[1] To be continued in the next issue under the title "The "blocking" statute (article 294[1] of the RF Criminal Code): details of criminal proceedings". An abridged Russian version was published in the journal of the RF Prosecutor General's Office: Litvishko P., 2025. Pervyj «blokiruyushchij» zakon protiv nepravomernoj transgranichnoj inostrannoj i mezhdunarodnoj pravoohranitel'noj i sudebnoj deyatel'nosti v kiberprostranstve [The first "blocking" statute against unlawful cross-border foreign and international law enforcement and judicial activities in cyberspace]. *Zakonnost' [Legality].* No. 10(1092). S. 24–28; No. 11(1093). S. 16–22.

Discussion and conclusion. *The actus reus is accomplished directly by a foreign or international official themselves or indirectly through the agency of a proxy and should not be made conditional on the finalization of the action or ultimate use of its product in proof, or the availability of its written or audiovisual record. The defendant official's immunity is examined, invoked or waived and determined according to the rules of domestic and general international law. However, customary international law tends to proceed from the absence of immunity in cases of such acts, which violate territorial sovereignty and are similar to offences of espionage. The mens rea premises that an offender acts with "triple" direct intent to perform the proscribed law enforcement or judicial measure and to breach the established procedure for its performance, as well as to pursue the purpose that runs counter to the interests of Russia; it also includes the mandatory scienter element of the location – knowingly within the Russian territory – of the individual targeted by the defendant's activity through the use of telecommunications. The offence can be detected and its perpetrators can be brought to justice by various methods and means described in the article. The neutralization of certain "extraterritorial backdoors" contained in the Hanoi Cybercrime Convention should be carried out primarily at the national statutory and law enforcement level, which Russia did by adopting the law at issue. Although the Convention does not cover the conduct or responsibility of states, its provisions regarding the obligations of states to cooperate with respect to acts criminalized by the Convention (in particular, illegal access or interception) may well be applied by states that have been injured by and are investigating the relevant illegal unilateral cross-border actions of specific state actors and their proxies, taking account of the applicable procedures for engaging international legal immunities.*

Introduction

Federal Law No. 282-FZ of 31 July 2025 supplemented the RF Criminal Code with article 294[1] ("Unlawful performance of investigative, other procedural actions and operational search measures in the territory of the Russian Federation"), pursuant to which "[t]he conduct by a foreign official or an official of a public international organization or international authority, in which the Russian Federation does not participate, of an action in the territory of the Russian Federation that in accordance with the legislation of the Russian Federation constitutes an investigative or other procedural action, or operational search measure[2], in the interests of a foreign state, public international organization or international authority, in which the Russian Federation does not participate, including through the use of video conferencing systems or other means of communication with a person who is present in the territory of the Russian Federation, in violation of the procedure for interaction with foreign and international law enforcement and judicial authorities provided for by an international treaty and (or) the legislation of the Russian Federation, and for purposes contrary to the interests of the Russian Federation, in the absence of elements of crimes envisaged in articles 276 or 284[3] of the present Code, – shall be punished by a fine in the amount from five hundred thousand to two million rubles or in the amount of a salary or other income of the sentenced person for a term of six months to two years or by deprivation of liberty for a term of up to five years".

[2] Subject to a number of reservations, covert and overt operational search measures in Russian law are an equivalent of special investigative techniques (SIT), which is an international term of art. Hereinafter, with some exceptions, both are referred to as SIT(s).

[3] The UN Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes of 24 Dec. 2024 (the Hanoi Convention).

Study

The significance and international legal aspects of the law

The first bill against unlawful cross-border foreign and international law enforcement and judicial activities in cyberspace was elaborated on the orders of the Prosecutor General by the Prosecutor General's Office jointly with other federal authorities concerned and introduced to the State Duma by the Chairman of its Committee on Security and Counteraction of Corruption and Commission on Investigation of Facts of Interference by Foreign States in Internal Affairs of Russia together with a group of deputies. The law is expected to grow in significance with signature and ratification of the Hanoi Convention against Cybercrime[3].

The new legal norm represents a so-called blocking statute aimed at precluding application in the territory of the enacting state of a law made by a foreign jurisdiction, in particular preventing unauthorized collection of evidence[4] [2. P. 43–72, 442–443].

The author's comprehensive commentary on the article focuses on its cross-border remote virtual component as the most complex from both international and criminal legal viewpoints, that is performance of criminalized unilateral actions by video conference or employing other telecommunications from abroad (while the article equally covers their use solely within Russia's territory) in light of international law, which nowadays takes place primarily via the Internet and therefore one talks about the application of the law in respect of cyberspace. This element of the novelty provision is based on the extensive scholarly research into substantive and procedural criminal jurisdiction in the information space, first of all from the angle of international law, which was presented at authoritative domestic and international fora, including the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes[5]. The examples of foreign statutes, among others those of the United States and Switzerland, used in drafting the bill, are set out in its explanatory note and preceding comparative research [4. P. 93–101; 12. P. 132–173].

