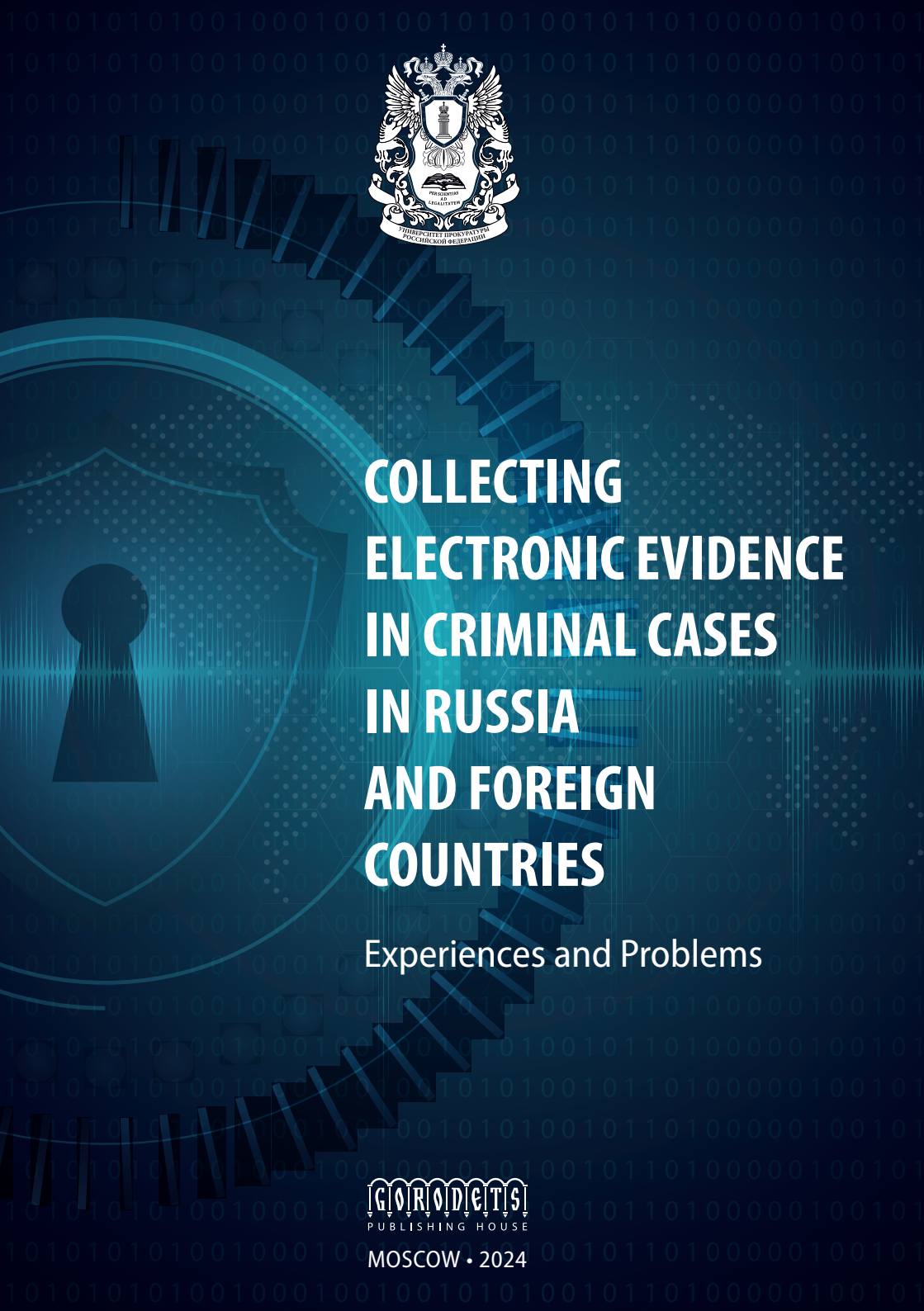


COLLECTING ELECTRONIC EVIDENCE IN CRIMINAL CASES IN RUSSIA AND FOREIGN COUNTRIES

Experiences and Problems

GORODETS
PUBLISHING HOUSE
MOSCOW • 2024

COLLECTING ELECTRONIC EVIDENCE IN CRIMINAL CASES IN RUSSIA AND FOREIGN COUNTRIES

EXPERIENCES AND PROBLEMS

GORODETS
PUBLISHING HOUSE
Moscow • 2024

UDC 343.14
BBC 67.411
C54

Editors:
S.P. Shcherba, Doctor of Law, Professor, Honored Scientist of the Russian Federation (Russian ed.), and **P.A. Litvishko**, PhD in Law (English ed.)

Reviewers:
G.V. Abshilava, Doctor of Law, Professor of the Department of Criminal Procedure, Ulyanovsk State University, President of the "House of Economics and Law. International Center for the Protection of Rights" ANO;

O.A. Zaitsev, Doctor of Law, Professor, Chief Researcher of the Center for Criminal, Criminal Procedure Legislation and Judicial Practice, Institute of Legislation and Comparative Law under the Government of the Russian Federation;

K.V. Kamchatov, PhD in Law, Head of Section of Scientific Support for Prosecutorial Supervision over Law Enforcement in Operational Search Activities and the Prosecutor's Participation in Criminal Proceedings, Scientific and Research Institute of the University of the Public Prosecutor's Office of the Russian Federation.

C54 **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. — 224 p.

ISBN 978-5-907762-35-0

The monograph explores the concepts, legal frameworks and practical aspects of electronic evidence in criminal proceedings in the Russian Federation and foreign countries; instruments and mechanisms of international legal and law enforcement assistance in criminal matters in the collection and use of electronic evidence; issues of international legal e-immunities, consular legal assistance in criminal matters, covert special investigative techniques and unilateral cross-border activities related to electronic evidence.

The book is intended for criminal investigators, public prosecutors, judges, lawyers, researchers, professors and students of educational institutions of higher legal education, as well as for all those interested in the role and problems of modern technologies in criminal procedure and criminal intelligence activities.

UDC 343.14
BBC 67.411

ISBN 978-5-907762-35-0

TABLE OF CONTENTS

Authors 5

Introduction 7

Chapter 1. **The Concept and General Characteristics of Electronic Evidence in Criminal Proceedings** (*E.A. Arkhipova, E.V. Bykova, S.P. Shcherba, P.A. Smirnov, A.D. Tsyplakova and A.G. Volevodz*) 9

§ 1. Theoretical and Legal Approaches to the Regulation of the Concept and General Characteristics of Electronic Evidence in Russian Criminal Proceedings 9

§ 2. Legal Regulation of the Concept and General Characteristics of Electronic Evidence in Criminal Proceedings of Foreign States 21

§ 3. Legal Status and Procedures for Recognition of Electronic Evidence as Evidence in Criminal Cases in the CIS Member States 44

Chapter 2. **Collection and Use of Electronic Evidence in the Framework of International Cooperation in Criminal Matters** (*P.A. Litvishko*) 58

§ 1. Legal Framework and General Rules for Collection of Electronic Evidence through International Cooperation in Criminal Matters 58

§ 2. Cross-Border Access to Information Systems, Information and Telecommunications Networks and Data for the Purpose of Gathering Electronic Evidence. International Information Security 81

§ 3. Special Investigative Techniques: Assessing the Need for Developing the Regional Frameworks 127

§ 4. Electronic International Law Immunities in Criminal Proceedings. Obtaining Evidence by Videoconference at State Foreign Missions 158

Jurisdiction of the Receiving State and the State of Transit. . . 162

Jurisdiction of the Sending State 171
Obtaining Evidence via Videoconferencing at State Foreign Missions 175
§ 5. Electronic Evidence, Provisional Measures and Confiscation relating to Virtual Assets 195
Jurisdiction 195
Provisional Measures and Confiscation 204
§ 6. Experiences and Problems of Recognition and Use of Electronic Evidence in the Context of International Cooperation in Criminal Proceedings 210

Conclusion 222

Authors

S.P. Shcherba, head of the group of authors, Doctor of Law, Professor, Honored Scientist of the Russian Federation (Introduction, Chapter 1 co-authored with E.A. Arkhipova, E.V. Bykova, P.A. Smirnov, A.D. Tsyplakova and A.G. Volevodz).

E.A. Arkhipova, PhD in Law, Senior Researcher, Section of Scientific Support for International Cooperation of the Public Prosecutor's Office and Comparative Law, Scientific and Research Institute of the University of the Public Prosecutor's Office of the Russian Federation (Chapter 1 co-authored with E.V. Bykova, S.P. Shcherba, P.A. Smirnov, A.D. Tsyplakova and A.G. Volevodz, Conclusion).

E.V. Bykova, PhD in Law, Leading Researcher, Section of Scientific Support for Prosecutorial Supervision over Law Enforcement in Operational Search Activities and the Prosecutor's Participation in Criminal Proceedings, Scientific and Research Institute of the University of the Public Prosecutor's Office of the Russian Federation (Chapter 1 co-authored with E.A. Arkhipova, S.P. Shcherba, P.A. Smirnov, A.D. Tsyplakova and A.G. Volevodz).

P.A. Litvishko, PhD in Law, Deputy Head of the General Department of International Legal Cooperation of the Prosecutor General's Office of the Russian Federation — Head of the Department of Legal and Law Enforcement Assistance, member of the delegation of the Russian Federation at the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes and member of this Ad Hoc Committee's Consistency Group, expert of the UNODC Expert Group on updating the UNODC Model Law on Mutual Assistance in Criminal Matters with provisions on electronic evidence and the use of special investigative techniques (Chapter 2).

P.A. Smirnov, PhD in Law, Associate Professor, Head of Section of Scientific Support for International Cooperation of the Public Prosecutor's Office and Comparative Law, Scientific and Research Institute of the University of the Public Prosecutor's Office of the Russian Federation (Chapter 1 co-authored with E.A. Arkhipova, E.V. Bykova, S.P. Shcherba, A.D. Tsyplakova and A.G. Volevodz).

A.D. Tsyplakova, LL.B., Lecturer, Department of Criminal Law, Criminal Procedure and Criminalistics, Moscow State Institute of International Relations of the Ministry of Foreign Affairs of the Russian Federation (MGIMO-University) (Chapter 1 co-authored with E.A. Arkhipova, E.V. Bykova, S.P. Shcherba, P.A. Smirnov and A.G. Volevodz).

