The First Global Treaty against Cybercrime: from Geopolitical Confrontation towards Professional Compromise

In August 2024, the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (hereinafter referred to as the Ad Hoc Committee), established by UN General Assembly Resolution 74/247 of 27 December 2019, approved the draft 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 (hereinafter referred to as the Convention or UN Convention[1]), and submitted it to the General Assembly for adoption. The treaty has been drafted over four years, with Ad Hoc Committee sessions and inter-sessional consultations held at UN headquarters in New York and Vienna.[2]

Foreign policy aspects of the Convention

The nature and image of crime and law enforcement of today are high-tech and sophisticated and no longer have much in common with the confrontation between their counterparts from Čapek's "Pocket Stories" of the relatively recent twentieth century. It is redundant to mention here the ubiquitous statistics about the exponential growth of cybercrime both at home and abroad to simply state that this global international treaty is a more than timely, long-awaited and momentous development for the world community.

Be that as it may, the negotiation process for the Convention, initiated by our country, was all along burdened by the extremely unfavourable geopolitical context of peaking international tension and many times teetered on the brink of failure. The civilizational clash between the neoliberal collective West and its

satellites and a large part of the world majority, especially the Islamic world, was expectedly reflected in it, as in a bad miniature, which was vividly highlighted by the Iranian-initiated vote on the draft Convention.

The early stages of the treaty's development took place against the backdrop of anti-Russian statements made by diplomatic agents of the opponents, who showed a lack of commitment to mutually respectful or at least purely pragmatic cooperation, provoking retaliatory measures. Closer to the finalization of the document, "diplomatic" blackmail and the creation of artificial time pressure were practiced. Such aggressive pursuit of a political agenda largely drowned out professional interstate dialogue among law enforcement, justice and digitalization experts, exacerbated the lack of mutual trust and a destructive environment in which the acceptance or rejection of certain proposals by delegates-practitioners on the text of the Convention sometimes depended not so much on their merits as on the author state.

The contributions from engaged multi-stakeholders – NGOs and Western IT corporations – as well as the arbitrary visa barriers incompatible with UN host country status played their destabilizing part. Influenced by such extraneous factors, the truth in such disputes is sometimes not born at all, and if it is born, it may die in infancy, and the dispute itself degenerates into a conflict lacking constructiveness.

The delegations were compelled to waste resources looking out for all sorts of malicious backdoors,[3] logic bombs and "Easter eggs" in the text of the draft Convention, in short, to identify vulnerabilities and signs of bad faith on the part of counterparties who might have introduced those vulnerabilities during the drafting process.

The development and promotion of Russian approaches in the Ad Hoc Committee and their consolidation in the form of specific norms in the Convention was facilitated by coordinated joint work within the Interagency

Working Group (IWG) and during the sessions of the Ad Hoc Committee, numerous negotiations with like-minded and constructive delegations organized by the Russian Ministry of Foreign Affairs, awareness-raising work, presentations of the monograph and report on the sidelines of the session (available in the UNODC SHERLOC portal and on the Ad Hoc Committee's website).[4]

The Public Prosecutor's Office of the Russian Federation, along with the Ministry of Foreign Affairs of Russia, plays a leading role in determining the global rules of the game in the international legal virtual field; the functions of these agencies to coordinate the activities of law enforcement agencies in combating crime, on the one hand, and to coordinate the implementation of a unified foreign policy of the State in this area and to coordinate the activities of federal executive bodies to implement the State policy in the field of international information security, on the other hand, are complementary.

By Order No. 352 of the Prosecutor General of the Russian Federation of 6 July 2020, an IWG on countering information crime was established under the auspices of the Prosecutor General's Office of the Russian Federation to participate in the work of the Ad Hoc Committee, to develop a consolidated Russian position on the draft Convention, and to work on issues related to improving the effectiveness of law enforcement agencies in combating cybercrime. The group, headed by the Deputy Prosecutor General, includes representatives of the Prosecutor General's Office, the Ministry of Foreign Affairs, the Office of the Security Council, the Investigative Committee, the Ministry of Internal Affairs, the Federal Security Service, the Foreign Intelligence Service, the Ministry of Digital Development, Communications and Mass Media and the Ministry of Justice.

As the part of its mandate to develop the Convention has been completed, the IWG's further work will be aimed, inter alia, at ensuring the implementation of domestic procedures for its entry into force for Russia (drafting declarations

and reservations, amending the current legislation of the Russian Federation with a view to ratification), as well as developing an additional protocol to the Convention (it is expected to contain only the substantive part – additional elements of acts subject to criminalization).

For example, a draft federal law developed by the Prosecutor General's Office of the Russian Federation is currently undergoing interdepartmental approval; it is aimed at regulating the procedure for ensuring the preservation of electronic data at the request of both foreign and Russian authorities and, at the same time, at preventing Russian providers from fulfilling foreign requests for the preservation or provision of data received directly from abroad.

Whether the entry into force and operation of the UN Convention will have a downward effect on the process of new accessions to the 2001 Council of Europe Convention on Cybercrime (Budapest Convention), remains to be seen.

On the one hand, main norms of the Budapest Convention have been reproduced or improved, although not fully updated, in the UN Convention adopted nearly a quarter of a century later. On the other hand, the mother 2001 Convention remains competitive insofar as it was substantially modernized in 2022 through the adoption of its Second Additional Protocol on enhanced co-operation and disclosure of electronic evidence, which contains relevant simplified extraterritorial mechanisms that are closer to the European Union's mutual recognition-based order instruments and which the UN Convention did not and a priori could not include, namely: direct disclosure by domain name registrars and ICT service providers, located in the territory of a state party to the Protocol, of information in their possession or control on domain name registrants or subscribers, pursuant to a request or an order of law enforcement or judicial authorities of another state party (in many respects, due to reservations, regimes of notifications and consultations with the state of the service provider, this provision may boil down to inter-State interaction); giving

effect to orders from another state party for expedited production of subscriber information and traffic data; expedited disclosure of stored computer data through the 24/7 Network points of contact without a request for (legal) assistance and provision of mutual (legal) assistance in emergencies; the language of communications, including direct communications with service providers. A state cannot participate in the Protocol with this simplified regime without participating in the mother Convention.

The application of the new global treaty should also take into account the risks of its possible bad-faith instrumentalization for political and military purposes, such as those emanating 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 already been created with substantial funding.[5] Such electronic evidence may be obtained under the Convention indirectly, exfiltrated via various proxies and under the guise of unrelated proceedings on ordinary-law crimes.