The legal norm of the kind had been called for by ordinary law enforcement practices for a long time and irrespective of the current state of affairs; the geopolitical developments of the last decade have just more vividly highlighted that need. Whereas the collective West is now concerned about so-called transnational repression[6], for Russia, the spotlight on the problem of extraneous extraterritorial law enforcement towards and on its soil was turned due to the special military operation and concomitant risks of the adversary's illegitimate gathering and exfiltrating evidence from its territory, especially in the new and border regions, from the outside and for understandable reasons primarily in a remote, virtual mode, also luring Russian nationals in this manner to travel abroad for the purpose of their arrest, detention and surrender. New challenges and threats emanate from the intensified capacity building and plans of Ukraine and its allies to massively collect electronic evidence, including open source intelligence, against the Russian Federation. For this purpose, a number of interstate projects have been created, with substantial funding [13][7].

Currently, law enforcement and judicial authorities of some foreign countries carry out criminal proceedings *in absentia* against Russian servicemen and officials in connection with the said operation; interstate joint investigation teams pursuing the goal of bringing them to trial were set up; aggressive anti-Russian activities aimed at investigating the armed conflict are underway on the part of the International Criminal Court, bodies of the European Union (Eurojust and Europol)[8], Council of Europe[9], quasi-investigatory Independent International

[4] Guide to Good Practice on the Use of Video-Link under the Evidence Convention. The Hague: The Hague Conference on Private International Law – HCCH Permanent Bureau, 2020. P. 39, 43; Transborder access and jurisdiction: What are the options? Report of the Transborder Group adopted by the T-CY on 6 Dec. 2012, Strasbourg, 6 Dec. 2012, T-CY (2012)3. P. 22. Para. 3.2.3.4.

[5] The main results of the research are contained in the monograph of the Prosecutor General's Office and the University of the Public Prosecutor's Office of the Russian Federation published in English at the initiative of the RF Ministry of Foreign Affairs: Collecting Electronic Evidence in Criminal Cases in Russia and Foreign Countries: Experiences and Problems: Monograph. Editors S.P. Shcherba (Russian ed.) and P.A. Litvishko (English ed.). 2024, Moscow.

[6] See, e.g.: Transnational Repression. CCP's covert, often illegal overseas policing draws international condemnation. December 18, 2023. Indo-Pacific Defense Forum. Available at: https://ipdefenseforum.com/2023/12/transnational-repression/ (accessed: 12.10.2025).

[7] CyberUA: Strengthening capacities on electronic evidence of war crimes and gross human rights violations in Ukraine. Available at: https://www.coe.int/en/web/kyiv/cyberua (accessed: 14.10.2024).

Commission of Inquiry on Ukraine (complementing the work of the Human Rights Monitoring Mission in Ukraine) established by resolution 49/1 of 4 March 2022 of the UN Human Rights Council[10], Moscow Mechanism of the Human Dimension of the Organization for Security and Co-operation in Europe invoked to investigate violations of international humanitarian and human rights law, war crimes and crimes against humanity committed in Ukraine.

By far not all of those investigations and inquiries are of a criminal legal character, consequently the measures undertaken within their frameworks to collect "evidence" cannot always be qualified as criminal proceedings or SITs.

The novel ban in criminal law is designed to send a clear signal and ensure a considerable dissuasive effect with regard to foreign law enforcement's readiness to undertake activities on which it is imposed, and similarly to Switzerland and the United States' practice, the information about the ban should be proactively and regularly brought in various forms to the attention of foreign target audiences of colleagues, its potential violators. Such an effect is slated to be secured even in cases of INTERPOL's refusals to provide their channels for international search for fugitives accused of this ordinary-law crime, since they can be tracked down, arrested and extradited or otherwise surrendered to Russia after having been established in the territories of friendly or neutral nation states as part of the bilateral cooperation without using those channels.

Blocking norms also serve as an additional means of challenging the admissibility of evidence obtained in the way specified therein. However, it would be erroneous to presume in all cases the automatic undermining of the admissibility of evidence collected in such an illegal way, even if it contained elements of an internationally wrongful act, since the admissibility and exclusionary rules are determined by the interested ultimate user of this evidence, especially if they apply the so-called protective norms (*Schutznorm*), which allow the admissibility of evidence to be preserved in case of breach of international law, provided that the fundamental rights of the suspect or accused are not violated (prohibition of torture, right to defence, fair trial) [10. P. 75].

State sovereignty and international norms and principles that flow from sovereignty (such as non-intervention or non-interference in the internal affairs of other States) apply to State conduct of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory[11].