A.G. Volevodz, Doctor of Law, Head of the Department of Criminal Law, Criminal Procedure and Criminalistics, Moscow State Institute of International Relations of the Ministry of Foreign Affairs of the Russian Federation (MGIMO-University), Honored Lawyer of the Russian Federation (Chapter 1 co-authored with E.A. Arkhipova, E.V. Bykova, S.P. Shcherba, P.A. Smirnov and A.D. Tsyplakova).

Introduction

Electronic information in the modern world is ubiquitous and is being formed in increasing volumes, varieties and speeds. It can be used both for the benefit of the person and society (electronic navigation, electronic medical consultations and cards, electronic banking, etc.), and for criminal purposes.

Modern technologies have become a common means of committing crimes and a reliable data medium. Its electronic traces are nowadays used by law enforcement and courts to restore and capture the picture of what happened, to establish the circumstances of a criminal case.

New technologies allow not only new types of crimes to be committed, but also have a significant impact on how to successfully solve and investigate crimes. Since crimes are increasingly committed on the Internet, the collection and procedural use of electronic evidence are crucial for effective and lawful prosecution.

Anonymity, the absence of real boundaries, fast adaptation to new conditions — these are the elements that make cyberspace an attractive environment for committing crime.

The globalization of crime causes the need to improve methods of combating it and the need for closer interaction between the competent authorities of different states, especially in the area of providing mutual legal assistance in criminal matters.

Analysis of relevant practice shows a growing need for new ways and means of collecting evidence, especially with the use of new technologies.[1]

The development of science and technology predetermined the emergence of a new species of evidence in criminal proceedings — electronic evidence (SMS messages, screenshots, electronic correspondence, flash cards, removable hard drives, etc.), which function as an effective means of establishing evidence, including within the framework of international cooperation in criminal matters. In this

[1] Н.Р. Ахметзакиров, *Сравнительное исследование осуществления правовой помощи по уголовным делам в Казахстане и России: монография* [A comparative study of the implementation of legal assistance in criminal matters in Kazakhstan and Russia: monograph] (М.: Юрлитинформ, 2016), p. 5.

regard, states must quickly adapt to the rapid development and use of technology, in particular in dealing with electronic evidence.

It is important to note that this form of evidence often does not have legal regulation in a particular legal system, since regulatory acts just follow the technological progress. At the same time, obtaining evidence in criminal cases is a central component of the provision of international legal assistance in criminal matters.

Thus, the totality of the circumstances outlined above actualizes the need for a comprehensive study of legal mechanisms of obtaining electronic evidence and the use thereof in the course of international cooperation in criminal cases, as well as the need for the development of proposals for improving the legal framework and practice of cooperation between the competent authorities of Russia and foreign states in collecting electronic evidence in criminal cases.

The present monograph:

- gives a general description of electronic evidence in criminal proceedings; discloses its concept, meaning and relevance;
- analyzes the legal regulation of the concept and general characteristics of electronic evidence in criminal proceedings of foreign countries;
- studies the international legal framework for collecting electronic evidence for it to be recognized as evidence in criminal cases, as well as interprets the experiences and problems of recognizing electronic evidence as evidence in criminal cases within the framework of international cooperation;
- examines the legal status and procedures for the recognition of electronic evidence in criminal proceedings in the CIS member states and some other countries.

Chapter 1

THE CONCEPT AND GENERAL CHARACTERISTICS OF ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS

(***E.A. Arkhipova, E.V. Bykova, S.P. Shcherba, P.A. Smirnov, A.D. Tsyplakova and A.G. Volevodz***)

§ 1. Theoretical and Legal Approaches to the Regulation of the Concept and General Characteristics of Electronic Evidence in Russian Criminal Proceedings

The collection, verification, evaluation and use of evidence in criminal proceedings are undoubtedly of great importance, since it is on the basis of the totality of evidence that the circumstances of the case are established, procedural decisions are made, and final judgments that resolve the criminal case on the merits are rendered (art. 5(33, 53.2) of the Criminal Procedure Code of the Russian Federation of 2001, with further amendments, hereinafter referred to as RF CPC).

Therefore, in criminal procedure science, proof is viewed as a cognitive activity regulated by law and carried out by authorized subjects, aimed at establishing the circumstances subject to proving through the collection, verification and evaluation of evidence.

As defined by the RF CPC, evidence in a criminal case is all information, on the ground of which a court, prosecutor, investigator or inquirer, in accordance with the procedure defined by the RF CPC, establishes the existence or the absence of the circumstances that are subject to proving in the course of the proceedings in a criminal case, as well as of other circumstances relevant to the criminal case (art. 74 RF CPC).

In the absence of a definition of the analyzed term "electronic evidence" in the Russian legislation, various approaches to the

interpretation thereof have developed in the criminal procedure doctrine. These approaches may be presented as the following generic stances.

In a narrow sense, namely from the point of view of standard definitions, "electronic evidence" can be considered as an object or document recognized as evidence, depending on the circumstances.

Electronic evidence is also considered to be "any electronically stored information that can be used as evidence in legal proceedings". This type of evidence includes any documents, emails or other files stored electronically, as well as electronic evidence, including records held by networks or Internet service providers.[1]

The term "electronic storage medium" was first introduced by Federal Law of 28 July 2012 No. 143-FZ "On Amendments to the Criminal Procedure Code of the Russian Federation" and is classified as an item that can be recognized as material evidence. Taking into account the fact that in most cases information, and not its carrier, is important for the investigation of a crime, it has become common for the preliminary investigation authorities to recognize both the media and the information contained on it as material evidence (for example, an optical disc with a video file recorded on it).

According to D.V. Ovsyannikov, computer information, received and checked in the manner prescribed by the criminal procedure law, can, too, become evidence. In a similar way, the author substantiates the term "electronic evidence".[2]

Unlike other authors who insist on the inclusion of a new article establishing the term "electronic information" in the RF CPC, the position of P.S. Pastukhov is that a new type of "electronic evidence" or a new evidentiary source of "electronic information carrier" should not be introduced, since, in his opinion, electronic information is quite capable of being perceived in the form of one of the traditional

---

[1] *Основы теории электронных доказательств*: *монография* [Fundamentals of the theory of electronic evidence: monograph] / под ред. д-ра юрид. наук С.В. Зуева (М.: Юрлитинформ, 2019), p. 253.

[2] Д.В. Овсянников, *Копирование электронной информации как средство уголовно-процессуального доказывания*: *автореф. дис. ... канд. юрид. наук* [Copying electronic information as a means of criminal procedural proof: PhD in Law dissertation abstract] (Екатеринбург, 2015).

types of evidence, namely as material evidence or a document.[1] A similar point of view is also expressed by L.V. Golovko.[2]

The term "electronic evidence" is also widely used in forensics; for example, V.B. Vekhov studied the problems of working with electronic evidence and the particularities of recording them.[3] In his opinion, electronic evidence should be understood as any information, messages (data) presented in electronic form, on the basis of which a court, prosecutor, investigator or inquirer, in accordance with the procedure established by the procedural legislation, determines the presence or absence of circumstances subject to proving during the proceedings, as well as other circumstances crucial for the correct consideration and resolution of the case.[4]

It should be noted that only a few scientists try to define "electronic evidence" not from an information technology position, but taking into account its procedural nature and significance in the field of criminal justice.

For example, D.V. Zamula defines "electronic evidence" as "information contained on an electronic medium that can be transmitted over information and telecommunication networks or processed in information systems and relevant for the consideration and resolution of a particular case".[5]

In this regard, one can agree with the position of M.P. Polyakov and A.Yu. Smolin that the phenomenon of electronic evidence is still only a concept (embryo), from which a new criminal procedural information technology is just beginning to develop, capable of

---

[1] П.С. Пастухов, *Модернизация уголовно-процессуального доказывания в условиях информационного общества: дис. ... д-ра юрид. наук* [Modernization of criminal procedural proof in the conditions of the information society: Doctor of Law dissertation] (M., 2015), pp. 16–17.

[2] Л.В. Головко, "Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция?" [Digitalization in the criminal process: local optimization or global revolution?], *Вестник экономической безопасности* 1 (2019), pp. 15–25.

[3] В.Б. Вехов, "Понятие, виды и особенности фиксации электронных доказательств" [The concept, types and particularities of recording electronic evidence], *Расследование преступлений: проблемы и пути решения* 1 (2016), pp. 155–158.

[4] В.Б. Вехов, "Электронные доказательства: проблемы теории и практики" [Electronic evidence: problems of theory and practice], *Правопорядок: История, теория, практика* 4 (2016), p. 47.

[5] Д.В. Замула, "Понятие электронных доказательств" [The concept of electronic evidence], *Вестник современных исследований* 8.4 (23) (2018), p. 187.

competing with the technology based on formal logic, enhanced by traditional writing.[1]

The emergence of an electronic form of recording, transmitting and using information dictates the need to develop new methods for detecting, recording and evaluating evidence of the commission of illegal acts, primarily related to the use of computer technology.[2]

Taking into account the fact that nowadays the legislator in certain cases equates a document on paper media to an electronic document, in criminal proceedings the latter may appear in a broad sense as "material evidence" or as "other document".[3]

In criminal procedure law, "electronic evidence" is most often referred to either as physical evidence or "other documents."[4] Some researchers point out that the delimitation of electronic media into material evidence and "other documents" should occur according to a criterion that is considered traditional for the law of evidence, namely, if information significant for the case is determined on the basis of the physical properties and qualities of an object of the material world, then such object or document must be attached to the case as material evidence; if, however, of legal significance is the meaning of the content of the object, then it must be considered as "other document."[5]

---

[1] М.П. Поляков, А.Ю. Смолин, "Концептологический анализ феномена электронных доказательств" [Conceptual analysis of the phenomenon of electronic evidence], *Юридическая наука и практика: Вестник Нижегородской Академии МВД России* 2 (46) (2019), p. 138.

[2] О.А. Зайцев, "Особенности использования электронной информации в качестве доказательств по уголовному делу: сравнительно-правовой анализ зарубежного законодательства" [Particularities of the use of electronic information as evidence in a criminal case: a comparative legal analysis of foreign legislation], *Журнал зарубежного законодательства и сравнительного правоведения* 4 (2019), p. 42.

[3] Н.А. Иванов, *Доказательства и источники сведений в уголовном процессе: проблемы теории и практики: монография* [Evidence and sources of information in the criminal process: problems of theory and practice: monograph] (M., 2015), p. 3.

