AJPDIS GLOBAL RESEARCH NETWORK

AMERICAN Journal of Public Diplomacy and International Studies
Volume 02, Issue 03, 2024 ISSN (E):2993-2157

International Law Standards for Obtaining of Electronic Evidence from Foreign Jurisdictions

Kharatishvili Anton Georgievich
Candidate of Legal Sciences, Associate Professor of the Department of Criminal Procedure and Criminalistics, St. Petersburg State University

Zokirov Sardorjon Karimjon ugli
Lecturer of the Criminal Procedure Law Department of the Tashkent State Law University

Abstract: The article discusses the features of the interaction of the competent criminal prosecution authorities with foreign jurisdictions and international legal standards for the execution of letter of request in order to obtain electronic evidence, as well as international initiatives and agreements aimed at combating crimes using computer networks

Key words: electronic evidence, letter of request, communication service providers, multilateral international agreements, human rights.

The life of modern homo sapiens is unthinkable without the Internet; almost half of the world's population are users of social networks. The flip side of the Internet is cybercrime, the damage from which in the global economy in 2023 reached 8 trillion U.S. dollars. More than 80% of cybercrime is committed by organized crime related to online black markets, computer viruses and the collection of personal and financial data[1]

The greatest danger to society comes from terrorists who are eager to use social media to spread propaganda, raise money, recruit supporters, and share information. Recent terrorist attacks have forced authorities to respond immediately to emergency incidents. Investigations have necessitated online data integrity and urgent requests for international cooperation.

In Resolutions 2322, 2331 (2016) and 2341, 2396 (2017)[2], the UN Security Council called for the collection and preservation of evidence to enable the investigation and prosecution of those responsible for terrorist attacks.

Thus, the development of electronic technologies and the growing number of cross-border crimes have led to the emergence of a new type of evidence that plays an important role in determining the location of the suspect, his connections and circle of contacts - electronic evidence (e-evidence, e-evidence), whose properties are characterized by instantaneous movement, and which is often located across borders[3].

A study conducted in the European Union confirmed their importance in 85% of all criminal

[1] https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/#:~:text=Our%20report%20provides%20a%20breakdown,%24154%20billion%20a%20Week.

[2] https://www.un.org/securitycouncil/ru/content/resolutions

[3] Pastukhov P. S. " Electronic evidence" in the normative system of criminal procedural evidence // Perm Legal Almanac. - 2019. - №. 2. - C. 695-707.

cases[4]. In two-thirds of investigations, however, it is necessary to make a request to a Communication Service Providers (CSP) in another jurisdiction, which confirms the increasing urgency for investigations to obtain cross-border access to e-evidence as soon as possible.

Some States may be able to assist based on principles of reciprocity or international comity or provisions of their national law. However, guaranteed recovery of electronic evidence is possible within the framework of legal grounds both established for traditional evidence and specifically focused on it. Such legal bases for Mutual Legal Assistance (MLA) are multilateral international agreements, among which regional, sub-regional and global ones are distinguished. For example, Article 18 of the UN Convention against Transnational Organized Crime (UNTOC), among other things, provides for "any other type of assistance not inconsistent with the national law of the requested State"[5].

The first international agreement aimed at combating crimes using computer networks is the Council of Europe Convention on Cybercrime of November 23, 2001 (Budapest Convention)[6], which aims to protect society from computer crimes, strengthen international cooperation in their investigation and collection of evidence in electronic form.

The Budapest Convention covers copyright infringement, computer fraud, child pornography, violation of network security, provides for a number of powers and procedures, such as search, seizure and interception of information on computer networks, as well as collection of information on traffic and content in online mode. My country, having initially signed it, subsequently refused to grant cross-border access to computer data on its territory.

The Arab League Convention on Combating Information Technology Offenses (CITO) was adopted in December 2010 and entered into force in February 2014[7]. Significant provisions include the obligation to comply with the principle of double punishability, the possibility of proactive disclosure of information to the other party, while there are no provisions for online collection of traffic or content. Provision is made for the establishment of a specialized body to provide emergency assistance in the investigation of information technology crimes.

The Agreement on Cooperation of the Member States of the Commonwealth of Independent States in Combating Computer Crime of June 1, 2001 may be used as a basis for electronic evidence by CIS countries until the date of entry into force of the Agreement on Cooperation of the Member States of the Commonwealth of Independent States in Combating Information Technology Crime, concluded on September 28, 2018.[8]

Commonwealth states have approved an alternative Plan for Mutual Assistance in Criminal Law Matters within the Commonwealth (Harare Plan Update). The parties have committed to implementing this treaty through their national legislation. At a meeting in Sydney in 2011, amendments to the Plan were adopted, including those relating to obtaining electronic evidence, online traffic, and content information.