Therefore, nowadays countries generally tend to regard remote "intangible" activities of representatives of a foreign state carried out from within its territory and physically reaching the persons and objects that are known to be located in those countries, with no boots on the ground (on the sea or in the air), as activities undertaken within their own territory. Such activities include cross-border contacts via any telecommunication networks (electromagnetic systems): terrestrial (landline, cable, for example, fiber-optic communications, radio relay, tropospheric scatter and other mobile (wireless) radio communications), space (satellite) radio communications, in other words, for instance, by telephone, video conferencing, e-mail, social media, instant messaging on the Internet with persons knowingly staying and using relevant end-point equipment on the territory of the country concerned[12]. Thus, one applies the legal fiction of the "territorialization" of cyberspace.

The landmark judgment of the Permanent Court of International Justice in the Lotus case

[8] Eurojust and the war in Ukraine; Core International Crimes Evidence Database (CICED). Available at: https://www.eurojust.europa.eu/eurojust-and-the-war-in-ukraine (accessed: 12.10.2025); Europol's solidarity with Ukraine. Available at: https://www.europol.europa.eu/europols-solidarity-ukraine (accessed: 12.10.2025).

[9] Russia's war against Ukraine. Available at: https://www.coe.int/en/web/portal/war-in-ukraine (accessed: 12.10.2025).

[10] See also: The UN and the war in Ukraine: key information. Available at: https://unric.org/en/the-un-and-the-war-in-ukraine-key-information/ (accessed: 12.10.2025).

[11] See, e.g., the UN General Assembly resolution 73/27 of 5 Dec. 2018 "Developments in the field of information and telecommunications in the context of international security" which again welcomes the set of international rules, norms and principles of responsible behaviour of States, enshrined in the reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security on the application of international law to State use of ICTs.

[12] See, e.g.: art. 20 of the 2000 Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union and art. 31 of the 2014 Directive regarding the European Investigation Order in criminal matters, governing cross-border interception of telecommunications without the technical assistance of another member state whose territory is affected by the interception, by means of remote access, and providing for mandatory notification and substantial authority to the affected state to influence the progress and results of the interception;

rendered back in 1927 acquired new "cyberspatial" dimension and scale in the digital age affirming that "the courts of many countries, even of countries which have given their criminal legislation a strictly territorial character, interpret criminal law in the sense that offences, the authors of which at the moment of commission are in the territory of another State, are nevertheless to be regarded as having been committed in the national territory, if one of the constituent elements of the offence, and more especially its effects, have taken place there"[13], while a ship on the high seas is assimilated to the territory of the state the flag of which it flies and that state possessing territorial (versus extraterritorial) jurisdiction over such a vessel of its nationality (subjective vs. objective territoriality and the effects doctrine; constructive vs. corporeal presence of the offender)[14]. The same may be argued in respect of a country's information infrastructure, especially that located within the boundaries of its territory.

The prevailing opinion in international law at the moment is that said cross-border remote access, search and seizure of data without the consent of the state in which this data is located, expressed in an international treaty or on a case-by-case basis, contravene the principles of territorial sovereignty (in particular, through interference with or usurpation of an inherently governmental function exclusively reserved to the territorial state under international law)[15] [17. P. 11–29, 51–78] and non-interference in the internal affairs of another state, constitute an internationally wrongful act and may entail the inadmissibility of evidence collected in this way[16]. However, at the same time , there is an ongoing discussion about the need to reach international agreements on the legalization of such unilateral actions[17], as well as about the existence of situations that preclude their wrongfulness, when the fundamental principle of territoriality cannot be observed, for instance, where there is "loss of location" of the data when using cloud computing and anonymizing techniques, or law enforcers are mistaken in good faith as to the actual location of data, or under the principles of "ubiquity" [14] or "deterritorialization (un-territoriality)" [16] of data, "center or degree of gravity" or "balance-of-interest" tests [15], "threshold of negative consequences for the territorial sovereignty" test[18] [9].

Indicative of different approaches of the states concerned to the legality of cross-border searches and seizures of data in information systems and networks is the well-known criminal case of the early 2000s of the United States against hackers A. Ivanov and V. Gorshkov, who were lured by US agents from Russia to the United States by way of an undercover action on the Internet, where, as part of another sting operation, they gave away the access credentials to their Russian information resources; whereupon these resources were subjected to unilateral cross-border search and seizure. Ivanov and Gorshkov were convicted and sentenced in the United States, and the Russian investigative authorities, in turn, initiated a criminal case against the US special agent, who carried out the said search and seizure, on the charges of illegal access to computer information committed by a person using his official position [7. P. 96-97, 101][19].

Judgment of the Court (Grand Chamber) of 30 Apr. 2024 in Case C-670/22, M.N. (EncroChat); art. 113(11–13) of the Criminal Procedure Code of Georgia on cross-border interviews by electronic means of communication outside the procedure of international legal assistance with the consent of the relevant foreign state.

[13] S.S. "Lotus" (*France v. Turkey*), Judgment, 1927 PCIJ (Ser. A) No. 10 (Sept. 7, 1927).