[4] Р.И. Оконенко, *«Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации: дис. … канд. юрид. наук* [«Electronic evidence» and the problems of ensuring the rights of citizens to privacy in the criminal process: a comparative analysis of the legislation of the United States of America and the Russian Federation: PhD in Law dissertation] (M., 2016), p. 20.

[5] А.А. Тушев, Н.А. Назаров, "Информация как основа всех видов доказательств в уголовном процессе" [Information as the basis of all types of evidence in the criminal process], *Общество и право* 3 (2012), pp. 196–197.

The difference of data contained in computer information from other types of evidence is not limited to the indicated features: the most characteristic feature of electronic data is that it is formed not only through physical patterns, but also according to a software algorithm that is set up by the program developer. In other words, if the formation of traces of a crime on an ordinary object is subject to physical, chemical, biological and other regularities that have an objective nature and exist beyond the will and consciousness of a person, in the course of the operation of a computer program, on the contrary, changes occur according to the algorithm specified by the developer, which he chooses at his sole discretion.[1]

If one is to say that computer information ("electronic evidence") truly has certain individual features, this does not automatically make it into a separate type of evidence. Only by linking these features with the goals and rules of application of the criminal procedure law, can we talk about "electronic evidence" as an established category of criminal procedure law.

Serving as electronic physical evidence can be not only material carriers of electronic information, but also electronic information itself, resulting from a criminal act and generated in the information environment as a trace of a crime. The specificity of digital traces[2] is manifested in the fact that computer data changes instantly, and that, therefore, it can only be examined using conventional computer tools or special expert equipment and by carrying out the relevant procedures.

Depending on the method of formalization of electronic information, the category of "electronic evidence" in accordance with the provisions of the RF CPC may include "other documents" (for example, a printout of SMS correspondence, a screenshot on a piece of paper, a response to a request from a telecommunications company in relation to a specific subscriber).

Art. 84 RF CPC contains a provision regarding documents that may contain information recorded both in writing and in another form. Such documents include photo, audio and video recording materials, as well as filming and other information media that was

[1] Р.И. Оконенко, *op. cit.*, p. 25..

[2] А.М. Багмет, В.В. Бычков, С.Ю. Скобелин, Н.Н. Ильин, *Цифровые следы преступлений: монография* [Digital traces of crimes: monograph] (М.: Проспект, 2021), 168 p.

received, requested or provided in the manner prescribed by art. 86 RF CPC. When such documents possess the features specified in art. 81(1) RF CPC, they can be recognized as material evidence by virtue of art. 84(4) RF CPC.

A clear illustration of the above is the verdict of the Vakhitovsky District Court of Kazan of 6 May 2014, on the basis of which citizen B. was found guilty of committing a crime under arts. 30(3) and 234(3) of the RF Criminal Code. The court in this criminal case established that citizen B., in the course of correspondence in one of the social networks with citizen V., who was an agent of the Federal Drug Control Service, agreed on the sale of a potent substance to the latter. As a result, citizen B. sold the indicated substance to an officer of the Federal Drug Control Service, who acted as a participant of the "test purchase" operational search activity, which led to citizen B.'s detention. Recognized as evidence in the case was a protocol of examination of documents and screenshots of social network pages containing correspondence between the indicated persons discussing the conditions for the sale of a potent substance.[1]

Physical evidence in the form of electronic media (for example, a hard drive with files contained on it, etc.) is seized in accordance with art. 164[1] RF CPC in the course of investigative actions with the participation of a specialist. At the request of the legal owner of the seized electronic media or the owner of the information contained on them, the specialist participating in the investigative action, in the presence of attesting witnesses, has to copy the information from the seized electronic media. Like other types of evidence, electronic evidence is collected through investigative and other procedural actions. In this case, it is necessary to underline such procedural actions as a search, as well as seizure and inspection, which allow to detect the evidence through relevant information media, for example, a personal computer, flash card, telephone, removable disk, etc.[2] Such evidence is collected, checked and evaluated by means of carrying out the seizure and inspection of the information carrier.

---

[1] Е.С. Ермакова, Д.М. Джумангалиева, "Электронные доказательства как новое направление в практике расследования преступлений" [Electronic evidence as a new direction in the practice of investigation of crimes], Молодой ученый 23 (209) (2018), p. 86.

[2] Н.А. Зигура, *Компьютерная информация как вид доказательств в уголовном процессе России: автореф. дис ... канд. юрид. наук* [Computer

For example, on 10 June 2013, citizen T. was found guilty by Gagarinsky District Court of Moscow of committing crimes under arts. 183(1), 183(2) of the RF Criminal Code. Substantiating the guilt of that person, the court based its conclusions on the protocol of seizure, during which a printout of T.'s e-mail messages and a CD with the electronic content of these messages were seized from Mail.ru LLC, as well as on the protocol of examination of items and documents impounded during the seizure.[1]

Phonograms of the recording of conversations are recognized as material evidence. According to art. 186(8) RF CPC, the phonogram shall be attached in full to the materials of the criminal case on the ground of the investigator's resolution as material evidence and shall be kept sealed up under the conditions precluding the possibility of listening or multiplying the phonogram by outsiders, and ensuring its safety and technical fitness for repeated listening, including that at a court session.

Recognized as material evidence could also be:

an annex to the conclusion of a forensic examination (expert opinion) or to the conclusion of a specialist;

a petition, statement, complaint or appeal filed with the court in the manner and within the time limits established by the RF CPC, in the form of an electronic document signed by the person who sent such a document with an electronic signature in accordance with the legislation of the Russian Federation, by filling out a form posted on the official website of the court on the Internet. Materials attached to the petition, statement, complaint or appeal are also filed in the form of electronic documents. Electronic documents produced by other persons, bodies or organizations in a free form or in the form established for such documents by the legislation of the Russian Federation must be signed by them with an electronic signature in accordance with the requirements of the legislation of the Russian Federation (art. 474^1 RF CPC);

an annex to the protocol of an investigative or court action (including the results of the use of technical means of fixing the progress and results of an investigative action in the manner prescribed by art. 170 (1^1 and 3) RF CPC, etc.);

information as a type of evidence in criminal process of Russia: PhD in Law dissertation abstract] (Челябинск, 2010), p. 14.

[1] URL: http://gagarinsky.msk.sudrf.ru, accessed July 19, 2020.

objects and documents seized and received in the course of investigation into a crime report, in the manner prescribed by art. 146 RF CPC;

the results of operational search measures provided to the body of preliminary investigation;

video recording of a video conference, namely of testimony, statements, etc. (of the accused (art. 35(6)), witness (arts. 240(4), 278^{1}), victim (arts. 240(4), $399(2^{1})$), legal representative of the victim or representative of the victim (art. $399(2^{1})$), defendant (arts. $241(6^{1})$, 293(1)), convict (arts. $389^{12}(2)$, 399(2), $401^{13}(2)$) RF CPC, etc.);

the results of using audiovisual, electronic and other technical means of control in the exercise of control (arts. 105^{1}, 107(14) RF CPC).

The collection of electronic evidence has its own specifics. This activity has both general and special features. For example, the preparation of a protocol of the relevant investigative action related to such evidence should be carried out by an authorized subject specified in the RF CPC, however, the participation of a specialist is mandatory. Conducting a forensic examination related to the study of electronic evidence is carried out by a specialist in the relevant field, and, for instance, inspecting a website, creating and saving screenshots should be carried out by an investigator or an inquirer with the participation of an appropriate specialist and attesting witnesses.[1] In order to properly collect and then evaluate electronic evidence, special technical means are required, as well as persons with special knowledge.

Electronic evidence is easily modified and instantly destroyed. For this reason, it is of particular importance to ensure its timely and correct fixation. It is necessary to single out the following features of recording electronic evidence: (1) promptness; (2) participation of a specialist; (3) availability of special devices for its recording, storage and reproduction.[2]

The use of electronic evidence in criminal proceedings is a promising direction in the investigation of criminal cases. Modern technical methods of collecting and fixing evidence are being used

[1] Н.Р. Мухудинова, *Процессуальная деятельность защитника по собиранию и представлению доказательств в российском уголовном судопроизводстве: монография* [Procedural activity of the defence counsel in collecting and adducing evidence in Russian criminal proceedings: monograph] (Саранск, 2008), p. 27.

[2] Е.С. Ермакова, Д.М. Джумангалиева, *op. cit.*, p. 86.

more often. Some of them might include information from social networks, as well as e-mail and various instant messenger correspondence. Currently, many organizations carry out electronic document management, there are also various databases of state and non-state organizations, which may contain information important for the investigation. Electronic document management is increasingly replacing paper workflow, and some types of information currently exist in electronic form exclusively.

Since the criminal process is associated with great possibility of restricting personal rights of the suspect or accused, as well as with the specifics of conduct of many investigative and other procedural actions, the possibility of using electronic documents in this type of process is significantly narrowed.[1] In particular, it is difficult to certify a document with a digital signature or other analogues of a handwritten signature. Attesting witnesses, witnesses, victims and defence counsel, participating in the conduct of procedural actions, may not always physically carry an electronic digital signature with them to have it at hand and are generally not obliged to have it in the first place.

In addition, an electronic digital signature in criminal proceedings cannot, in our opinion, in all cases be equated with a handwritten signature, since by signing a document, the suspect, accused, victim, witness confirm the correctness of the information contained in it and their personal attitude towards it.

The mechanism for putting a handwritten signature is directly determined by the psychophysical characteristics of the human body, which is why this signature is inextricably linked with the personality of the signer. A handwritten signature allows to establish (identify) a specific person on the basis of handwriting through a forensic examination. An electronic digital signature cannot be considered as a property inherent in the personality of its owner.

The authenticity of an electronic signature only indicates that the person who signed with it knows the private key of the electronic signature. In this regard, the possibility of using an electronic signature by a third party with access thereto is not excluded.

---

[1] Т.А. Полякова, "Вопросы создания правовых условий внедрения электронного документооборота и использования электронных документов в качестве доказательств" [Issues of creating legal conditions for the introduction of electronic document circulation and the use of electronic documents as evidence], *Человек: преступление и наказание* 1 (2008), pp. 26–28.

At the same time, one should be aware of the importance of legal regulation of the criminal procedural form of digital technologies. The improper nature of such regulation entails certain legal consequences, including the recognition of evidence as inadmissible.

The RF CPC regulates a number of issues related to copying information from seized electronic media in the course of performing urgent investigative actions.