To prevent the materialization of such and other scenarios of threats to national security, the Regulation on interagency cooperation in processing requests from competent authorities of foreign States related to crimes and other offences committed through the use of information and telecommunications technologies, computer attacks and computer incidents has been developed and is currently being approved.

The main content of the Convention can be divided into substantive (criminalization of acts) and procedural, as well as intrastate and interstate (domestic and international) parts. This publication focuses mainly on the procedural and interstate parts, taking stock of their respective advantages and disadvantages, and reproducing the drafting history to highlight the intentions of the drafters as a means of treaty interpretation.

Scope of the Convention

Russia has consistently advocated the need for comprehensive scope of the Convention in accordance with the established mandate of the Ad Hoc Committee in both its substantive and procedural parts, low thresholds for anti-crime cooperation, while the opposing camp insisted on the maximum narrowing and high thresholds for activation of obligations; called for "not stealing the air" for less important requests, not overloading countries' limited resources with them in a counterproductive way, not to mention those that do not meet the dual criminality requirement, in matters of administrative offences, *de minimis*, which, among other things, would not take into account the cumulative effect of less serious offences and would have a negative impact on crime prevention.

In the end, however, the possibility of executing such requests was included in the Convention as an exception to the rule of refusal – at the free discretion of the requested party, similar to the 2000 UN Convention against Transnational Organized Crime (Palermo Convention) and some other conventions. If the condition of dual criminality is not met, the requested party may also refuse to preserve the data.

The obligations of parties to the Convention regarding international cooperation in the exchange of electronic evidence (in contrast to the domestic regime) and within the 24/7 network are limited, in addition to the offences established in accordance with the Convention, to serious crimes as defined in the Convention, whereas, for example, under the Budapest Convention, such a limitation can be imposed by states parties only on the interception of the content of communications or traffic data.

However, the scope of international cooperation is narrowed mainly by way of circumscribing its principal forms exclusively in relation to the offences established in accordance with the treaty (set out in its chapter on

criminalization), in particular extradition, temporary transfer of persons in custody, transfer of criminal proceedings, joint investigations, any provisional and confiscatory measures against assets and even law enforcement cooperation (article 47).

Several provisions of the Convention (including article 38 on the transfer of sentenced persons) are formulated as discretionary rather than imperative (the requested party may, but is not obliged to provide assistance – may vs. shall), which, although occurring in treaty practice, largely deprives these norms of added value since for such a "may" states do not need to conclude an international treaty among themselves, which is always aimed at creating mutual obligations, and are free to provide the relevant assistance at their own discretion, including based on the principles of reciprocity or international comity. Therefore, the wording "shall endeavor" or "shall take (effective, appropriate) measures (steps)" has been used as a compromise solution to certain key provisions of the Convention that did not find consensus.

The fundamentally important norms on international cooperation in the real-time collection of traffic data and interception of content of communications, by analogy with the Budapest Convention (although it lays down a direct obligation for such cooperation, and not only the endeavor toward it, as in the UN Convention), only operate by reference to other treaties and (or) the national legislation of the parties and are applied only in conjunction with them. Some delegations did not accept the imperative nature of these norms on the grounds that they lacked the resources in their countries for this type of cooperation. Interception of content cannot generally be provided by the United States.[6]

The Convention, like a number of other UN conventions, for the purposes of both domestic and interstate application, uses the stage triad of investigation, prosecution and judicial proceeding.[7]

In contrast to Russian criminal proceedings, (criminal) investigation in the universal international legal framework means, in addition to our procedures of preliminary investigation or inquiry, also pre-investigative verification of reports of offences and operational search measures, as well as financial investigations by financial intelligence units.[8]

International literature outlines reactive investigation and proactive investigation (usually related to the use of controlled delivery, infiltration, etc.), sometimes also disruptive investigation, which in principle correspond to our concepts of investigation and prosecution, detection and suppression of crime, respectively.[9]

The supranational EU order instruments employ the formula of "reasonable grounds to believe that the offence has been committed, is being committed or is likely to be committed" to enable cross-border exchange of evidence, including electronic evidence,[10] within the EU.

The reluctance of opponents to extend the Convention's mechanisms of cooperation (legal and law enforcement assistance, with the exception of preventive measures, limited information exchange and technical assistance), especially those representing intrusive coercive measures requiring a judicial decision, to the stages of detection, prevention and disruption of crimes, both in the domestic and international context of the application of this global treaty, has been largely circumvented and overcome.

In addition to the Convention's cross-cutting use of the pair "prevent and combat" and article 47 (Law enforcement cooperation) of the Convention, this has been achieved mainly by providing the necessary definition of the term "criminal investigation" in the Interpretative notes on specific articles of the Convention, which in fact constitute an integral annex to the Convention, including through article 19 of the Convention on the preparation for an offence and attempt to commit an offence (inchoate offences). In this context, the

functional features of the 24/7 network (article 41) are also of particular importance.

According to paragraph 4 of the Interpretative notes (on articles 23 and 35 of the Convention), the term “criminal investigations” covers situations where there are reasonable grounds to believe, on the basis of factual circumstances, that a criminal offence (including an offence set out in article 19 of the convention) has been committed or is being committed, including when such an investigation is aimed at stopping or impeding the commission of the offence in question.

Thus, "investigation" in its international legal universal interpretation, for the domestic and international components of the Convention throughout its text, may encompass both investigative actions and proactive covert operational search measures as they are understood in Russian law – at the stages of detection, prevention and frustration of criminal offences.[11]

It is important to note that the Budapest Convention has been surpassed in this respect, which, in its literal interpretation, does not contain any indication as to the applicability of its mechanisms to the stages of crime prevention.

Many delegations took a firm stance on the need for a high threshold to deploy the relevant norms of the Convention – only in the case of a crime already committed, later pointing to the non-binding nature of the Interpretative notes.[12]

In addition to such statements, which are likely to be made to the Convention by individual States Parties, it would be difficult for the Russian Federation for another reason to use the provisions of the Convention relating to international cooperation in collecting electronic evidence, in particular articles 44 (search and similar access, seizure and disclosure of stored electronic data), 45 (real-time collection of traffic data) and 46 (interception of content data), not for investigative[13] or judicial actions, but for requesting and carrying out operational search measures[14] in criminal intelligence cases in the absence of

a pre-investigative examination or a criminal case initiated. The fact is that the Convention requires these measures to comply with the procedure of mutual legal (judicial) assistance in the field of criminal justice, which under Russian law (articles 453–457 of the Criminal Procedure Code of the Russian Federation (RF CPC)) is possible only in the framework of criminal proceedings (preliminary investigation or at least examination of a crime report, as well as court proceedings) and is aimed at obtaining admissible evidence in the case, while operational search measures are generally conducted through international law enforcement (police-to-police) assistance, aimed at obtaining indicative, operationally relevant information. The Budapest Convention in all relevant cases uses a more favorable and broader concept of "mutual assistance" (articles 31, 33 and 34), which can cover both legal assistance and law enforcement cooperation.