[14] See also: International Criminal Court, Office of the Prosecutor. Policy on Cyber-Enabled Crimes under the Rome Statute. December 2025. P. 19–20 (among others, citing the Court of Appeal of England and Wales holding unanimously in 2024 that "as a straightforward use of language, the remote manipulation from abroad of a computer located in the United Kingdom is an act within the United Kingdom. The true position in such a case is that the agents of the foreign state commit acts both in this country and abroad"); Damian K. Graf, Kommentierung zu Art. 32 CCC, in: Damian K. Graf (Hrsg.), Onlinekommentar Übereinkommen über die Cyberkriminalität (Cybercrime Convention) – Version: 26.10.2023. Available at: https://onlinekommentar.ch/de/kommentare/ccc32 (accessed: 16.06.2025).

[15] Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices. Study for the LIBE Committee. Brussels: European Union, 2017. P. 9, 28–30, 66–67.

[16] Crimes related to computer networks. Background paper for the workshop on crimes related to the computer network. Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders. Vienna, 10–17 April 2000 (UN Doc. A/CONF.187/10 of 3 February 2000) (paras. 63–65).

[17] Recommendation No. R (95) 13 of the Committee of Ministers to Member States concerning problems of criminal procedural law connected with information technology (Adopted by the Committee of Ministers on 11 Sept. 1995 at the 543rd meeting of the Ministers' Deputies) (paras. 17–18).

[18] Jurisdiction in Cyberspace. Sino-European Expert Working Group on the Application of International Law in Cyberspace (EWG-IL), Research Group Report 2024. Geneva: Geneva Centre for Security Policy, 2024.

In our view, such unlawful acts can be classified both as those of a territorial character under art. 11 of the RF Criminal Code (based on the physical location of informational resources on the territory of the Russian Federation (in a computer, on a server, etc.)) and of an extraterritorial nature under art. 12 of the RF Criminal Code (on the grounds of the victim's citizenship, direction of the act against the interests of the state).

The general recognition of the actions at issue as unlawful under international law, as internationally wrongful acts attributed to a state does not translate into the universal readiness of countries to classify them as illicit and, moreover, criminalize and penalize them, under their domestic law. In the absence of an express legislative prohibition of such actions, the reactions by the injured countries are normally confined to diplomatic démarches.

For example, in 2015, in connection with the Litvinenko inquiry, the Ministry of Foreign Affairs of the Russian Federation issued an official statement to the effect that "[t]his is not the first time the British "public inquiry" has demonstrated such disregard for international and Russian law: it transpired during the hearings that its secretariat, in order to make enquiries, repeatedly via means of communication contacted potential witnesses located in the Russian Federation without giving advance notice to the Russian authorities. Thereby they extended enforcement jurisdiction of a foreign State to the territory of Russia without the latter's consent, violated its sovereignty and the fundamental international principle of non-interference in internal affairs. By the way, the same legal norms are also in force in the United Kingdom. Witnesses located in the UK must not be contacted directly by means of communication unless UK law enforcement agencies have first been informed"[20].

In addition, the injured state can apply retorsions or reprisals or other countermeasures. The states can hold consultations, negotiations or employ other peaceful means of settlement of their disputes as to the interpretation or application of relevant treaties, arbitration and, finally, as a last resort, submission of the dispute to the International Court of Justice (e.g., in accordance with art. 63 of the Hanoi Cybercrime Convention).

The criminal liability under the new law attaches once the following two major cumulative conditions are fulfilled: first, the actions are to be carried out in violation of the procedure stipulated by an international treaty and (or) the legislation of the Russian Federation (including the principle of reciprocity contained therein), and second, contradict the interests of the Russian Federation. Otherwise, on the one hand, one would have criminalized the activities of representatives of foreign countries' competent authorities occurring in practice that, although performed in violation of the established procedure, – like a foreign officer directly conducting on his own a transborder interview by videolink of a Russian tourist who returned to Russia after falling victim to some ordinary-law criminal offence in the country of the foreign officer, – are devoid of sufficient public danger as they do not run counter to the interests of Russia. On the other hand, where the actions have been carried out in observance of the procedure in force (which presently in all cases requires the prior consent or permission of the Russian competent authorities) but against the interests of the Russian Federation, this would entail significant difficulties in assessing the elements of the *actus reus,* including decisions and actions of the Russian party to give the said consent or permission.

Such high threshold of public danger as an essential element requiring that the act be directed against the interests of Russia to be able to trigger the effect of this blocking statute distinguishes the latter from its foreign counterparts used in developing the bill[21], since they proceed from the sufficiency of whatever unauthorized activities by state actors or their non-state proxies in foreign sovereign space to constitute the *corpus delicti,* regardless of their

[19] See: arts. 272 (illegal access to computer information committed by a person with the use of his official position) and 273 (use of malicious computer programs committed by a person with the use of his official position) of the RF Criminal Code.