According to art. 81(4) RF CPC, electronic carriers of information seized in the course of pre-trial proceedings, but not recognized as material evidence, are to be returned to the persons from whom they were seized, subject to a reasonable period of criminal proceedings (art. 6^1 RF CPC).

In accordance with art. 82(2^1) RF CPC, if after the performance of urgent investigative actions it is impossible to return the electronic carrier of information seized during the investigative actions to its rightful owner, then the computer information on these media can be copied at the request of the legal owner to electronic media provided by him, subject to the mandatory participation of a specialist. Participation of a specialist is a condition that excludes unlawful change or loss of information during copying.

In this regard, one should agree with the conclusions that experts come to when analyzing the provisions of the RF CPC in terms of electronic media, which are as follows: Russian legislation recognizes that digital technologies modify existing social relations, are able to have a serious impact on the legal side of the activities of the participants in the criminal process, and therefore their features and possibilities should be taken into account by the procedural law.[1] At the same time, the purpose of including information technologies in the field of criminal procedure regulation is to ensure the rights of citizens (for example, the rights of legal owners of electronic carriers of information), rather than to improve the institution of proof,[2]with all the ensuing consequences.

Meanwhile, the introduction of electronic technologies will allow, to a certain extent, to balance the possibilities of defence and prosecution. Naturally, only up to a certain point, since the defence does not have the right to use coercive measures. However, the technical ability to record this or that event, as well as the activities that

[1] Р.И. Оконенко, *op. cit.*, p. 40.
[2] *Ibid.*

are happening "right here and right now", and subsequently legalize such recording in a fair trial, allows to reveal the cognitive potential of information technologies.[1] The actual inequality of the parties might be thus compensated for, and the investigative monopoly to generate evidence might be changed.

The European Court of Human Rights draws special attention to this in its judgment in the case of *Batsanina v. Russia* of 26 May 2009, which states that the principle of equality and competitiveness of the parties requires a fair balance between the parties, therefore each party must be provided with a reasonable opportunity to present one's position on the case in conditions that do not put it in a significantly less advantageous position compared to their opponent.

The evidence, including the information presented in electronic form, can acquire a legal status only after its judicial examination. A party that would have at its disposal a video recording of a certain event related to the crime would therefore have the opportunity to petition directly before an independent court, and not before their procedural opponent. Such a position is in line with the Decree of the Plenum of the Supreme Court of the Russian Federation of 26 December 2017 No. 57 "On some issues of the application of legislation governing the use of documents in electronic form in the activities of courts of general jurisdiction and arbitration courts".

In conclusion, one should consider the latest changes introduced into the RF CPC, relating to the issue at hand.

Federal Law of 27 December 2018 No. 533-FZ establishes a special legal procedure that governs the seizure of electronic media and copying information from them in the course of investigative actions (art. 164^1 RF CPC) in criminal cases related to crimes committed in the field of entrepreneurial activity, which are listed in art. $164(4^1)$ RF CPC.

The seizure of electronic media is possible only in cases when:

a court assigns a forensic expert examination in relation to electronic media;

electronic media are seized on the basis of a court decision;

---

[1] С.И. Кувычков, *Использование в доказывании по уголовным делам информации, представленной в электронном виде: дис. … канд. юрид. наук* [Use of information presented in electronic form as proof in criminal cases: PhD in Law dissertation] (Нижний Новгород, Нижегородская академия МВД России, 2016), p. 44.

electronic media contain information that the owner of the electronic media does not have the authority to store and use, or which can be used for committing new crimes, or copying which, according to a specialist's opinion, may result in its loss or change (art. 164[1](1) RF CPC).

Electronic media containing the copied information are transferred to their legal owner or the owner of the information contained on them. An entry is made in the protocol of the investigative action on the copying of information and on the transfer of electronic media containing the copied information to their legal owner or the owner of the information contained on them. The protocol shall be accompanied by electronic media containing information copied from other electronic media in the course of the investigative action.

Taking into account the developments in legal literature, it can be concluded that electronic evidence is an electronic information carrier containing information on significant circumstances in a particular criminal case and featuring: a significant amount of memory; ease of transfer and copying of information from one medium to another; possibility of remote access to the content of electronic media and information and telecommunication systems; and finally, relativity and non-obviousness of its content.[1]

In the context of the above, it is proposed to use the possibilities of collecting evidence through such investigative and other procedural actions as a search of computer hardware or computer data; seizure of computer hardware or computer data; an order to provide information about subscribers; an order to provide stored data on information flows; an order to provide stored content data; collecting real-time data on information flows; collecting real-time information about the content of the data; ensuring operational security of computer data; using the results of a remote computer-technical expert analysis; cross-border access to a computer system or data.

Attributed to the advantages of electronic evidence could be the fact that electronic evidence contains information that is accurate, complete, clear, true, objective and neutral, given that it comes from an electronic element in which there is no subjectivity when compared, for example, with statements made by witnesses that may be contradictory. At the same time, however, there are difficulties in establishing the legal value of such evidence due to the lack of a

[1] Р.И. Оконенко, *op. cit.*, p. 8.

clear data processing procedure and differences in the interpretation of laws in this regard. There are also concerns voiced about the vulnerability and ease with which electronic evidence can be manipulated, which is one of the inconveniences in identifying its authenticity.

Solving the problem of "electronic evidence" *de facto*, i.e. given the need for direct application of existing doctrinal approaches right here and right now, most scientists agree on the possibility of giving it the form of material evidence or "other documents". This solution is temporary at best. Nonetheless, the term "electronic evidence" is firmly emerging in circulation in the scientific community, regardless of the variety of approaches demonstrated.[1]

§ 2. Legal Regulation of the Concept and General Characteristics of Electronic Evidence in Criminal Proceedings of Foreign States

The use of information and telecommunication technologies in the commission of crimes complicates their detection, suppression, investigation and prevention, which necessitates the introduction of new legal, forensic and organizational forces and means in the fight against traditional types of crimes on the part of the state.

Within the framework of the United Nations, the Council of Europe and a number of other universal and regional organizations, fundamental documents have been adopted containing international legal principles and standards for the use of electronic forms of recording, transferring and using information on crimes, both planned and committed.

The 1991 Statement of principles and programme of action of the United Nations crime prevention and criminal justice programme recommends that UN member states:

- develop and apply at national level the norms and procedures for detecting and investigating the abovementioned crimes;

[1] К.В. Обидин, "Электронное доказательство: необходимый этап развития уголовного судопроизводства" [Electronic evidence: a necessary stage in the development of criminal proceedings], *Актуальные проблемы российского права*, vol. 15, No. 11(120) (2020), p. 201.

- provide law enforcement agencies with the necessary equipment and train agents in the effective investigation of transnational crimes;
- develop telecommunications equipment, network software and other related products and services in order to prevent and facilitate crime detection, investigation and prosecution.

Increased public danger of computer crimes is expressed in its intentional and organized character, in the fact that computer crimes have a high latency and, from a technical point of view, are transnational, which complicates the successful fight against them in a separate state. Additional difficulties in the fight against this criminal phenomenon are due to the rather complicated mechanism of international legal cooperation and interaction between law enforcement agencies of foreign countries in the criminal law field.

The absence of physical borders of states in information and telecommunication networks creates many procedural risks in the activities of domestic bodies of preliminary investigation, which, inter alia, include problematic issues of determining:

- applicable jurisdiction in relation to the information resource, its owner and physical place of its storage;
- places of commission of computer crimes and the jurisdiction for criminal cases of the analyzed category;
- the sequence of actions of a person conducting criminal proceedings when inspecting information resources, the access to which requires user verification (entering a username and a password or other authentication methods), including the data located in cloud storages (i.e., a "virtual" search, investigative experiment or verification of evidence on the spot using information and telecommunication networks, etc.);
- the concept of electronic evidence and generally accepted ways of recording it.

The introduction of electronic document management in the information documentation processes has already been carried out by CIS member states. The work on the creation of legislative and other acts regulating the use of electronic documents and digital signatures and endowing them with legal force, has been carried out both within member states themselves and within the Commonwealth.

In particular, at the sixteenth plenary session of the Interparliamentary Assembly of the CIS Member States, the Model Law "On

Electronic Signature" (Resolution of 9 December 2000 No. 16-10) was adopted, which within the CIS represents a set of unified rules and procedures accepted by all member states and introduced in their national legislations. Such a law provides for a legally regulated exchange of electronic documents within the CIS.

The Recommendations on legal regulation of the operation of open telecommunication networks for the prevention of their use for terrorist and other illegal purposes for the CIS member states of 29 November 2013 stipulate that a feature of modern terrorism is that terrorists widely use information and technical impact on individual elements of the information and telecommunications infrastructure of states with the aim of damaging, suppressing and destructing them.

The Agreement between the governments of the SCO member states on cooperation in the field of ensuring international information security of 16 June 2009 provides for the creation of a comprehensive mechanism for interaction between the member states, including monitoring and actively exchanging information.

Essential to fighting crime in the context of criminal prosecution is the acquisition of evidence from other countries so that it could be used in the national criminal proceedings of the requesting states, whereby the form of cooperation is largely determined by legal formalities caused by the differences between national legal systems.[1]

The Romano-Germanic (mixed) legal system is characterized by highly elaborated legal concepts and terms and, accordingly, by highly elaborated classification of means of proof. At the same time, the Anglo-Saxon legal system is characterized by the great role of judicial precedents (case law) and applied legal doctrine. Here the question of whether "electronic evidence" represents a separate type of evidence, is not essential, and legal concepts are not as important.

---

[1] А.О. Шорор, *Уголовно-правовые и криминологические проблемы международного полицейского сотрудничества: дис. … канд. юрид. наук* [Criminal law and criminological problems of international police cooperation: PhD in Law dissertation] (M., 2003), p. 4; Е.А. Архипова, В.Н. Додонов, "Проблемы международно-правового сотрудничества при выявлении, расследовании и предупреждении преступлений, совершенных с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации" [Problems of international legal cooperation in detecting, investigating and preventing crimes committed using information and telecommunication networks and in the field of computer information], *Московский журнал международного права* 2 (2020), p. 82.

In most European countries representing the Romano-Germanic legal system, the admissibility of electronic evidence in the course of preliminary investigation and court proceedings is usually regulated by the general provisions of criminal procedure law on traditional evidence.