In July 2014. The African Union approved the Convention on Digital Security and Personal Data Protection, which, however, does not provide a legal basis for international cooperation on electronic evidence, does not provide a comprehensive set of procedural powers to investigate and prosecute computer crime, and lacks provisions for obtaining electronic evidence in domestic investigations.

Other regional and subregional treaties and agreements on MLA assistance in criminal matters have been concluded under the auspices of various regional organizations and entities, including

[4] https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Documents/Events/Regional%20Initiatives/RI5%20confidence%20in%20ICT/Report%20on%20Building%20confidence%20and%20security%20in%20the%20use%20of%20ICTs%20in%20the%20CIS.pdf
[5] https://lex.uz/docs/1304112
[6] https://rm.coe.int/1680081580
[7] https://www.unodc.org/e4j/ru/terrorism/module-5/key-issues/middle-east-and-gulf-region.html
[8] https://lex.uz/docs/4748982

the Association of Southeast Asian Nations, the Cooperation Council for the Arab States of the Gulf, the Economic Community of West African States, the Council of Europe, the European Union, the Organization of American States, the South Asian Association for Regional Cooperation, and others.

Where States are not parties to regional agreements, global treaties may be invoked. In particular, the international legal framework on counter-terrorism includes 19 conventions and protocols on counter-terrorism[9], as well as relevant UN Security Council Resolutions[10]. In addition, the UN Conventions against illicit trafficking in narcotic drugs and psychotropic substances, against transnational organized crime, against corruption, etc. may also apply. Chapter VII of the UN Charter makes them binding, including on non-ratifying states.

However, obtaining relevant information under MLA is often a time- consuming task. The existing procedure for executing international letters of request (Letter of Request, ILOR or LOR) is complex and bureaucratic, often resulting in long delays in investigations. This seriously hampers law enforcement efforts to combat cross-border crime and does not take into account the fast-paced nature of cybercrime. At the same time, it must be considered that obtaining data from another State outside the MLA framework may violate both the law of the requested State, up to and including the commission of a criminal offense, and the requirements for admissibility of evidence, which may result in its inability to be used for criminal justice purposes.

UN Security Council Resolution 2322 (2016) explicitly notes the significant increase in requests for cooperation regarding the collection of evidence in the form of digital data from the Internet and emphasizes the importance of re-evaluating investigative techniques and methodologies related to electronic evidence.

In this regard, the most important tools of procedures in the area of preservation and retrieval of electronic evidence are the various guides issued, for example, by the United Nations Office on Drugs and Crime (UNODC), the most recent of which in 2018 was developed jointly with the UN Counter-Terrorism Committee Executive Directorate (CTED) and the International Association of Prosecutors (IAP) - Practical Guide on Procedures for Requesting Electronic Evidence from Other Countries.

According to the guidelines developed, it is not necessary to resort to MLA to obtain data from CSPs, there are faster ways, among which are: searching public sources; direct requests to CSPs; contacting the user with an offer to provide account data; police cooperation.

Open source searches refer to ways of obtaining electronic evidence at the national level, which involves an algorithm of actions to locate a user using publicly available online tools (such as an IP address), identify the owners of domain names, and investigate accounts on publicly available social networks. Evidence may include incriminating publications, images or videos posted by individuals.

The most important initial task for investigators in handling e-evidence is to secure it, which involves creating a snapshot of the user's account. Many CSPs allow law enforcement agencies to contact them directly regarding the preservation of electronic evidence in order to ensure the speed of this process.

However, this procedure contains several complicating features. First, the data may be located in different jurisdictions, so to make a request for safeguarding it is necessary to establish where the CSP disposes of and manages it.

Second, some CSPs store a limited amount of data for a short period of time. The account only

[9] http://www.un.org/en/counter-terrorism/legal-instruments.shtml.
[10] https://www.un.org/counterterrorism/ctitf/en/resolutions.

stores information for the moment of securing. For example, WhatsApp deletes content information as soon as it is viewed by all recipients or 30 days after it is sent.

Third, some states refuse to execute LORs when investigating minor offenses, which, for example, in the U.S. include offenses that carry a sentence of less than 12 months' imprisonment or cause less than $5,000 in damage. By the British competent authorities, a request is considered minor if the damage or criminal benefit is less than 1,000 pounds sterling. If the offense under investigation falls into this category, the CSP may also refuse the request.