[20] Deputy Director of the Information and Press Department, MFA of Russia, Alexander Bikantov's answers to media questions on the Litvinenko case and Dmitry Kovtun's refusal to testify in British court via video link from Russia, 31 July 2015. Available at: http://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/1629306 (accessed: 14.10.2025).

[21] Swiss Criminal Code of 1937 (arts. 271 (unlawful activities on behalf of a foreign state), 299 (violation of foreign territorial sovereignty)); 18 U.S.C. 951 and 28 C.F.R. 73.1–73.6 (actions in the United States as an agent of a foreign government without prior notification to the Attorney General); Penal Code of the Republic of Estonia of 2001 (§ 233 (non-violent acts committed by alien against the Republic of Estonia)).

intents and purposes. Likewise, the Russian law could hardly assimilate and adopt, in and of itself, such comprehensive formula of any and all activities irrespective of the areas of legal relations, within which they take place.

The Russian statute bans a clearly restricted scope of activities that include, firstly, SITs, investigative and other procedural actions, including court proceedings and measures of procedural coercion, in criminal cases, which, due to the inherently compulsory nature of criminal proceedings, in the most perceptible manner interfere with human rights and sovereignty of another state; secondly, any other proceedings related to the process of proof and exercise of other powers of a procedural character as part of civil, arbitration, administrative proceedings and proceedings on administrative offences. At the same time, unlike foreign laws, the Russian criminal statute does not apply to purely administrative, including law enforcement, penitentiary and other extraprocedural measures, extraterritorial "soft power" activities promoting foreign culture, arts, education, science, sports or trade.

On the other hand, the Russian law as a trailblazer in its regulatory endeavor goes beyond what its foreign counterparts have managed to regulate so far, and in accordance with the contemporary and prevalent international legal views on the nature of cyberspace assimilates and equates it, solely for the purpose of application of the new legal norm, to the physical or geographical space of the state territory that includes the land territory, internal waters, territorial sea and air space over them, which in the long term can be expected to contribute to the progressive development of customary international law.

Application of the law in the context of the UN Convention against Cybercrime

Despite all the efforts by Russia and its like-minded allies during the negotiations to elaborate the UN Convention against Cybercrime, the resistance by the collective West and their satellites prevented sufficient safeguards of contracting states' sovereignty, including digital one, finding their way into the Convention, while some extraterritorial "backdoors" were ushered into the treaty. In addition, the attempts to establish minimum global deconfliction rules of the game concerning unilateral proactive extraterritorial cyberexfiltration operations of "government hacking"[22] hit a roadblock of resistance on the part of developed cyber powers, who were allegedly interested in keeping them in a legal grey zone [5].

At the same time, the Convention itself, while establishing specific mechanisms for bilateral cooperation, does not articulate a ban on any unilateral extraterritorial law enforcement actions (and such a ban cannot be definitively deduced from its object and purpose). Like any other anti-crime treaty, the Convention naturally proceeds from the obligation on the part of the requested party to execute an incoming request for access to electronic data or other assistance, and not from the obligation on the part of the requesting party to forward such request in the first place. It provides for the right, but not the obligation, of the party to address the other party with any request for legal or law enforcement assistance.

Therefore, neutralization of the said inevitable conventional extraterritorial backdoors should be carried out primarily at the national statutory and law enforcement level, which Russia did by adopting the law at issue.

Although the Convention does not cover the conduct or responsibility of states, its provisions regarding the obligations of states to cooperate with respect to acts criminalized by the Convention[23] (in particular, illegal access or interception under arts. 7 and 8) may well be applied by states that have been injured by and are investigating the relevant illegal (unlawful under their domestic law, and also constituting internationally wrongful acts under international law) unilateral cross-border actions of specific state actors – individuals, namely foreign law enforcement officers acting in an official capacity[24], and their proxies, taking account of the applicable procedure for engaging international legal immunities.

[22] Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices. Study for the LIBE Committee. Brussels: European Union, 2017. P. 9, 28–30, 66–67.

[23] See, e.g.: Western special services' involvement in anti-Russia activities. Briefing by Foreign Ministry Spokeswoman Maria Zakharova, Moscow, March 20, 2025. Available at: https://mid.ru/ru/press_service/spokesman/briefings/2004214/?lang=en; Interview of Deputy Secretary of the Security Council of the Russian Federation O. Khramov to Rossiyskaya Gazeta, October 11, 2023. Available at: http://www.scrf.gov.ru/news/allnews/3573/ (accessed: 14.10.2025).

[24] See the position of the UN International Court of Justice on a similar issue: Application of the International Convention for the Suppression of the Financing of Terrorism and of the International Convention on the Elimination of All Forms of Racial Discrimination (*Ukraine v. Russian Federation*), ICJ, Judgment of 31 Jan. 2024, paras. 56 and 142.