In the criminal procedural legislation of the Federal Republic of Germany, the procedural actions aimed at obtaining evidence about the circumstances of the socially dangerous act committed, include control of telecommunications, listening and recording of statements made non-publicly, the use of technical means, etc.

The Swiss Criminal Procedure Code provides that the authorities shall use all the legally admissible evidence that is relevant in accordance with the latest scientific findings and experience and can serve to establish the truth. The Swiss law does not contain absolute restrictions on the types of evidence that may be presented in court. Therefore, authorities may use new evidence originated as a result of scientific progress, even if it is not expressly provided for in procedural law.

The Spanish Criminal Procedure Act provides for electronic evidence as the means of word, sound and image reproduction, as well as the instruments for filing or reproducing words, figures and mathematical operations carried out for accounting or other purposes that are relevant to the proceeding.

According to the Italian Criminal Code, an electronic document is understood as any computer tool that contains information with evidentiary value or any software for the processing of this information.

Pursuant to the 2007 Criminal Procedure Act of Australia evidentiary material is considered an object related to a crime, including such object in electronic form. It is worth noting that Australian legislators have also legally secured the possibility of fulfilling the requests of foreign states aimed at obtaining computer information (Mutual Assistance in Criminal Matters Act 1987).

The admissibility of digital documents as evidence is provided for by the laws of Belgium, the Netherlands, Portugal, Romania, Finland and a number of other countries.

One can state that the legislation of European countries doesn't have a concrete definition of electronic evidence in criminal cases, nor the rules for its admissibility during the investigation and trial

of a criminal case. In general, electronic documents are equated to paper documents to give them evidentiary value.

In England, a police officer investigating a crime must be able to digitally capture evidence at the crime scene (in particular, victims and witnesses' statements), take statements and upload case information using mobile devices. Subsequently, this digital information is transmitted to the Crown Prosecution Service for them to decide whether to bring charges against the suspect. The electronic evidence collected in the case, without duplicating it on paper, is further investigated in court and used by it to issue the final decision on the criminal case.

Scotland also tries to completely abandon the paper format of the criminal case and use the Digital Evidence Sharing System. The system is designed to work with various types of evidence, providing access thereto to the authorized participants of the criminal proceedings.

Police officers in England, Wales and Northern Ireland when investigating a crime rely on the Digital Evidence Handbook. This document establishes certain requirements for persons involved in the collection of electronic evidence, as well as in the identification of digital information necessary for the investigation of crimes.

Basic principles of working with digital evidence in the case, therefore, could be defined as: the immutability of the data obtained, which can later be used in court; expert knowledge of the officials who know how to handle the seized evidence, and are well aware of the consequences and content of their actions; maintaining records of all processes applied to digital evidence; ensuring the observance of the principles of working with digital evidence by the officials conducting an investigation.

In the United States, digital evidence is defined as any data stored or transmitted in digital form and that a party to a criminal proceeding can use as evidence in litigation.[1]

The US law governing electronic evidence in criminal investigations consists mainly of two sources: the Fourth Amendment to the US Constitution and statutory privacy laws codified in 18 USC §§ 2510-22, 18 USC §§ 2701-12 and 18 USC §§ 3121-27.

[1] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computer and the Internet*. 3rd ed. (Baltimore, 2011), p. 7.

In the United States, evidentiary procedures using digital evidence in a criminal case are regulated in more detail in the Searching and Obtaining Electronic Evidence Manual.[1] In accordance with this document, electronic evidence is classified into non-hearsay and hearsay.

Non-hearsay records are created by a process that does not involve a human assertion, and can be divided into two categories: (1) records created by a computer; 2) records stored in the computer memory.

Hearsay records contain assertions by people, such as: a personal letter; a memo; bookkeeping records; and records of business transactions inputted by persons, to which hearsay rules apply.

Taking into account the origin, two groups of computer evidence are distinguished as: (1) the results of human activity stored on an electronic medium (hard disk, floppy disk, compact disk, streamer) and containing information entered by the user; (2) evidence created by a computer in accordance with the embedded program and representing the result of processing certain initial data.

In India, cybercrime is defined as any illegal act using a computer, communication device or computer network in order to commit or assist in committing a crime. Any information in an electronic record, or which is presented on paper, stored, recorded or copied onto an optical or magnetic medium produced by a computer, is also considered a document if collected in accordance with the rules listed in the 1872 Indian Evidence Act, and can be used in the future in any legal proceedings without further confirmation of its authenticity and the provision of the original.

It is worth noting an innovative approach of the Government of India in the fight against cybercrime, aimed at creating an Internet portal where one can report an impending or a committed cybercrime. Information and complaints sent to this portal are considered by law enforcement agencies in the usual manner.[2]

The 2015 Criminal Procedure Code of the Socialist Republic of Vietnam (hereinafter referred to as the SRV CPC), designates "electronic data" as a source of evidence (art. 87).

---

[1] *Searching and Obtaining Electronic Evidence Manual 2009, United States Department of Justice*. URL: http://cybercrime.Gov/ssmanual/05ssma.html.

[2] https://cybercrime.gov.in/

According to art. 99 SRV CPC, electronic data is composed of signs, letters, numbers, images, sounds or similar elements created, stored and transmitted or acquired through electronic media.[1]

When considering criminal cases, electronic data is viewed as one of the sources of evidence specified in the SRV CPC, in its natural state, in which electronic data is stored on electronic devices and means, or transmitted, received by electronic devices, which signifies that when using the appropriate (compatible) software, such evidence appears in the form of signs, letters, numbers, images, sounds or similar forms that can be recognized by human consciousness.[2]

At the same time, for the proof procedure, there is a number of features attributed to electronic data, such as the following:

- electronic data does not exist separately, but is attached to at least one electronic device or medium, since it is the way it is created, stored, transmitted and received.

The digital memory of such electronic devices and means is always being changed and modified (smart cards, smart media, GPS devices, barcode readers, computers, scanners, mobile phones, cameras, copying machines, HD storage devices, USB, removable hard disks, floppy disks, CDs, etc.);

- electronic data can be edited and supplemented.

This happens after the forced generation of data. Using devices, electronic means, software, hackers can interfere with the original data in order to change or increase the electronic data of the original, which generates new electronic data containing messages other than the original electronic data messages when they were first created;

- electronic data can be deleted.

The generated electronic data may be deleted. This means that before being deleted, electronic data is manifested with the use of devices, electronic media and software into messages containing information in the form of signals, letters, numbers, images, sounds or similar elements recognizable by humans. However, once deleted,

[1] Bộ luật Tố tụng hình sự nước Cộng hòa xã hội chủ nghĩa Việt Nam, số: 101/2015/QH13 ngày 27.11.2015 [The Criminal Procedure Code of the Socialist Republic of Vietnam of 27 Nov. 2015 No. 101/2015/QH13].

[2] Фам Ньы Хан, "Электронные данные и электронные доказательства в Уголовно-процессуальном кодексе Вьетнама 2015 года" [Electronic data and electronic evidence in the Criminal Procedure Code of Vietnam of 2015], *Вопросы российской юстиции* 9 (2020), p. 1146.

despite the use of the same devices, electronic means or software, electronic data cannot be transferred;

- electronic data can be recovered.

After the electronic data is deleted, specialists can restore the original data using special software or certain electronic means, i.e. can return electronic data in to the state in which it existed;

- electronic data can be copied from the original.

Through devices, electronic means with the same attributes and software standards, electronic copies of data might appear in identical messages containing information in the form of characters, letters, numbers, images, etc.

Classifying electronic data, the legislators of Vietnam chose to divide it into the following categories:

- electronic data automatically generated by a computer, such as "cookies", "URLs", email logs, web server logs, IP addresses, account access information, website access information, etc.;
- electronic data created by criminals or victims, such as: documents, spreadsheets, images, information displayed in electronic messages, emails, chats, documents downloaded and uploaded to the Net. This data may contain false messages due to editing, deletion/distortion of all or part of the electronic information;
- electronic data created by the competent authorities, for example, data in electronic devices collected during the performance of special investigative measures, in which an investigative experiment, a crime scene, an interrogation etc. are recorded.

As one can see, the 2015 SRV CPC regulates electronic data as a source of evidence and at the same time determines the procedures for collecting, evaluating, transforming and using evidence in the process of resolving a criminal case.

SRV CPC also requires that the body conducting the proceedings, or the competent person conducting the proceedings should possess expert knowledge relating to the process of collecting, maintaining, evaluating and using different sources of evidence, as well as electronic data, so as to establish the factual circumstances of the case.[1]

The collection of evidence is one of the crucial steps in the proof process in SRV. All the competent procedural authorities have the

[1] Фам Ньы Хан, "Некоторые обновления в теории доказательств в уголовном судопроизводстве Вьетнама" [Some novelties in the theory of evidence in criminal proceedings of Vietnam], *Вопросы российской юстиции* 12 (2021), p. 444.

right to collect evidence. In accordance with art. 88 SRV CPC, the investigative body, the prosecutor's office and the court collect evidence by: summoning individuals knowledgeable about the case in order to interview them and assess their statements related to the case; carrying out examinations, conducting searches, inspecting the crime scene and performing other investigative actions; sending requests to departments, organizations and individuals for the provision of documents, objects and facts, so as to clarify the circumstances of the case. Defence counsel, in order to collect evidence, are entitled to meet with persons whom they defend, crime victims, witnesses and other individuals knowledgeable about the case to interview them and assess their statements related to the case; to request authorities and entities to provide documents, items and electronic data related to the defence. Other participants in legal proceedings, authorities and entities can adduce evidence, documents, items, electronic data, etc. Competent procedural authorities, when receiving evidence, documents, items and electronic data related to the case from individuals as stated in art. 88(2 and 3) SRV CPC, shall make written records of submission, verify and assess such as per this Code. When collecting evidence from new sources of evidence, the following must be taken into account:

- electronic media must be immediately seized, described fully and duly and sealed immediately after being seized. Sealing and uncovering of the seal are carried out in accordance with the law;
- when collecting, blocking the collection and backing up electronic data from electronic devices, computer networks, telecommunication networks or directly on the transmission line, the authorized body must draw up a certificate of data collection as an annex to the case file;
- having received a decision on the appointment of forensic examinations, all competent legal entities or organizations are responsible for performing the restoration, search, verification of electronic data, as well as for the translation of such electronic data into the forms that can be read, heard or seen.

Electronic means and electronic data must be stored as evidence in accordance with the provisions of the SRV CPC.