The formula achieved made it possible to compensate to some extent for the completely absurd, from the point of view of the inherent arsenal of means and methods of combating cybercrime, vanishing from the Convention, due to the passive position of the majority, of the classical norm on covert special investigative techniques, available in the Palermo Convention and other universal instruments.

By and large, due to misunderstanding by some delegations of the essence of the issue, the Convention did not include the traditional institution of consular legal assistance in criminal matters,[15] complemented by provisions on the videoconferencing or telephone conferencing, from the Russian draft Convention of 2021 (article 54). In fact, little of this initial draft remains in the Convention.[16] The Convention does not make any mention of the modern problems of electronic immunities, including international legal immunities, in criminal proceedings.[17]

The treaty does not encourage States Parties, despite the urgent need to do so, for the purpose of effectively ensuring the admissibility and legal validity of

evidence collected in accordance with the Convention, to consider establishing among themselves secure platforms and channels of communications that provide authentication and certification of requests for legal assistance and evidence transmitted solely in digital (paperless) form, and when necessary, mutual recognition of electronic signatures, seals or stamps affixed to such requests and evidence, where appropriate, incorporating the said platforms and channels into 24/7 contact points. A vague norm only remotely resembling such a provision is set forth in article 40(14) (legal assistance) of the Convention.

The opponents' opposition to the scope had another obvious explanation. Participation in the Budapest Convention, although claiming global rather than regional status, and its protocols for non-members of the Council of Europe is actually linked to membership in a select club of "developed democracies", the door to which is cracked only by invitation of the Committee of Ministers of the Council of Europe, while the UN Convention is wide open for any state to be admitted. The developed democracies are unwilling to cooperate with those who are listed in their ranking as rogue states, allegedly violating human rights and misbehaving in cyberspace, to the same extent and according to the same rules as among themselves within a decent society. The final product of common efforts shows that this unwillingness has been overcome in one way or another.

Human rights

The pro-Western camp has sought to saturate the Convention with provisions that would prevent its application, both in the domestic context and for international cooperation, on broad grounds of threats to human rights. The unprecedented extent to which the treaty being drafted intrudes into fundamental human rights and freedoms, in particular those relating to secrecy of communication, personal privacy and secrets, and the need to introduce corresponding safeguards for their observance, were emphasized.

As is known, who wants to cooperate looks for opportunities, who does not want – for reasons. In the case of the Convention, there is no need to look for acceptable reasons for refusing the requested assistance – there is a variety of them for all cases, in particular, in article 40(21), and two of them, due to the current case law, can be considered as comprehensive, covering a number of others – possible prejudice to *ordre public* and contradiction with the requirements of the legal system of the requested State. Therefore, along with the potential for their political misuse mentioned below, all other things being equal and from the purely practical point of view of the work of countries' central and other competent law enforcement and judicial authorities on legal and law enforcement assistance, it is justified to perceive the fight against the human rights "backdoors" in the Convention as tilting at windmills.

These are everyday scenarios of bilateral communications between the requesting and requested states parties to the Convention to grant or deny legal assistance to each other on the grounds set out in the Convention. And nothing prevents, for example, the Conference of the Parties to the Palermo Convention, which does not contain broad human rights "guardrails", or any other convention review mechanisms from addressing human rights violations in their application.

The provisions of article 6(2) (Respect for human rights) of the Convention (even grammatically flawed, like the name of the Convention, as a result of unwillingness to undo the reached compromise) became one of the most non-consensual in the negotiation process, but withstood the voting. Article 24 of the Convention lays down broad conditions and safeguards to ensure human rights, including the principle of proportionality, while article 36, among the rules on personal data protection, actually contains an additional ground for refusal to cooperate with reference to domestic legislation on personal data protection. In addition, the classic human rights formula for denying extradition on grounds of

discrimination is also extrapolated to grounds for refusal of legal assistance, which is not found in the existing sectoral conventions.

At first glance, a legitimate question arises: who among us fulfilling our voluntary obligations under international human rights treaties and having enshrined similar values and their guarantees in the Basic Law of our country, sharing and professing them, can be against these right formulations of the Convention? Their rejection by many countries is primarily due to the "dilution" of the provisions of the anti-crime convention with human rights language that is not inherent to its purposes, which, in turn, has no analogues in the past and creates an undesirable precedent, as well as to the danger of their weaponization for political gain, to the detriment of bilateral cooperation between the parties to the Convention. This danger may come from any third party to the Convention or group of such parties wishing, directly, or else indirectly through the Conference of the Parties, to try on the role of self-proclaimed assessor of compliance with the requirements of the Convention in this part, and name and shame both the requesting country and, primarily, the assisting state for their real or perceived violations, blacklist and monitor wrongdoers, impose sanctions against them, which would have a dissuasive, chilling effect on bilateral cooperation under the Convention.

Orwellian conspiracy theories were also exploited as part of the human rights agenda. The process of drafting and adopting the Convention at all stages was accompanied – just as its application will predictably be – by incompetent bluster and downright disinformation misrepresenting it as an alleged tool of national security – mass surveillance (interception) of bulk communications, especially in the hands of non-democratic regimes.

Evidently, the Convention itself has nothing to do with national security intelligence or counterintelligence; it rests exclusively in the domain of criminal justice, is aimed at obtaining admissible evidence subject to judicial review (while

the intelligence community cares little about the admissibility of evidence), and can also serve for law enforcement or criminal intelligence. It is precisely to dispel any concerns about this that the text includes, by analogy with the Budapest Convention and in the view of many, redundantly for reasons of obviousness, the words "specific/specified" to refer to individual, particular criminal investigations, prosecutions or judicial proceedings and the data and communications gathered within them, as opposed to general, proactive and indiscriminate capturing and retention of data. At one time, particularly in the wake of the Snowden revelations, the Budapest Convention Committee was hard-pressed to fend off similar attacks from the European Union in connection with the drafting of the prototype of the second additional protocol to that Convention and in the context of its article 32(b).[18]

There were no prospects for agreement on the related issue of establishing obligations for ICT service providers to retain data, including because of positions that the Convention should not impose such obligations on the private sector, which would also entail prohibitive, and for many of its representatives unaffordable, costs. The situation was similar when the Budapest Convention was being adopted.[19]

Extraterritorial "backdoors"

The Russian Federation took a strong stance against the expansive extraterritorial reach of the treaty, especially the introduction of any provision similar to article 32(b) of the Budapest Convention. At the same time, given that the central level of cyberspace is formed of the logical (virtual) layer that has no material or geographical boundaries, the territorial sovereignty safeguards enshrined in article 5 of the Convention easily become ephemeral, subject to free interpretation by an interested party, whose point of view would depend on their point of location within the physical space of a particular country.