Conclusion

As a matter of course, when regular channels, methods and means of international anti-crime cooperation for some reason get inoperative, countries have to get inventive in looking for compensatory alternative windows of cross-border opportunities and exploiting all kinds of loopholes and vulnerabilities in order to be able to lay their hands on the required admissible evidence and actionable intelligence overseas. All the more so in a scenario where such much-needed pieces of evidence or intelligence for criminal proceedings are located in a country which is the very target of these very proceedings and cannot reasonably be expected to be cooperative in making a rod for its own back.

The novel ban is expected in the first place to secure a chilling effect with regard to hostile foreign and international law enforcement and judiciary's preparedness to engage in the kind of activities on which it is imposed, and where broken, then to be effectively employed so that the guilty perpetrators get their just deserts, along with making their countries liable for the respective internationally wrongful acts. In times of geopolitical trouble, with Russia currently exposed to the hostile environment, it is a long-awaited and indispensable legal tool aimed at protecting Russia's national security and other essential interests.

That said, a legal framework of the kind had been called for by ordinary law enforcement practices for ages and irrespective of any politics or policies' flux. The last decade's global events just reinforced the need for this norm, contributed to and accelerated its adoption.

Going forward, among others in order to implement arts. 25 and 42 of the UN Cybercrime Convention, a draft of another blocking federal law developed by the Prosecutor General's Office is about to undergo an interdepartmental approval; it is aimed at regulating the procedure for ensuring the preservation (quick-freeze) of specific, individually defined electronic data in excess of the statutory retention periods in case of their expiry, at the request of both foreign and Russian authorities and, at the same time, at blocking, preventing Russian providers, under administrative penalty, from fulfilling foreign requests for preservation or provision of data received directly from abroad.

References:

1. Basova T.B., Kuleshov Yu.I., 2025. Ugolovno-pravovaya zashchita processual'nogo suvereniteta Rossijskoj Federacii (st. 294¹ UK RF): o nekotoryh aspektah zakonodatel'noj novelly [Criminal legal protection of procedural sovereignty of the Russian Federation (art. 294¹ of the RF Criminal Code): on some aspects of the legislative innovation]. *Problemy ekonomiki i yuridicheskoj praktiki [Economic Problems and Legal Practice].* Vol. 21. No. 6. S. 274-280.
2. Golovko L.V., 2022. Gosudarstvo i ego ugolovnoe sudoproizvodstvo: monografiya [State and its criminal proceedings: monograph]. Moscow.
3. Litvishko P.A., 2014. Vozbuzhdenie i rassledovanie ugolovnogo dela o prestuplenii, sovershennom dolzhnostnym licom inostrannogo gosudarstva [Initiation and investigation of a criminal case on a crime committed by an official of a foreign state]. *Mezhdunarodnoe ugolovnoe pravo i mezhdunarodnaja justicija [International criminal law and international justice].* No. 3. S. 5–8.
4. Litvishko P.A., 2023. O rossijskih iniciativah po protivodejstviyu protivopravnomu sboru dokazatel'stv v kiberprostranstve predstavitelyami inostrannyh gosudarstv i mezhdunarodnyh organov [On Russian initiatives for countering unlawful collection of evidence in cyberspace by representatives of foreign states and international authorities]. *Problemy protivodejstviya kiberprestupnosti: materialy mezhdunarodnoj nauchno-prakticheskoj konferencii [Problems of countering cybercrime: proceedings of the International scientific and practical conference] (Moscow, 28 April 2023). The Moscow Academy of the Investigative Committee of the Russian Federation.* Moscow. S. 93–101.
5. Litvishko P., 2024. Pervyj global'nyj dogovor protiv kiberprestupnosti: ot geopoliticheskoj konfrontacii k professional'nomu kompromissu [The first global treaty against cybercrime: from geopolitical confrontation towards professional compromise]. *Mezhdunarodnaya zhizn' [International life].* No. 11. S. 4–27.
6. Ugolovnyj process Rossii i stran Evropy: sravnitel'no-pravovoe issledovanie: monografiya [Criminal procedure of Russia and countries of Europe: comparative law study: monograph]. *General and scientific editor S.P. Shcherba.* 2023, Moscow.
7. Collecting Electronic Evidence in Criminal Cases in Russia and Foreign Countries: Experiences and Problems: Monograph. *Ed. by S.P. Shcherba (Russian ed.) and P.A. Litvishko (English ed.).* 2024, Moscow.
8. Damian K. Graf, 2023. Kommentierung zu Art. 32 CCC [Commentary on Art. 32 CCC]. *Damian K. Graf (Hrsg.). Onlinekommentar Übereinkommen über die Cyberkriminalität [Online commentary on the Convention on Cybercrime] (Cybercrime Convention).* Version: 26.10.2023. URL: https://onlinekommentar.ch.