When evidence is presented, electronic data must be accompanied by a medium for storing electronic data or a copy thereof. Verification and evaluation of evidence is carried out in accordance with art. 108 SRV CPC:

(1) each piece of evidence must be verified and evaluated to determine its legality, authenticity and relevancy for the case. The determination of evidence acquired must be sufficient to solve criminal cases;

(2) the competent person conducting proceedings on the case, within the limits of his powers, must consider and evaluate the sufficiency, objectivity and comprehensiveness of all the collected evidence.

Evidence verification and evaluation activities are aimed at determining: the authenticity, reliability and value of the collected evidence; the ability to use certain evidence in the system of evidence to prove a criminal case; the compatibility of evidence in terms of nature, significance and scope; the direction in which the evidence is used or might be continued to be used in a criminal case.

Evaluation of evidence is a mental activity of the subjects in the conduct of criminal proceedings in accordance with the provisions of the SRV CPC, and other subjects in the course of the investigation, as well as verification of the collected evidence. Based on the assessment of evidence, conclusions are drawn on the authenticity or non-authenticity of evidence, its legality or illegality, relevance or irrelevance of evidence for the case. All collected evidence relevant to the case must be assessed separately and as a whole. Thus, the investigative body, the prosecutor's office and the court are obliged, in accordance with the established procedure, to evaluate evidence based on its analysis and generalization. Verification and evaluation of evidence are essential for the resolution of criminal cases, therefore they constitute an obligation of both the judicial authorities conducting the proceedings and the subjects of the proceedings. Evaluation of evidence plays an important role in criminal proceedings, is essential for proving the elements of the crime, the guilt of the offender and solving the criminal case. Verification and evaluation of evidence is an important basis for the use of evidence; verification and evaluation of evidence play an important role in determining the objective truth in the case; evaluation of evidence is the basis for making decisions on the merits of a criminal case.[1]

[1] Фам Ньы Хан, "Собирание, проверка и оценка доказательств в уголовном судопроизводстве Социалистической Республики Вьетнам" [Collection, verification and evaluation of evidence in criminal proceedings of the Socialist Republic of Vietnam], *Вопросы российской юстиции* 10 (2020), pp. 460–462.

The majority of Arab countries belong to the religious legal system because the Noble Qur'an and the Sunnah of the Prophet Muhammad prevail as sources of law. Nevertheless, one may consider the Arabian Peninsula as having mixed legal systems because of dualism of secular and religious law and elements of different legal systems applicable in various law's branches.

Although the first articles of the Arab laws often contain core notions, still not all acts provide a definition. For instance, the Emirati Federal Decree Law No. 34 of 2021 on combating rumors and electronic crimes (the UAE FDL No. 34-2021)[1] determines digital evidence by listing its three features. It is any electronic information that has proof weight or value. It is stored, transmitted, retrieved or obtained from computers, information networks and the like. It can be collected and analyzed using specific technical devices, software or applications.

Arabic legal doctrine categorizes digital evidence into several groups: computer-related, related to the Internet and other networks, and that related to device-to-device communication protocols.[2]

Taking into account the theory of common origin of sources or procedures (النظرية العامة للأصول أو الإجراءات), civil procedure rules may be applied as *lex specialis*.[3] It is they that govern digital evidence. Saudi Royal Decree No. M/43 introduced such an amendment in Nizam of 2013 on criminal measures (Criminal Procedure Regulation)[4] on 30 December 2021 (art. 218).

Pursuant to Saudi Evidentiary system of 2022,[5] digital evidence (دليل رقمي) refers to any data created, issued, received, stored or communicated by digital means that can be recovered or obtained

---

[1] Cabinet of Ministers of the United Arab Emirates, Federal Decree Law No. 34 of 2021 on combating rumors and electronic crimes [مرسوم بقانون اتحادي رقم 34 لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية], https://laws.uaecabinet.ae/ar/materials/law/1526?page=1.

[2] Al-Hamdani Maysoun Khalaf Hamad, "Legality of electronic evidence as evidence in a criminal case", *Journal of the College of law/Al-Nahrain University* 18(2) (2016), p. 198.

[3] Jalat Tharwat and Suleiman Abdel Al-Manijm, *Principles of criminal procedure. Criminal case* (Beirut: Arab Fund for Research and Publications,1996), p. 9.

[4] Bureau of Experts of the Council of Ministers of the Kingdom of Saudi Arabia, Nizam dated 12.06.2013 on criminal measures [نظام الإجراءات الجزائية], https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/8f1b7079-a5f0-425d-b5e0-a9a700f26b2d/1.

[5] Bureau of Experts of the Council of Ministers of the Kingdom of Saudi Arabia, Nizam on evidence dated 07.01.2022 [نظام الإثبات], https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/2716057c-c097-4bad-8e1e-ae1400c678d5/1.

in an intelligible manner. The list is not exhaustive and includes a digital record (السجل الرقمي), digital content or catalog (المحرَّر الرقمي),[1] digital signature (التوقيع الرقمي), digital correspondence, inter alia, e-mail (المراسلات الرقمية بما فيها البريد الرقمي), communication facilities (وسائل الاتصال), digital media (الوسائط الرقمية), etc. (any digital tool that allows evidence to be presented and, if necessary, verified under art. 14 of the Decision of the Saudi Minister of Justice No. 921 of 2022[2]).

Procedural manuals to the Evidentiary system of 2022[3] provide another division: publicly available digital means (any means that has been made available for general use or to dealers with a specific type of interaction) and documented digital means (any means licensed by the competent authority that has been made available to dealers).

Electronic documents are often equated with written ones.[4] For instance, pursuant to art. 425 of Emirati Federal Decree Law No. 38 of 2022 on criminal measures (the UAE Criminal Procedure Code entered into force on 1 March 2023), electronic documents have the same legal effect as official and ordinary documents according to the criminal procedure law, if they meet the requirements set forth in the Emirati Federal Decree Law No. 46 of 2021 on electronic transactions and trust services.[5] This supports the theory of common origin of procedures. It is worth mentioning the Decision of Emirati Minister of Justice No. 60 of 2019 on procedural guidelines

---

[1] Tariq Muhammad Al-Jamli, *Digital Evidence in the Field of Criminal Procedure*, https://www.startimes.com/?t=30245909.

[2] Ministry of Justice of the Kingdom of Saudi Arabia, Ministerial Decision No. 921 dated 12.10.2022 on controls over electronic evidence procedures [ضوابط إجراءات الإثبات إلكترونياً], https://laws.moj.gov.sa/legislation/ps6CWt8A6oJ1b6j+n6vr%2Fw==.

[3] Ministry of Justice of the Kingdom of Saudi Arabia, *Procedural manuals to the Evidentiary system dated 12.10.2022* [الأدلة الإجرائية لنظام الإثبات], https://laws.moj.gov.sa/legislation/8ST%2Fur3URoFaiLSA0IAGGw==#content-card-VeTqvtWGcIOGGQvMXQ.

[4] Rashid bin Hamad Al-Balushi, "Evidence in information crimes", *Journal of the Faculty of Law of Legal and Economic Studies [Alexandria University]* 1 (2008) [راشد بن حمد البلوشي. الدليل في الجريمة المعلوماتية // مجلة الحقوق للبحوث القانونية والاقتصادية. كلية الحقوق ، جامعة الأسكندرية. 2008. العدد الأول. 1-58 ص.], pp. 38–39.

[5] [المرسوم بقانون اتحادي رقم (46) لسنة 2021 بشأن المعاملات الإلكترونية وخدمات الثقة Federal Law-Decree No. 46 of 2021 on electronic transactions and trust services], Telecommunications and Digital Government Regulatory Authority, https://tdra.gov.ae/-/media/About/Legal-References/LAW/LAW-English/Electronic-Transactions-and-trust-sevices-law-AR.ashx.

for the regulation of litigation using electronic means and remote communication in civil proceedings,[1] since it allowed the use of electronic documents and electronic signatures as evidence under Emirati Federal Law No. 1 of 2006 on electronic transactions and commerce.[2]

Further, the standing of digital evidence and procedures for its admissibility as evidence in criminal cases in GCC countries[3]are explored.

In the past, it was the judge who evaluated whether the digital evidence is admissible. His conviction derived from the sources orally presented before him. The principle of free evaluation of evidence (نظام الإثبات الحر) prevails until a person's guilt is proved (نظام الاقتناع الذاتي is a system of self-conviction). For instance, in the Sultanate of Oman, the following approach is predominant: It is sufficient to adjudicate innocence only upon a reasonable doubt as to the validity of attributing a charge to the accused or upon insufficient evidence, for the basic principle is innocence, and crime is a form of deviant behavior beyond the common bounds» (judgment of the Supreme Court No. 50 of 2004 on appeal No.22/2004).

This principle is firmly rooted in the practice of the UAE Federal Supreme Court, especially when it comes to electronic crimes (cybercrimes). For instance, the court held that the criminal judge enjoys full freedom to make a decision based on the law, the Islamic Shariah and forms his conviction on the basis of oral or technical evidence or arguments. In forming his conviction, he relies on a correct picture of the facts of the case and related legal facts from

---

[1] قرار وزاري رقم 260 صادر بتاريخ 27/3/2019م في شأن الدليل الإجرائي لتنظيم التقاضي باستخدام الوسائل الإلكترونية والاتصال عن بعد في الإجراءات المدنية [Ministerial Decision No. 260 dated 27.03.2019 on procedural guidelines for the regulation of litigation using electronic means and remote communication in civil proceedings], The UAE Official E-Legislation Database, https://elaws.moj.gov.ae/UAE-MOJ_LC-Ar/00_مدنية%20اجراءات/UAE-LC-Ar_2019-03-27_00260_Karwi.html?val=AL1.

[2] The UAE Official Online Legislation Database, Federal Law No. 1 of 2006 on electronic transactions and commerce [قانون اتحادي رقم 1 لسنة 2006م في شأن المعاملات والتجارة الإلكترونية], https://elaws.moj.gov.ae/UAE-MOJ_OG/10002S_2006/01-31-2006_0442/UAE-OG_2006-01-30_00001_kait.pdf.

[3] It is مجلس التعاون لدول الخليج العربية in Arabic. It can be translated as Cooperation Council for the Arab States of the Gulf and also known as the Gulf Cooperation Council.

all the elements presented by deduction and induction (judgment No. 1468 of 25 April 2023[1]).