As already mentioned, the Ad Hoc Committee missed the unique chance to ensure regulation of the prevention of unilateral cross-border surreptitious cyber operations undertaken by the States Parties, which aim at bypassing bilateral coordination, risk generating blue-on-blue undercover activities, abuses of human rights, tensions between states and generally run counter to international law in terms of both the state sovereignty and the human rights protection[20]. The attempts to establish minimum global rules of the game in this area hit a roadblock of resistance on the part of developed cyber powers of the collective West, who were allegedly interested in keeping their unilateral proactive extraterritorial cyber operations of “government hacking” in a legal grey zone, – again, under the plausible excuse that the highly extensive interference of covert measures with the human rights sphere is undesirable, apart from those enshrined in the Convention (electronic surveillance in the form of covert interception of traffic and content data).[21]

In turn, a draft "blocking" federal law, which is currently under consideration at the State Duma of the Federal Assembly of the Russian Federation, was developed to preclude foreign and international bodies from undertaking unilateral measures to illegitimately collect evidence and intelligence themselves, on their own, including electronic evidence, in or from the territory of the Russian Federation, including through remote cross-border contacts from abroad with individuals and legal entities located on the territory of the Russian Federation, or to lure Russian nationals in this manner to travel abroad in order to detain them there.[22]

The state, by consenting, in whatever form, to hosting in its territory of a foreign service provider’s servers, networks and other equipment, generally gives thereby its express or implied consent to such provider’s using or otherwise processing, including for extraterritorial law enforcement purposes, the data stored in or transmitted through them, being in the possession or under the

control of this provider, unless such hosting state establishes stringent localization rules for such data or otherwise conditions their processing, for example, based on the nationality of the subject of the processed personal data. Conversely, the state, whose provider offers its services abroad, places its technical infrastructure there, or even gets legally localized (“landed”) by the receiving country, normally thereby consents to its service provider’s interacting with such countries’ authorities, including in the law enforcement area, and irrespective of the nationality of the subject of the personal data processed.

Therefore, in practice there objectively exists the positive conflict of several states’ jurisdictions over data depending on the location of: the service provider; storage or transmission of the data and/or device (equipment) used for the storage or transmission of the data; subscriber (end-user), to which under certain circumstances one could add the state of the subscriber/user’s nationality.

Article 27 of the Convention has a considerable extraterritorial potential, although, unlike article 32 of the Budapest Convention, is included in the domestic rather than international section of the treaty. One should note that the "domestic" articles require that a state party establish for its authorities powers that are only regarded as minimum powers under the Convention, leaving entirely up to the state party the scope of their extension (article 59).

According to article 27 of the Convention, which is similar to article 18 of the Budapest Convention, each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a) A person in its territory to submit specified electronic data in that person's possession or control that are stored in an information and communications technology system or an electronic data storage medium; and b) A service provider offering its services in the territory of the State Party to submit subscriber information relating to such services in that service provider's possession or control.

Thus, the provisions of article 27(a) of the Convention do not preclude their potential application to enable unilateral transborder access for the authorities of one state to data stored in the territory of another state, without employing the procedures of international legal or law enforcement assistance, by recourse, with the use of coercive measures if necessary, to the person that has the data at his/her disposal, whose nature, ownership and legality of possession by that person are not limited in any way.

Such person may be any individual or legal person who has illegal remote extraterritorial access to servers and other devices in another state and the data stored therein, which in turn may come into his/her possession as a result of committing an offence covered by the Convention and thus be legalized by that norm of the Convention for the purposes of criminal proceedings; this person may be a defector carrying classified information or the like. Finally, despite the existence of a special extraterritorial norm on service providers in the next paragraph "b" of the same article, the interpretation material concerning the identical article 18 of the Budapest Convention fairly states that paragraph "a" also covers service providers.[23] Unlike the strictly limited nature of the data referred to in paragraph "b", their categories in paragraph "a" in the articles of both Conventions are not restricted in any way. Providers, and first of all foreign providers, may have at their disposal any data from foreign servers and other devices.[24]

Article 27(b) of the UN Convention contains a target jurisdictional criterion empowering the parties' competent authorities to directly order a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. Thus, given the volatility of the location of data in the cloud, the only factors that matter are the location where the service is offered and the fact that the data of interest are possessed or controlled by the service provider, but not

the location (including abroad) of the service provider or the data (servers) themselves.

The Budapest Convention Committee's guidance note defines the notions of the "offering services in the territory of a Party" and the "real and substantial connection" of a service provider to that Party. "Parties could consider that a service provider is "offering its services in the territory of the Party", when: the service provider enables persons in the territory of the Party to subscribe to its services (and does not, for example, block access to such services); and *(cumulative condition – P.L.)* the service provider has established a real and substantial connection to a Party. Relevant factors include the extent to which a service provider orients its activities toward such subscribers (for example, by providing local advertising or advertising in the language of the territory of the Party), makes use of the subscriber information (or associated traffic data) in the course of its activities, interacts with subscribers in the Party, and may otherwise be considered established in the territory of a Party. The sole fact that a service provider makes use of a domain name or electronic mail address connected to a specific country does not create a presumption that its place of business is located in that country. Therefore, the requirement that the subscriber information to be produced is relating to services of a provider offered in the territory of the Party may be considered to be met even if those services are provided via a country code top-level domain name referring to another jurisdiction."

The guidance note also indicates that "[l]egal regimes increasingly recognise that, both in the criminal justice sphere and in the privacy and data protection sphere, the location of the data is not the determining factor for establishing jurisdiction."