9. Delerue F., Zhu L., Wrange P., Yang F., 2024. Working Paper: The Principle of Sovereignty and the Application of International Law in Cyberspace. *EU Cyber Direct – EU Cyber Diplomacy Initiative.* April. URL: https://eucyberdirect.eu.
10. Koops B.-J., Goodwin M., 2016. Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities of International Law. *Tilburg Law School Legal Studies Research Paper Series.* No. 5.
11. Litvishko P.A., 2025. A beacon of hope among "the unfriendly". *Pravo i upravlenie. XXI vek [Journal of Law and Administration].* No. 3(76). S. 17–29.
12. Litvishko P.A., 2016. Non-Treaty Forms of Extraterritorial Judicial and Law Enforcement Activities. *Collection of Materials on International Cooperation of the Investigative Committee of the Russian Federation.* Moscow. P. 132–173.
13. Novo L., 2025. In or Out? Managing Risks from the UN Cybercrime Convention. *2025 17th International Conference on Cyber Conflict: The Next Step.* Ed. by C. Kwan, N. Gratzer, K. Podiņš, M. Tolppa. CCDCOE Publications. Tallinn. P. 57–74.
14. Osula A.-M., 2017. Remote search and seizure of extraterritorial data: PhD in law dissertation. Tartu.
15. Research Handbook on Extraterritoriality in International Law. *Edited by A. Parrish and C. Ryngaert.* 2023, Cheltenham, UK; Northampton, MA, USA.
16. Ryngaert C., 2023. Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts. *German Law Journal.* Vol. 24. Special Issue 3. P. 537–550.
17. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. *Ed. by M.N. Schmitt, L. Vihul.* 2017, Cambridge.

ПЕРВЫЙ «БЛОКИРУЮЩИЙ» ЗАКОН ПРОТИВ НЕПРАВОМЕРНОЙ ИНОСТРАННОЙ ПРАВООХРАНИТЕЛЬНОЙ И СУДЕБНОЙ ДЕЯТЕЛЬНОСТИ В КИБЕРПРОСТРАНСТВЕ

Введение. *Федеральным законом от 31 июля 2025 г. № 282-ФЗ УК РФ дополнен ст. 294[1] (незаконное осуществление следственных, иных процессуальных действий и оперативно-разыскных мероприятий на территории РФ). Публикация представляет собой комментарий к ней с акцентом на ее применение к действиям в информационном пространстве. Освещаются обстоятельства принятия и международно-правовые аспекты новеллы, анализируются признаки состава преступления, особенности производства по уголовному делу о нем, а также действие закона в контексте Конвенции ООН против киберпреступности.*

Материалы и методы. *В статье исследуются соответствующие международные договоры и обычное международное право, мягкое право, а также национальные и иностранные законы и правила. В качестве источников используются также судебная практика, правоприменительная практика межгосударственных, российских и зарубежных правоохранительных органов, а также научная литература. Методологическую основу исследования составили формально-юридический и сравнительно-правовой методы, методы системно-структурного анализа и синтеза социально-правовых явлений.*

Результаты исследования. *Новая норма права относится к «блокирующим» законам (blocking statute), направленным на предотвращение (блокирование) применения на территории издавшего их государства законодательства другого государства, и исходит из юридической фикции «территориализации» киберпространства. Проблема чужого экстратерриториального правоприменения на российской территории актуализировалась в связи с проведением специальной военной операции и сопутствующими ей рисками нелегитимного сбора и вывода противником доказательств с территории нашей страны извне, по понятным причинам преимущественно в удаленном виртуальном режиме, без физического присутствия «на земле». Российский закон по-новаторски пошел дальше иностранных аналогов, что в долгосрочной перспективе должно способствовать и прогрессивному развитию международного права.*

Обсуждение и заключение. *Объективная сторона преступления выполняется непосредственно самим иностранным или международным должностным лицом либо опосредованно через их прокси, при этом не должны выдвигаться требования о завершенности действия или реализации в полном объеме его результатов, такой*

как использование затем этих результатов в доказывании по делу, об обязательном наличии фиксации проводимого или проведенного действия в протоколе или иного процессуального оформления, включая аудио- и видеозапись иностранцами. Иммунитет обвиняемого должностного лица рассматривается, задействуется либо осуществляется отказ от него, устанавливается его наличие или отсутствие в соответствии с правилами внутригосударственного законодательства и общего международного права. Вместе с тем обычно-правовые нормы международного права в основном исходят из отсутствия иммунитета в делах о подобных деяниях, нарушающих территориальный суверенитет и схожих с преступлением шпионажа. Преступление совершается с «тройным» прямым умыслом провести запрещаемое действие, при этом нарушить установленный порядок его проведения и преследовать цель, которая противоречит интересам России; также обязательно наличие признака заведомости для виновного нахождения лица, с участием которого планируется проведение действия по средствам связи, в пределах территории России. Выявление преступления и привлечение виновных к ответственности могут осуществляться различными описанными в статье способами и средствами. Нейтрализация экстратерриториальных «закладок», содержащихся в Ханойской конвенции против киберпреступности, должна осуществляться в первую очередь на национальном нормотворческом и правоприменительном уровне, что и было реализовано российским законодателем. Несмотря на то что Конвенцией не охватываются поведение и ответственность государств, ее положения в части обязанностей стран сотрудничать в отношении криминализированных Конвенцией деяний (в частности, незаконных доступа и перехвата) вполне могут применяться государствами, пострадавшими и расследующими соответствующие неправомерные односторонние трансграничные действия конкретных государственных акторов и их прокси, с учетом правил о порядке применения международно-правовых иммунитетов.