Another issue to consider is the possibility that the owner of the account of interest may learn of the request from the CSP server either automatically or due to the CSP's policy of notifying the account owner. Therefore, it is recommended that you always include a non-disclosure request in the request text.

Many CSPs publicize their procedures for dealing with such requests in their law enforcement cooperation manuals, which include contact information for making requests and serving court orders, safeguarding procedures and a form to be completed by law enforcement representatives, conditions for voluntary disclosure of data, which may include, for example, requiring the consent of the user or next of kin, and procedures for preparing and submitting emergency requests[11].

Based on a direct request from law enforcement, CSPs do not disclose content

information unless the user's consent is obtained to access the device on which the relevant content information is stored, account or application by providing usernames and passwords. Thus, only voluntary disclosure of content and traffic information should be considered for direct request to CSPs.

Data preservation is different from data retention, as the former is performed on a targeted request for a particular user's data, the latter helps to determine whether the CSP can retain the data that is being preserved in anticipation of a request for electronic evidence. Data retention periods are the minimum or maximum period a CSP is legally obliged to retain data as evidence, after which it must be deleted.

For example, in the Russian Federation, telecommunication service providers (including CSPs) are obliged to store content information for 6 months, traffic and subscriber information for 1 and 3 years respectively[12]. Online services such as messengers, e-mail services and social networks that use encrypted data are obliged to provide access to encrypted messages.

Similar requirements are found in other countries. For example, in Australia, under the Telecommunications (Interception and Access) Act 2017, telecommunications companies must retain customer data for 2 years, except for content information.

In accordance with the Regulation on the Protection of Communications Secrets in the Republic of Korea, information on the dates and period of communications, the communication number of outgoing and incoming calls is retained for 12 months; Internet logs of service usage, tracking data on the location of information and communication networks, devices used by users of communications, or the Internet are retained for 3 months[13].

In the European Union, Directive 2006/24/EC of March 15, 2006 on the retention of data created or processed in connection with the provision of publicly available electronic communications services or public communications networks was invalidated by the European Court of Justice in 2014[14]. Moreover, under the General Data Protection Regulation (GDRP), European Union users have the right to know what data CSPs store, to obtain a copy of it and to ensure its deletion through appropriate recourse.

---

[11] https://iee.unn.ru/wp-content/uploads/sites/9/2017/03/Konspekt-lektsij-po-IB_2017.pdf
[12] https://www.consultant.ru/document/cons_doc_LAW_61798/a3cba9a7c2ac9aa487df2d4172734dd5139376f5/
[13]https://d-russia.ru/zakony-respubliki-koreya-o-zashhite-dannyx.html
[14] Дело C-293/12, Digital Rights Ireland Ltd против Министра связи и дело Tele2/Watson, декабрь 2016 г.

At the same time, some European countries have established the obligation of CSPs to store data. For example, in Italy, data on traffic related to terrorism or mafia is stored for 6 years, in other cases - 2 years. In Norway, data must be deleted by the CSP after 21 days. In Serbia, according to the Law on Electronic Communications, CSPs keep data for 12 months.

In 2016, the Swiss Federal Law on the Supervision of Post and Telecommunications came into force, requiring all CSPs to store 6 months of data on the type of connection, credentials and address information of the source and user, the duration of the connection, the time the email was sent or received, information from the SMTP protocol header, and the IP addresses of the sender and recipient of the email.

U.S. and Canadian law does not contain data retention requirements, so large CSPs in the U.S. and Canada typically accept preservation requests directly from law enforcement agencies and retain electronic evidence for 90 days, a retention period that can be extended for an additional 90 days.

This is not allowed in other States. This means that the requesting State must use police cooperation channels or send an urgent LOR to the competent authorities of the requested State.

If the country's legislation does not provide for a duty to preserve data, electronic evidence may be obtained in the following cases. An urgent LOR can be sent to the competent authorities of the requested State, accompanied by a judicial search and seizure warrant. If there is an ongoing investigation in the requested State on the same matter, the results of the investigation can be requested.

The LOR should consider the high standards of protected human rights in democracies, including freedom of expression, the right to privacy and others. A request may be denied if the conduct in question is protected under the law of the requested state.