The Convention does not contain the norm (which has not actually been pushed for by anyone actively) similar to article 32(b) of the Budapest

Convention, which Russia regards as contentious, on the right and power to unilateral trans-border access to computer data that are stored in another State Party to the Convention and are not publicly available, with the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the foreign party, and without a mandatory notification to this other State. As an example of the application of the norm, one usually refers to an inspection of the (cooperative) suspect's device with an open mailbox, whose data is located in another State Party to the Convention (on a foreign domain/server), with his consent. Other scenarios of an unlimited scope, wherever and whenever the person in question is located, are also possible.

In its official interpretation given by the Budapest Convention Committee's guidance note, this norm is practically not applicable to soliciting from foreign ICT service providers the data of their customers, since, allegedly, "[s]ervice providers are unlikely to be able to consent validly and voluntarily to disclosure of their users' data under Article 32. Normally, service providers will only be holders of such data; they will not control or own the data, and they will, therefore, not be in a position validly to consent".[25] (This interpretation contradicts another guidance note of the Committee to article 18 of the Convention (article 18(1)(a)) that points to service providers being included in the range of similar authorized persons.[26])

By comparing the provisions of the UN Convention and those of the Budapest Convention in the sections at hand, it can be concluded that if the person providing the consent pursuant to article 32(b) of the Budapest Convention is located not abroad,[27] but on the territory of the state whose authority is obtaining access to the data located overseas (the main scenario under article 32(b)), the provisions of article 32(b) of the Budapest Convention will largely coincide with the provisions of its article 18(1)(a and b) and article 27 of the UN Convention. Possibilities of the extraterritorial reach for the purposes

of preservation of and access to data are also contained in articles 16 and 17 of the Budapest Convention and articles 25 and 26 of the UN Convention, as they do not limit the range of persons obligated to respond to orders from competent authorities, nor do they refer to other territorial elements of their application.

Thus, the main differences between article 27 of the UN Convention and article 32(b) of the Budapest Conventon taken together point to the greater potential extraterritorial reach of article 27 of the UN Convention as compared to article 32 of the Budapest Convention in cases of the above scenario and can be summarized as follows:

in the former, the specified data are submitted by the person, while in the latter, the specific data are accessed or received by the competent authorities on their own or through somebody via a computer system located in the territory of their state. The desired outcome is the same: getting possession of the sought data from overseas; although, in the case of their direct access, the authorities may lay their hands on the data beyond the scope of the person’s consent, such unauthorized data set may be considered inadmissible evidence;

in the former case, the actions of the authorities are compulsory, the person is obliged to comply, while in the latter one, the actions of the authorities gaining access themselves or through whatever intermediary may be carried out only with the lawful and voluntary consent of the person;

the former one does not contain the requirement of the lawfulness of the person's disposal of the required data; the latter prescribes that the person must have the lawful authority to disclose the data to the authorities through the said computer system.

In light of the above-mentioned provisions of both paragraphs of article 27 of the UN Convention, the practical implementation of the special "anti-extraterritorial" norm introduced into bilateral intergovernmental agreements on cooperation in ensuring international information security since 2022, may prove

problematic. For instance, in accordance with the Agreement between the Government of the Russian Federation and the Government of the Republic of Azerbaijan on Cooperation in the Field of International Information Security of 24 June 2022 (article 2), "cross-border access to computer information stored in the information system of one of the States of the Parties, without official interaction with the relevant competent authorities of the States of the Parties, is not allowed; such interaction can be carried out, in particular, within the framework of bilateral and multilateral international treaties, including on legal assistance in criminal matters, as well as within the framework of international cooperation of law enforcement authorities."[28]

It is thus clear that this treaty prohibition is imposed against transborder access to computer information proper, without any exceptions for such access thereto by the authorities both directly or by means of any person or ICT service provider. Furthermore, this prohibition has no limitations as to the nature of the information, which may in fact be publicly available (open sources). That is why the said standard wording requires improvement.

Due to the use of foreign instant messaging apps, e-mail, cryptocurrency exchanges[29] and other foreign Internet services by the population, the evident fact should be recognized that the actions of law enforcers referred to in these norms of the UN Convention, including with regard to an unlawful data holder, as well as the mentioned example of applying the demonized article 32(b) of the Budapest Convention, are a daily, routine professional practice; therefore, limiting the location of the ICT system and data medium referred to in article 27 to the territory of the state whose authorities exercise the power to issue relevant orders would not be practicable and in keeping with the realities "on the ground".[30] On the contrary, the spatial scope of the rules on the search and seizure of data (article 28) is strictly limited to the territory of the state of the ordering authorities where the ICT system or its part or the electronic data

storage medium storing the data at stake are located, while the rules on the interception of traffic or content data (articles 29 and 30) are limited to the territory of the state where the relevant technical means are applied or where the sought communications are transmitted by means of the ICT system.

Articles 42, 44 and 45 of the Convention name as the state to be requested to preserve or produce electronic data the state in whose territory the ICT system storing the data is located, and when traffic data is intercepted – the state in whose territory communications are transmitted by means of an ICT system (while when intercepting content pursuant to article 46, the touchpoint state to be addressed whose territory is affected is not specified). These wordings *per se* in the current realities may be regarded as misleading and impracticable: the investigator who makes a request for legal assistance does not and cannot know for certain and specify in his/her request, where exactly, in which information system, country and at which moment precisely the provider stores and processes data and transmits communications the investigator is interested in.

When cloud computing and anonymizers are used, one faces problems of data localization: “loss of location” of data, including where the service providers themselves do not have the information about the data location; situations when data that form a single whole unit (information resource) get actually scattered in a fragmented and/or dynamic, migrating state over different jurisdictions, or have their numerous mirror copies in those jurisdictions. The uncontrolled outflow of domestic traffic disassociated from the national information infrastructure, including as a result of the operation of non-geostationary (low-Earth orbit) satellite communication systems and broadband Internet access such as Starlink, is another issue of relevance here.

For these reasons, in the current national practices, under the general rule, the principal addressees of requests for the preservation and submission of data are the states of "nationality" of ICT service providers or other custodians. The

procedural jurisdiction of a state over information systems, networks and data, based on the localization of the service provider/data custodian or their operations, is illustratively defined in relation to a requested state in the UNODC Model Law on Mutual Assistance in Criminal Matters: it is the state, in which the service provider having possession, control or custody of the sought data is located or established, or through storage, transmission or other data processing activities, otherwise operates from this state.[31]

At the insistence of the Russian delegation to the Ad Hoc Committee, relevant formulas to reflect the real state of affairs have been included in the Convention. In article 41 (24/7 network), the tasks of a point of contact include the provision of information about the location of the service provider, if known to the requested State Party, to assist the requesting State Party in making a request. Article 42 (International cooperation for the purpose of expedited preservation of stored electronic data) establishes that the requesting State Party may use the 24/7 network provided for in article 41 of the Convention to seek information concerning the location of the electronic data stored by means of an ICT system and, as appropriate, information about the location of the service provider. The above-mentioned provisions of these two articles also serve to facilitate the application of articles 43–46 of the Convention.[32] Besides, the requests should include, as alternative types of information: any available information identifying the custodian of the stored electronic data or the location of the ICT system (requests for data preservation); any available data identifying the owner or user of the data, or the location of the ICT system (requests for real-time collection of traffic data).