Литвишко Петр Андреевич,
кандидат юридических наук,
заместитель начальника Главного
управления международно-правового
сотрудничества Генеральной прокуратуры
Российской Федерации – начальник
управления правовой помощи
и правоохранительного содействия,
старший помощник Генерального
прокурора Российской Федерации,
Москва, Россия.

Ключевые слова:
ст. 294[1] УК РФ, неправомерная правоохранительная деятельность в киберпространстве, блокирующий закон, Конвенция ООН против киберпреступности, международно-правовой иммунитет

Keywords:
article 294[1] of the RF Criminal Code, unlawful law enforcement in cyberspace, blocking statute, UN Convention against Cybercrime, international legal immunity

Литература:

1. Басова Т.Б., Кулешов Ю.И. Уголовно-правовая защита процессуального суверенитета Российской Федерации (ст. 294[1] УК РФ): о некоторых аспектах законодательной новеллы // Проблемы экономики и юридической практики. 2025. Т. 21. № 6. С. 274–280.
2. Головко Л.В. Государство и его уголовное судопроизводство: монография. М., 2022.
3. Литвишко П.А. Возбуждение и расследование уголовного дела о преступлении, совершенном должностным лицом иностранного государства // Международное уголовное право и международная юстиция. 2014. № 3. С. 5–8.
4. Литвишко П.А. О российских инициативах по противодействию противоправному сбору доказательств в киберпространстве представителями иностранных государств и международных органов // Проблемы противодействия киберпреступности: материалы международной научно-практической конференции (Москва, 28 апреля 2023 г.). М.: Московская академия Следственного комитета Российской Федерации, 2023. С. 93–101.
5. Литвишко П. Первый глобальный договор против киберпреступности: от геополитической конфронтации к профессиональному компромиссу // Международная жизнь. 2024. № 11. С. 4–27.
6. Уголовный процесс России и стран Европы: сравнительно-правовое исследование: монография / Под общ. и науч. ред. С.П. Щербы. М., 2023.
7. Collecting Electronic Evidence in Criminal Cases in Russia and Foreign Countries: Experiences and Problems: Monograph / Ed. by S.P. Shcherba (Russian ed.) and P.A. Litvishko (English ed.). Moscow, 2024.

8. Damian K. Graf, Kommentierung zu Art. 32 CCC // Damian K. Graf (Hrsg.), Onlinekommentar Übereinkommen über die Cyberkriminalität (Cybercrime Convention) – Version: 26.10.2023. URL: https://onlinekommentar.ch.
9. Delerue F., Zhu L., Wrange P., Yang F. Working Paper: The Principle of Sovereignty and the Application of International Law in Cyberspace // EU Cyber Direct – EU Cyber Diplomacy Initiative, April 2024. URL: https://eucyberdirect.eu.
10. Koops B.-J., Goodwin M. Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities of International Law // Tilburg Law School Legal Studies Research Paper Series. No. 05. 2016.
11. Litvishko P.A. A beacon of hope among "the unfriendly" // Право и управление. XXI век. 2025. № 3(76). С. 17–29.
12. Litvishko P.A. Non-Treaty Forms of Extraterritorial Judicial and Law Enforcement Activities // Collection of Materials on International Cooperation of the Investigative Committee of the Russian Federation. Moscow, 2016. P. 132–173.
13. Novo L. In or Out? Managing Risks from the UN Cybercrime Convention // 2025 17th International Conference on Cyber Conflict: The Next Step / Ed. by C. Kwan, N. Gratzer, K. Podiņš, M. Tolppa. Tallinn, 2025. P. 57–74.
14. Osula A.-M. Remote search and seizure of extraterritorial data: PhD in law dissertation. Tartu, 2017.
15. Research Handbook on Extraterritoriality in International Law / Edited by A. Parrish and C. Ryngaert. Cheltenham, UK; Northampton, MA, USA, 2023.
16. Ryngaert C. Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts // German Law Journal. 2023. Vol. 24. Special Issue 3. P. 537–550.
17. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / Ed. by M.N. Schmitt, L. Vihul. Cambridge, 2017.