For example, with respect to online propaganda, the 2012 Investigative Guide to Obtaining Electronic Evidence in the United States states, "...the United States will deny a request for assistance if it involves an individual who has used expression (written, oral, or otherwise) that falls within the protection of freedom of expression under the U.S. Constitution (hate speech is constitutionally protected even if objectionable), unless such expression falls outside the scope of permissible, protected speech)"

In addition, the violation of the right to privacy must comply with the principles of necessity and proportionality, as well as non-discrimination. The objectives of the investigation and the measures taken to prevent their disclosure are decisive in deciding whether to share such information.

Compliance with the LOR sufficient justification standards depends on the supporting facts of the case and the demonstration of a link between the criminal act and the evidence sought. Content information requires a step-by-step substantiation, i.e., first requesting subscriber and traffic information.

The information provided in the LOR must not be outdated, the facts must justify the preservation of electronic evidence where a search is required. Information older than 60 to 180 days in the context of electronic evidence will be deemed to have lost its novelty.

The justification for LORs must be based on reliable information, meaning that all evidence used in legal proceedings must originate from authentic and verifiable sources with a high degree of credibility. For example, when deciding whether to issue a search warrant, an investigating judge in the US conducts a credibility test by assessing the reliability of the sources of the information. These may include a confidential informant whose reliability has been previously established and who has first-hand knowledge of illegal matters; an informant who provides incriminating testimony about both him and the target and whose information has been partially verified; a victim; a witness; or another law enforcement officer.

There are difficulties in obtaining data from the cloud as it may be located in different states at

the same time and is in constant migration. The European Commission proposes to simplify the retrieval of electronic evidence from the cloud through a European preservation order either requiring CSPs to retain certain data or an information provision order allowing direct request of electronic evidence from CSPs.

There remains an unresolved issue related to end-to-end encryption (E2EE), which prevents third parties from decrypting data exchanged or stored on a server. For example, WhatsApp cannot transmit the content of its customers' messages in response to an LOR. This is exploited by terrorists and organized crime. The proposed tactics are limited to obtaining encryption keys by various means, including voluntary transfer or the introduction of informants.

On March 23, 2018, the Clarification of Lawful Overseas Use of Foreign Data (CLOUD) Act was enacted in the U.S. to address a number of ongoing challenges faced by law enforcement regarding electronic evidence. CLOUD requires CSPs to provide data regardless of where it is stored, including outside the US. The scope of court order authority under CLOUD is consistent with the Budapest Convention on Cybercrime. The U.S. government has the authority to enter into interstate agreements to enforce court orders to remove legal impediments.

Thus, the effectiveness of the activity of reclaiming electronic evidence from foreign jurisdictions directly depends on the development of international cooperation and knowledge of the specifics of interaction between competent authorities in the field of electronic technologies.

Literature

1. https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion- annually-in-2023/#:~:text=Our%20report%20provides%20a%20breakdown,%24154%20billion%20a%20Week.
2. https://www.un.org/securitycouncil/ru/content/resolutions
3. Pastukhov P. S. " Electronic evidence" in the normative system of criminal procedural evidence // Perm Legal Almanac. - 2019. - №. 2. - C. 695-707.
4. Zokirov S. RIGHTS REGULATION OF CRIPTOVALUTE IN EUROPEAN UNION // Eurasian Journal of Law, Finance and Applied Sciences. - 2024. - T. 4. - №. 2. - C. 133-137.
5. Zokirov S. Specifics of search and seizure in cybercrime investigations // Modern approaches to evidence in criminal proceedings. - 2023. - T. 1. - №. - C. 3-7.
6. https://www.itu.int/en/ITU-D/Regional =Presence/CIS/Documents/Events/Regional%20Initiatives/RI5%20confidence%20in%20ICT/Report%20on%20Building%20confidence%20and%20security%20in%20the%20use%20of%20ICTs%20in%20the%20CIS.pdf
7. https://lex.uz/docs/1304112
8. https://rm.coe.int/1680081580
9. https://www.unodc.org/e4j/ru/terrorism/module-5/key-issues/middle-east- and-gulf-region.html
10. https://lex.uz/docs/4748982
11. https://iee.unn.ru/wp-content/uploads/sites/9/2017/03/Konspekt-lektsij-po- IB_2017.pdf
12. https://www.consultant.ru/document/cons_doc_LAW_61798/a3cba9a7c2a c9aa487df2d4172734dd5139376f5/
13. https://d-russia.ru/zakony-respubliki-koreya-o-zashhite-dannyx.htm
14. Case C-293/12, Digital Rights Ireland Ltd v Minister for Communications and the Tele2/Watson case, December 2016