The Budapest Convention on Cybercrime names as the only criterion for determining a requested state to be addressed via international cooperation the territory of the location of the sought data (communications to be intercepted, computer systems), which does not conform with the modern cloud computing

reality, represents an insufficient and outdated approach. The 2022 Second Additional Protocol to the Budapest Convention rightly substitutes it for the location of the physical presence of the service provider in the relevant state.[33]

The exceptions are wiretapping and other kinds of real-time interception of communications or other data, which can be requested not only from the state of the service provider, but in many if not most cases, from other touchpoint states where the following persons or facilities are located:

the subscriber/user and/or the end-point device belonging to or used by him or her;

the gateway, terminal or transit equipment or network of the service provider, through which the data traffic is routed.

Language of the Convention

To ensure the consistency of equally authentic texts of the Convention in the UN's six official languages, the Ad Hoc Committee's Language Consistency Group was established, which comprised six representative language sub-groups (each consisting of representatives of different countries where the relevant language is the official language), who held regular consultations in close coordination with the Translation Sections of the UN Office at Vienna.

The Group's experts decided not to regard the texts of the Palermo and other UN Conventions as "inviolable" and not to compile special glossaries of terms modeled on that of the Palermo Convention, but instead to correct – in the new Convention – many inaccuracies and inconsistencies between the language versions identified over almost a quarter of a century of application of the Palermo Convention and the 2003 UN Convention against Corruption (Merida Convention). The Russian version of the text was carefully checked against the English (which was the "first among equals," since the Convention was drafted mainly in English) and Spanish (and afterwards with the other languages in UN

agencies) with the active participation of members of the Russian delegation – representatives of judicial and law enforcement agencies, the Ministry of Digital Development, Communications and Mass Media, and diplomats. This inter-agency format made it possible, in collaboration with the translators in Vienna, to elaborate a linguistically and legally quality text in Russian, while at the same time rectifying the deficiencies found in English and Spanish, and to ensure the equivalence of multilingual legal terms in their contemporary meaning.

The drafters, by analogy with the Budapest Convention, initially agreed to use only technologically neutral language in the treaty to ensure that the Convention be applicable indefinitely, regardless of the emergence of new technologies; it does not even contain the definition of electronic evidence and instead uses "evidence in electronic form," which can be interpreted as both broader and narrower than electronic evidence, since electronic evidence can sometimes consist of certain hard-copy information.[34]

Detection, prevention *("предупреждение")*, suppression *("пресечение")* and solving of crimes are recognized as stages of countering or combating crime. Sometimes such measures include *"профилактика"* (proactive preventive measures), while *"предупреждение"* and *“пресечение”* are incorporated in the scope of the notion *"предотвращение"* (all three of them conveyed by the single term "prevention" in English). The point was to ensure the inclusion of all these stages into the domestic and international sections of the Convention. Unlike the Ad Hoc Committee's mandate, it was decided to use the term "combating" instead of "countering". The choice of the English equivalent for the narrow Russian term of art *"пресечение"* proved somewhat challenging, since its closest English synonyms – the terms "disruption" and "frustration", which denote terminating some started and unfinished action, – while they are used in foreign laws and regulations, are not used in conventions in this narrow specific meaning.

At the same time, the term "suppression" that the latter do use, is variably conveyed, both as *"пресечение"* and as *"борьба"* ("fight") in general, and has a broader meaning of inhibiting, blocking an activity rather than strictly interrupting it, just as "deterrence" has a broader scope (blocking, avoidance). Native English speakers tend to view *"пресечение"* as a component of prevention, without distinguishing it as an independent element within the term "prevention". The initial idea, approved by many, of conveying one notion using two terms ("prevention" to mean both *"предупреждение и пресечение"*), though it is sometimes implemented (for instance, with "integrity" standing for *"честность и неподкупность"*), appeared undesirable, including in view of Chapter VI (Preventive measures) of the Convention, which in fact deals with proactive preventive measures only. Finally, the better option was chosen: to include the stage of *"пресечение"* of an offence in the scope of the notion of investigation, or rather in one of its purposes (stopping or impeding the commission of the offence) in the Interpretative notes to the Convention.

It should be taken into account that, in view of the differences in the legal systems of countries across the world (for example, convergence of preliminary (pre-trial) investigation and operational search activities, variability of the substance of the concept of "criminal case") and the universality of the language of international documents, the names of procedural (investigative, judicial) actions in foreign and international law often do not coincide with those used by Russian law, and Russian (covert) operational search measures in most cases are referred to as investigative measures, criminal (law enforcement) intelligence operations or are included within the umbrella international legal notion of special investigative techniques. Therefore, the terminology itself is relative and should not be determining when opting for a particular kind of legal or law enforcement assistance.

In Russian legal order, for the purposes of international treaties, “judicial authorities” are traditionally understood as preliminary investigation bodies, public prosecutor's offices and courts;[35] thus, "judicial documents" mean documents issued by them or otherwise emanating from them.

The following specific issues pertaining to the translation should be also noted.

The dual translation of the term "offence" as *"правонарушение"* and *"преступление"* depending on the context: the first is mainly used in the combination "criminal offence" (in many jurisdictions it is divided by gravity into “crimes” (i.e., felonies) and misdemeanors) etc. when the Convention establishes (criminalizes) the acts at issue, while the second is used in other contexts, where its meaning as a crime already established or covered by the Convention is evident. The same applies to the term "seizure": the context defines whether it is a narrow special procedural term *"выемка"* or *“арест”* that refer to separate investigation or court measures, especially those requiring a judicial decision, or a wider term *"изъятие"*, which encompasses both *“выемка”* and an inspection and any other investigative or judicial actions and operational search measures which can include seizing objects in any manner.

The term "grooming" in article 15 of the Convention has no one-word equivalent in Russian to denote the required phenomenon that could be regarded as a commonly used loanword suitable for use in legal acts at this level. The etymology of the term implies courting, wooing. The transliterated notion *"груминг"* in the Russian language is mainly used in its different meanings associated with zoology and pet grooming. Therefore, the English term is conveyed using the Russian definition that reflects the substance of the phenomenon – trust building (for the purpose of committing a sexual offence against a child).