One achieves confidence in conclusion by two kinds of knowledge: material/tangible (حسية) and mental/rational (عقلية). The former means perception through the senses and the latter is inference or findings based on analysis or deduction about the relationship of a fact to the circumstances.[2] In doing so, the judge must not make a judgment contrary to what is known. The court evaluates the evidence in terms of sufficiency in the first place.[3] For instance, in its judgment No. 34 of 11 January 2018, the Saudi Supreme Court held that digital evidence is considered an evidentiary tool as long as it remains clear beyond any doubt. However, its enforceability as an evidentiary tool differs depending on the case and its facts.[4]

With regard to electronic evidence, it is necessary to comply with the principles of legality (شرعية or قانونية), freedom of access to evidence and the lawfulness of this access, certainty (يقينية), deliberation (مشروعية), acceptance (قبول), validity or reliability (مصداقية), repeatability (تكرار), integrity (سلامة), causation (سبب و مسبب is the cause and being the cause) and documentation (توثيق).

Although it is preferable to use well-known mechanisms for obtaining or preserving electronic data, an experienced investigator (prosecutor) may use experimental advanced techniques. Should they not violate fundamental human rights and be justified, they can be adopted. Meanwhile, the methodology must be reproducible so that another official can reconstruct the sequence of actions. The mechanism must be credible and ensure that evidence is preserved and traceable.[5]

---

[1] The UAE Official Online Legislation Database, Appeal No. 1468 of 2022 decided 25.04.2023 [الطعن رقم 1468 لسنة 2022 صادر بتاريخ 25/04/2023], https://elaws.moj.gov.ae/UAE-MOJ_CP-Ar/00_2023/00الاحكام%20الجزائية_UAE-CP-Ar_2023-04-25_01468_Taan.html.

[2] Rashid bin Hamad Al-Balushi, *op. cit.*, p. 29.

[3] Younis bin Ahmad Al-Musheikykh, "Prosecutorial discretion in a criminal case according to the Saudi criminal procedure provision", *Journal of King Saud University. Law and Political Science* 32(2) (2020), p. 248.

[4] L. Samaha, *The Characteristics of Electronic and Digital Evidence in Saudi Arabia*, https://www.tamimi.com/law-update-articles/the-characteristics-electronic-and-digital-evidences-in-saudi-arabia/.

[5] Ahmad Hamo, Ala Awaad and Wala Abdullah, *Electronic evidence: legal and technical aspects* (Palestine: Birzeit University Law Institute, 2015), p. 19; A. Geschonneck, *Computer-Forensik. Computerstraftaten erkennen, ermitteln,*

Secondly, should the judges reach a reasonable degree of certainty about a person's guilt on the basis of what computer data has been made available to them, what has imprinted in their mind and what is possibly relevant to the case, the electronic outputs have evidentiary weight and value. However, the form in which a document, record, information or data is preserved for later presentation may be different from that in which it was originally created, sent or received. The key point is to reflect the essence in court, to establish the source, the correspondent, the date and time of sending and/or receipt. In doing so, the value of the evidence is based on accurate science and the judge cannot discuss the fact itself. The judge relates the incident's context to the circumstances of the evidence obtained.[1]

During the seizure of data, in order to preserve its integrity, documentation is maintained, i.e. reports of investigative operations kept by clerks of investigators (prosecutors) or expert statements with the examination of tangible and intangible components: the device itself (of both sender and receiver), including input, RAM, arithmetic-logic, control, output and secondary storage units, as well as software, content (showing changes made to the device and recovery of deleted files, password recovery and network tracking, sent messages, bin, images, Internet activity log, notes, contacts, keychain, applications), date and time (taking into account possible changes for false traces), cables and disks connected to the device, establishing real and digital location, connected networks and servers and security system.[2]

Thirdly, since all pleadings must be examined and orally presented for free discussion, digital evidence must also be presented orally by the expert at the hearing in person to the judge, as if they were witnesses to the events themselves. Orality is one of the principles, especially at the criminal trial stage. Electronic output data cannot be presented only through the materials of the criminal

aufklären. 5. aktualisierte und erweiterte Auflage (Heidelberg: dpunkt Verlag, 2011), p. 66.

[1] Safa Hassan Nassif, "Procedural problems associated with crimes in the field of informatics", *Journal of Legal and Political* Sciences 5(2) (2016), pp. 255–290; Mahmoud Naguib Hosni, *Explanation of the law of criminal procedure*. 3-rd ed. (Cairo: Dar al-nahda al-arabiya, 1998).

[2] Usamat Ghanim Al-Abaidi, "Electronic evidence in information crimes", *Journal of King Saud University. Law and Political Science* 20(1) (2013), pp. 64 and 67.

case or the records of the preliminary investigation, they must be discussed and analyzed with a trier of fact.[1]

The primary investigative action or procedural method (وسيلة إجرائية) is taftiishun (تفتيش), which refers to search, scrutiny (examination), inspection or control.[2] The following principles are to be followed: secure, analyze, present (تأمين، تحليل، عرض).[3] This raises difficulties with the duty to disclose information or secrets of access to electronic means by private parties due to privacy. Where the accused is concerned, they enjoy the right to remain silent and cannot be compelled to disclose the keys to access electronic media systems or to print out files or data stored in those systems.

Other individuals, such as computer operators, programming experts, analysts, communications engineers and theoretical managers serve as witnesses or experts. Therefore, the law imposes an obligation on them to disclose codes, passwords, programs, or loopholes used to enter systems, and to assist in accessing, disclosing, transferring, or preserving data for investigative purposes.[4] Legal entities may also be subject to inspection or considered as a place of inspection or search.[5]

Chapter 2 of Bahraini Legislative Decree No. 60 of 2014 on information technology crimes[6] provides for orders of public prosecution and judicial rulings allowing authorities to preserve and gain access to data.

---

[1] Rashid bin Hamad Al-Balushi, *op. cit.*, pp. 26–27 and 30–32.

[2] Adnan Ibrahim Al-Hajjar and Fayez Khedr Bashir, "Digital Evidence and Cybercrime Evidence: Between Rooting and Interpretation", *Journal of Al-Istiqlal Research University* 6(1) (2021), p. 138; Harwal Nabil Hiba, *Procedural aspects of internet crimes at the collection stage: a comparative study*. 1-st ed. (Alexandria: House of University Thought, 2007), p. 223.

[3] Ahmad Hamo, Ala Awaad and Wala Abdullah, *op. cit.*, p. 21.

[4] The jurisprudence is unambiguous on the issue of waiver or abstention. Al-Mahmoud Ali Hamudatu, "Cybercrime Evidence, Intent and Evaluation in Criminal Evidence Theory Frameworks", *Journal of Security and Law* 1 (2003), pp. 46–47; Hisham Muhammad Harid Rastum, "*Information crimes: the origins of technical criminal investigation*", in Conference on the study of law, computers and the Internet in cooperation with the Emirates Center for Strategic Research and Development and the Center for Information Technology at the University: a compilation (Al Ain: UAE University, College of Shariah and Law, 2004), pp. 77–88.

[5] *Ibid.*, p. 55.

[6] General Directorate of Anti-Corruption and Economic and Electronic Security of the Kingdom of Bahrain, Law No. 60 dated 30.09.2014 on information technology crimes [قانون رقم 60 لسنة 2014 بشأن جرائم تقنية المعلومات], https://www.acees.gov.bh/cybercrime/anti-cyber-crime-law-in-the-kingdom-of-bahrain/.

Bahraini Public Prosecution may order any person to maintain expeditiously the integrity of certain IT data, including traffic/route data stored within the IT system in its possession or under its control, whenever it deems that such data may be considered as evidence and likely to be lost or altered. The person must preserve the data and its integrity for a period not exceeding 90 days, and the Grand Criminal Court may authorize the Public Prosecution, upon request accompanied by reasons submitted three days before the expiration of the said period, to extend the period not exceeding a total of another 90 days. The Public Prosecution may also order to maintain the confidentiality of the order. Under the Public Prosecution order, a person possessing or having under his/her control certain data shall promptly transmit it, including data stored in the IT system or any other IT means. Under the Public Prosecution order, any service provider shall transmit any information in its possession or under its control about any subscriber or user, whether such information is in the form of IT data or in any other form, excluding traffic/route data and content.

The Public Prosecution may issue an entry order (أمرا مسببا بالدخول) to inspect the crime-related IT system or any element thereof, and any IT data stored therein, any of the IT devices on which the crime-related data is likely to be stored. If the Public Prosecution has reasonable grounds to believe that crime-related data is stored on another IT system or part thereof, and such data can be accessed through the former IT system or legitimately available via it, the authorities may issue an order to extend access and verify or inspect the latter system. During the verification or inspection, the prosecutors have the authority to seize and preserve IT data, inter alia, performing the following actions:

(1) control and retention of the IT system, or any part thereof, or any of the IT storage media;

(2) reproducing the IT data and retaining a copy;

(3) maintaining the integrity of the IT data;

(4) uploading IT data from an IT system that has been accessed or that was made inaccessible.

At the Public Prosecution request and after review of the documents, the court may issue an injunction to:

(1) promptly preserve offence-related traffic data, regardless of whether the transmission was broadcast through one or more service providers;

(2) disclose sufficient traffic/routing data to enable the authorities to identify the service provider and the route by which the data was transmitted, if this facilitates the discovery of the truth (art. 14).

Implementation of art. 14(2) of Bahraini Legislative Decree No. 60 of 2014 on information technology crimes is supported by Public Prosecution's powers and corresponding duties of third parties. It may assign any competent person to collect and record traffic/route and/or content data, indicating the specific messages sent by the IT system when such messages occur. It may order any service provider to perform the mentioned work or to provide the necessary assistance to those entrusted by the authorities with these tasks. It may instruct any competent person to block the data of the content of any IT device or any part thereof by which the interruption was committed. The order shall be valid for a period not exceeding 30 days, renewable for one or more similar periods.

Moreover, at the request of the Public Prosecution and after reviewing the documents, the judge may issue injunction as to any person competent or familiar with how the IT system works and the measures applied to protect the data stored in that system, to provide to a reasonable extent the information necessary to carry out the procedures stipulated in arts. 15–16 of Bahraini Legislative Decree No. 60 of 2014 on information technology crimes.