Conclusion

Any international treaty, and first of all multilateral treaty, is to a greater or lesser extent a product of compromise. In the case of the Convention, it was a much more delicate balance and compromise taken together, which are *a priori* unable to generate something very breakthrough. Against all odds, however, a quality and practically relevant text that builds on the fusion of the best elements of the Palermo and Budapest Conventions has been produced. The allegory of a baby can be well applied to any treaty (not only to a bilateral one, more natural in this sense), and twice as much to the Convention. This long-awaited firstborn was carried in a toxic environment that had little to do with the spirit of the United Nations, and delivered in painful labour “as is”, despite the initial plans and demands of the knowingly ill-matched parents. Whichever the case, the Convention is our own child, whose healthy development and success in life is in our hands.

All of us will need to continue and improve our professional diligent work to counter cybercrime within the multipolar architecture of the modern world order, including the bloc of "unfriendly" states,[36] now that we have at our disposal a new universal instrument, whose effectiveness will depend first and foremost on our own efforts, and a new holiday to be designated to mark the adoption of the Convention – the International Anti-Cybercrime Day. What the specific achievements we are going to celebrate on that day will be – also depends on us.

Original publication:

Литвишко П. Первый глобальный договор против киберпреступности: от геополитической конфронтации к профессиональному компромиссу // Международная жизнь. – 2024. – № 11. – С. 4–27.

URL: https://interaffairs.ru/virtualread/ia_rus/112024/files/assets/downloads/publication.pdf

Author: Pyotr Litvishko, PhD, Deputy Head of the General Department of International Legal Cooperation – Head of the Department of Legal and Law Enforcement Assistance, Prosecutor General's Office of the Russian Federation, Senior Assistant to the Prosecutor General of the Russian Federation

---

[1] Currently, Vietnam's capital city is being considered as a possible venue for the opening for signature of the Convention, so that it may be traditionally named as the Hanoi Convention in the future.

[2] The author was a member of the Russian delegation to the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (2021-2024), a member of the Ad Hoc Committee's Consistency Group from the Russian Federation.
The contents of this publication reflect the author's own legal assessments and do not represent the official position of his agency.

[3] The slang term *"закладка"* ("backdoor"), which is common in the international information security environment and beyond, is not always used correctly in relation to the treaty practice of introducing undesirable provisions into a document under development ("human rights backdoors", etc.), as it does not take into account the etymology and meaning in cyber lexicon of the term "software (hardware) backdoor", from which it is derived. It implies, first of all, the covert or at least implicit nature of installation and operation of certain hidden or undeclared functionality (see the terms and definitions of GOST R 51275-2006). Where treaty provisions and their intended effect are self-evident (as in the case of human rights "backdoors"), it is wrong to speak of them as backdoor means.

[4] National legal frameworks and approaches to challenges in gathering electronic evidence across borders in light of the new global Convention provisions: Russian Federation's perspective: Side event at the Concluding session of the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes; United Nations HQ, New York, Jan. 30, 2024.
Here and hereinafter materials from the official website of the Ad Hoc Committee. URL: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home, accessed Oct. 14, 2024.

[5] CyberUA: Strengthening capacities on electronic evidence of war crimes and gross human rights violations in Ukraine. URL: https://www.coe.int/en/web/kyiv/cyberua, accessed Oct. 14, 2024; Eurojust and the war in Ukraine; Core International Crimes Evidence Database (CICED). URL: https://www.eurojust.europa.eu/eurojust-and-the-war-in-ukraine, accessed Oct. 14, 2024; S. Hill, "International Efforts to Collect Evidence Related to Russia's Aggression Against

Ukraine", *Saint Louis University Law Journal*, vol. 68, No. 2 (2024), pp. 243–255; Ch. Quilling, "The Future of Digital Evidence Authentication at the International Criminal Court", *Journal of Public & International Affairs* (2022), p. 7; А.А. Назарко, "Електронні докази в українському кримінальному судочинстві: Дослідження правових реалій та теоретичних перспектив" [Electronic evidence in Ukrainian criminal proceedings: study of legal realities and theoretical prospects], *Науковий вісник Ужгородського Національного Університету. Серія Право*, вип. 80, ч. 2 (2023), pp. 183–188; П.А. Литвишко, "Уголовно-процессуальные аспекты решения Международного Суда ООН по делу "Украина против Российской Федерации" от 31 января 2024 года" [Criminal procedural aspects of judgment of the International Court of Justice in the case "Ukraine v. Russian Federation" of 31 January 2024], *Вестник Университета прокуратуры Российской Федерации* 4(102) (2024), pp. 108–123.

[6] *The Practical Guide for Requesting Electronic Evidence across Borders* (Vienna: United Nations, 2021), p. 39.

[7] According to the sources of official interpretation of a number of universal conventions, the term "judicial proceedings" used in them, in addition to a trial, may in some countries include pretrial proceedings, while "the term "proceeding" is intended to cover all official governmental proceedings, which may include the pre-trial stage of a case." Also, the term "proceeding", depending on the context, can denote both an entire procedure of processing a criminal case, i.e. from the receipt and pre-investigative examination of a crime report through the investigation stage to the adjudication at court, and just a single procedural action.

See: *Legislative guides for the implementation of the United Nations Convention against Transnational Organized Crime and the Protocols thereto* (New York: United Nations, 2004), pp. 217 and 220, paras. 453 and 465; *Legislative guide for the implementation of the United Nations Convention against Corruption* (New York: United Nations, 2012), p. 168, para. 597; *Technical guide to the United Nations Convention against Corruption* (New York: United Nations, 2009), p. 163; *Legislative Guide to the Universal Legal Regime against Terrorism* (New York: United Nations, 2008), pp. 39–40; *Travaux Préparatoires of the negotiations for the elaboration of the United Nations Convention against Transnational Organized Crime and the Protocols thereto* (New York: United Nations, 2006), pp. 215–216; *UNODC Revised Manual on the Model Treaty on Mutual Assistance in Criminal Matters*, pp. 67–68 and 70, paras. 5–7 and 12; *Mutual Legal Assistance Manual* (Belgrade: Council of Europe Office in Belgrade, 2013), p. 75.

[8] See in more detail: Д.В. Кольцов, "Негласные оперативно-розыскные мероприятия как форма реализации специальных методов расследования в российском законодательстве" [Covert operational search measures as a form of implementation of special investigative techniques in the Russian legislation], *Труды Академии управления МВД России* 4(64) (2022), pp. 147–158.

[9] *Toolkit to Combat Trafficking in Persons* (New York: UN, 2008) (Tools 5.2–5.5), pp. 177–186; P.A. Litvishko, *The Convergence of Preliminary Investigation and Operational Search Activities in International Cooperation in Criminal Matters*, in Collection of Materials on International Cooperation of the Investigative Committee of the Russian Federation (Moscow: Prospekt, 2016), pp. 173–191.

[10] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings; Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings.

[11] Explanatory notes on the Updated draft text of the convention and the revised draft General Assembly resolution, 15 July 2024, p. 14; Statement by the delegation of the Russian Federation at the resumed final session of the UN Ad Hoc Committee (New York, July 29-August 9, 2024): Interpretation of the term "Investigation".

[12] See, e.g.: Posición del Ecuador respecto al texto aprobado, p. 1.

[13] Obtaining information on completed connections between subscribers and/or subscriber devices (art. 186[1] RF CPC), inspection and seizure of electronic messages or other communications transmitted over telecommunications networks (art. 185(7) RF CPC), monitoring and recording of conversations or other communications, as well as obtaining information on connections between subscribers and/or subscriber devices in real time (arts. 186–186[1] RF CPC).

[14] Control of communications, wiretapping, capturing information from technical communications channels and obtaining computer information (art. 6 Federal Law of 12 Aug. 1995 No. 144-FZ “On Operational Search Activities”).

[15] Draft Federal Law No. 280226-8 “On introduction of amendments to articles 453 and 456 of the Criminal Procedure Code of the Russian Federation (on the issue of the consular function of performing particular procedural actions in criminal cases pursuant to requests of competent authorities of the sending state)”, Explanatory note thereto; *Уголовный процесс России и стран Европы: сравнительно-правовое исследование: монография* [Criminal procedure of Russia and countries of Europe: comparative law study: monograph] / под общ. и науч. ред. С.П. Щербы (М.: Проспект, 2023), pp. 174–205.

[16] See also: Statement of the Delegation of the Russian Federation at the Fifth Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (Vienna, 11–21 April 2023) related to International Cooperation.

[17] See in more detail: *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.) (Moscow: Publishing House “Gorodets”, 2024), pp. 158–195.

[18] *Transborder access to data and jurisdiction: Options for further action by the T-CY: Report prepared by the Ad-hoc Subgroup on Transborder Access and Jurisdiction adopted by the 12th Plenary of the T-CY (2-3 Dec. 2014)* (T-CY (2014)16 of 3 Dec. 2014), pp. 5 and 10–11, paras. 2.2.1 and 2.4; *Criminal justice access to data in the cloud: challenges: Discussion paper prepared by the T-CY Cloud Evidence Group* (T-CY (2015)10 of 26 May 2015), p. 6, para. 2.2.
Here and hereinafter materials from the official website of the Cybercrime Convention Committee. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention, accessed Oct. 14, 2024.

[19] Explanatory Report to the Convention on Cybercrime. Budapest, 23.XI.2001, p. 21, para. 135.

[20] Statement of the Delegation of the Russian Federation at the Fifth Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of

Information and Communications Technologies for Criminal Purposes (Vienna, 11–21 April 2023) related to International Cooperation.

[21] See in more detail: *Collecting Electronic Evidence...*, pp. 81–157.

[22] Draft Federal Law No. 462337-8 "On amendments to the Criminal Code of the Russian Federation and article 151 of the Criminal Procedure Code of the Russian Federation (concerning the establishment of responsibility for unlawful performance of investigative, other procedural actions and operational search measures in the territory of the Russian Federation)", Explanatory note thereto.

[23] *T-CY Guidance Note #10: Production orders for subscriber information (Article 18 Budapest Convention) adopted by the T-CY following the 16th Plenary by written procedure (28 Feb. 2017)* (T-CY(2015)16 of 1 Mar. 2017), para. 3.1.

[24] Statement by the Russian Federation in the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes concerning the entire text of the Convention (30 July 2024).

[25] *T-CY Guidance Note # 3: Transborder access to data (Article 32) adopted by the 12th Plenary of the T-CY (2-3 Dec. 2014)* (T-CY (2013)7 E of 3 Dec. 2014), pp. 4–5 and 7–8, paras. 3, 3.6 and 3.8.

[26] *T-CY Guidance Note #10*, para. 3.1.

[27] The guidance note indicates that "[i]t should be taken into account that many Parties [to the Convention] would object – and some even consider it a criminal offence – if a person who is physically in their territory is directly approached by foreign law enforcement authorities who seek his or her cooperation".

[28] See also: Agreement between the Government of the Russian Federation and the Government of the Republic of Tajikistan on Cooperation in the Field of Ensuring International Information Security of 19 June 2023 (art. 7); Agreement between the Government of the Russian Federation and the Government of the Republic of the Union of Myanmar on Cooperation in the Field of International Information Security of 5 Dec. 2023 (art. 3).

[29] See in more detail: *Collecting Electronic Evidence*..., pp. 195–209.

[30] *Ibid.*, pp. 81–126.

[31] *Model Law on Mutual Assistance in Criminal Matters (2007), as amended with provisions on electronic evidence and the use of special investigative techniques (2022)* (UN Doc. E/CN.15/2022/CRP.6 of 11 May 2022).

[32] Explanatory notes on the Updated draft text of the convention and the revised draft General Assembly resolution, 15 July 2024, p. 16.

[33] Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, Strasbourg, 12.V.2022, paras. 99 and 128.

[34] See in more detail: *Collecting Electronic Evidence*..., pp. 58–59 and 210–221.

[35] E.g., according to the declaration of the Russian Federation on article 24 of the 1959 European Convention on Mutual Assistance in Criminal Matters as amended by article 6 of the 2001 Second Additional Protocol thereto, the courts, public prosecutor's offices, bodies of inquiry and preliminary investigation are considered as judicial authorities in the Russian Federation (Federal Law of 6 June 2019 No. 120-FZ "On ratification of the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters").

[36] П. Литвишко, “Антикриминальное взаимодействие Российской Федерации с иностранными государствами и территориями, совершающими недружественные действия в отношении Российской Федерации, её юридических и физических лиц” [Anti-crime interaction of the Russian Federation with foreign states and territories committing unfriendly actions with regard to the Russian Federation, its legal and natural persons], *Законность* 5(1075) (2024), pp. 26–35.