Emirati legislation provides a narrower range of law enforcement actions. Pursuant to art. 62 of the UAE FDL No. 34-2021, during the investigation of acts against state security, the competent authorities may, on their own initiative or at the request of the Attorney General, issue an order to correct, amend, delete, close and prohibit access (block) to the publication, republishing or dissemination of illegal content or content containing false data. Acts against state security include the following:

- crimes under the UAE FDL No. 34-2021 committed for or on behalf of a foreign state, terrorist group, gang, organization or illegal body;
- penetrating or damaging the information systems of government agencies (GAs), damaging the information systems of a publicly important facility, tampering with emails, electronic websites and accounts of GAs, illegal interception and disclosure of communication, information or data of GAs;

- collection and processing of confidential data and information in violation of the law, publication of data or information that does not comply with media content standards;
- calling for and advocating violations of the Constitution and laws, inciting non-compliance with the law, endorsing and advocating terrorism, disseminating information that is detrimental to the interests of the state;
- incitement to harm state security and attacking criminal justice officials, promoting sedition and harming national unity;
- desecration and damage to the state reputation and state symbols, and insulting a foreign state;
- calling for and advocating demonstrations without authorization;
- conducting statistical studies or surveys without a license with the intent to influence or damage the state interests;
- spreading rumors and false news, providing illegal content and refusing to remove it, as well as receiving a gift to perform the above-mentioned activities.

Within 3 working days from the notification date, a complaint against it may be filed. Within a week after receipt, the competent authority must make a decision. Failure to respond after the deadline is considered a rejection. This judgement may be appealed to the federal court located in the capital of the Federation, with the submission of evidence and documents within one week from the ruling date. The court considers the appeal in a deliberative chamber and decides on it within seven days. It may set aside the orders in whole or in part or dismiss the appeal after considering the defendants' motions. The judgment is final. Evidence may be obtained during search, technical expertise, monitoring of negotiations or correspondence, seizure of electronic correspondence and electronic monitoring of networks.

The issue arises as to whether a digital footprint (البصمة الرقمية) can be used as evidence. For instance, the record of website visits, logs and operational status tables with access to intermediate, main or service computer addresses may be captured either through data from service providers or established by an expert. At the same time, there are cases where the court limited itself to the report of a technical expert as an evidentiary basis of a person's guilt (e.g., judgment of the Court of Cassation of the Emirate of Dubai of 2

August 2019 on Appeal No. 13/2010 and the practice of the Court of Cassation of Cairo in 2014–2020).[1]

Arab countries seek and provide mutual legal assistance in criminal matters (MLA) under arts. 32 and 34 of the Arab Convention on Combating Information Technology Offences (Cairo, 2010),[2] taking into account the procedural rules of the requesting and requested States in the absence of a bilateral treaty. The requested State may not refuse a request merely on the grounds that the act is a financial offence or that the dual criminality is not met due to legal and technical differences in national criminal law. However, the execution of a request may be refused if it concerns a political offence or if it could harm the sovereignty, security, public order or interests of the requested State. The Arab Convention also regulates the operational preservation of data stored in information systems, prompt disclosure or collection of tracking information of protected users, and granting of access to information stored in IT systems. A State Party to the Arab Convention may, without authorization from another State Party, access information available to the public (from an open source), regardless of the geographical location of the information, as well as, through information technology in its territory, access or receive information found in another State Party, provided that the voluntary and legally valid consent of the person legally authorized to disclose the information is obtained.

The latter is regulated by specific policies or laws. For instance, on 5 May 2020, the Saudi Authority for Data and Artificial Intelligence issued the National Data Governance Policy[3] covering personal data protection, classification of information,[4] exchange and provision of open or public (عام) data, disclosure of restricted information and

---

[1] A.A. Kandel, "Cybercrime: a comparative study", *International journal of academic research* 9(1) (2020), p. 94; Mahmood Sobhi Muhammad Mahmood Zaid, "Authoritativeness of electronic evidence in a criminal case and discretionary power of a judge", *Behna Journal of Human Sciences* 1(2) (2022), pp. 43–44.

[2] League of Arab States, Arab Convention on Combating Information Technology Offences [الاتفاقية العربية لمكافحة جرائم تقنية المعلومات], http://www.lasportal.org/ar/legalnetwork/Documents/التصديق%20على%20الاتفاقية%20العربية%20لمكافحة%20جرائم%20تقنية%20المعلومات20.pdf.

[3] Saudi Authority for Data and Artificial Intelligence, National Data Governance Policy [سياسات حوكمة البيانات الوطنية], https://sdaia.gov.sa/en/SDAIA/about/Documents/Policies005.pdf.

[4] The classification levels are sirriyun lil-gaayati or top secret/confidential/specially secret (سري للغاية), sirriyun or secret (سري) and muqayyatun or restricted (مقيد).

transfer of data outside the Kingdom. However, neither Data Sharing Policy (سياسة مشاركة البيانات), nor Freedom of Information Policy (سياسة حرية المعلومات) are applicable to MLA requests (متطلبات قضائية) or for purposes of inquires (تحريات) or investigations (تحقيقات). Moreover, e.g., Legislative Decree of the Omani Sultane No. 118 of 2011 (amended by Decree No. 52-2022) on the classification of state documents and regulation of protected places[1] does not contain provisions on data sharing either.

To sum up, one may conclude that admissibility of digital evidence has been the judge's discretion for a long time. The investigator (prosecutor) must secure the information and present it in court for discussion. Depending on the medium and form in which the data is stored and presented, the nature of the evidence differs. Digital evidence can be considered both primary and circumstantial, and a judgment can be based solely on it. Secondly, there are a number of procedural obstacles to access the carrier or the data: the right to privacy, the transnational nature of the act or the lack of data exchange regulation. Thirdly, Saudi Arabia is more advanced in terms of the definition and classification of digital evidence; powers of competent authorities and general principles are more elaborated in the UAE and the Kingdom of Bahrain, although each state addresses these issues in different acts.

Thus, the evidentiary value of electronic data is determined by how electronic data is created, stored or transmitted.

The globalization of crime makes it necessary to improve the methods of combating it, including in the field of mutual legal assistance in criminal matters. An analysis of relevant practice shows an increasing need for new methods of obtaining evidence, especially with the use of new technologies.

Information presented in electronic form is replacing paper documents everywhere and has a lot of advantages in terms of visibility, transmission speed, storage capacity for huge amounts of data, information protection and fast search technologies. Such information, obtained using electronic devices and networks, located in files of various data presentation formats, such as a text document, database, spreadsheet, photo, video and sound information, vari-

[1] E-Database Qanoon, Decree No. 118 dated 26.10.2011 (amended by Decree No. 52-2022) Law on the Classification of State Documents and Regulation of Protected Places [قانون تصنيف وثائق الدولة وتنظيم الأماكن المحمية], https://qanoon.om/p/2011/l2011118/.

ous service log files, programs and utilities that store the browsing history, can be used in proving criminal cases.[1]

For evidence containing electronic data, the introduction of new legal standards of "good quality" (authenticity) is especially relevant. The emphasis is shifted from the formal (investigative) requirements for admissibility to technical guarantees for verifying the authenticity of information submitted to the court. If the technical capabilities make it possible to confirm the authenticity of information presented in electronic form, then it can be considered of probative value — that is used as a means of proving a legally significant fact. The important thing is that it shall be reliable and relevant to the facts being proved, i.e. it shall be "evidence material", that is, convincing and useful for establishing factual circumstances essential to the case.

Researchers have highlighted the undeniable advantages of using electronic evidence in criminal proceedings, which are as follows:

Reducing the time limits of criminal proceedings by reducing the terms for sending petitions, transferring case materials to the court for the application of a measure of restraint, and for giving permission to conduct investigative actions that are carried out only pursuant to a court order, transfer of materials to the head of an investigative body, the prosecutor, the court to consider complaints, carry out inspections, etc. The terms for familiarizing the trial participants with the materials of the criminal case are also reduced, since this can be done at any time (and not just working hours), anywhere and simultaneously by all such participants.

Improving access to the materials of the criminal case for all participants of the criminal proceedings, creating additional opportunities for their interaction. In electronic form, petitions and challenges can be both submitted and resolved, an expert and a specialist can also send their conclusions remotely, in some cases a decision on the appointment of an expert examination may also be sent to the forensic expert electronically.

Creating additional opportunities to ensure the right of the suspect, the accused, the defendant to defence. For example, a defence counsel is empowered to send documents to be attached to the criminal case file as evidence directly to the investigator, the inquirer or the court, as well as can get acquainted with the ma-

[1] С.И. Кувычков, *op. cit.*, p. 6.

terials of the case and submit complaints electronically, etc. This will reduce the working hours of the defence counsel, his expenses and, ultimately, has a positive impact on the availability of qualified legal aid for the suspect and the accused. The same applies to the representatives of the victim, civil plaintiff, civil defendant and private prosecutor.

Creating additional guarantee of the right of participants in the legal proceedings of access to justice, which ultimately affects the degree of real security of the rights and freedoms of each participant in the criminal process.

Increasing the requirements for the quality of the work of the inquirer, the investigator, the court, the quality of the preparation of procedural documents, performance of investigative and other procedural actions, increasing the responsibility of officials authorized to carry out the proceedings, and the quality of criminal process in general.

Facilitating the verification of criminal case materials by the head of an investigative body, prosecutor or court and simplifying control over proceedings in the case as a whole (materials for verification are placed in the appropriate section, to which the relevant participants in the process get access). This will help lighten and reduce the process by which a court authorizes certain procedural actions (search, seizure, control and recording of conversations, etc.).

Reduction of expenses in the course of criminal proceedings (postage charges, expenses on making copies of materials of the criminal case, expenses on legal aid, some other procedural expenses).

Organizational simplification of the process of reviewing court decisions by higher courts (in terms of access to procedural documents and materials subject to verification).

Systematization and structuring of the materials of the criminal case, necessary in the work of an inquirer, investigator, prosecutor and court.

The possibility of automated maintenance of statistics on criminal cases.

A significant reduction in the risk of falsifications and corrections in the materials of a criminal case (primarily in relation to investigative and other procedural actions, the materials of which have already been uploaded to the electronic portal).

Increasing the transparency of justice in criminal cases.[1]

The international community is faced with the challenge of finding a reasonable compromise between privacy and public interest in the investigation of crimes using electronic information as evidence in criminal cases. The national criminal procedural legislation should enshrine the basic legal guarantees developed and enshrined in international documents that meet the requirement of fair justice.

§ 3. Legal Status and Procedures for Recognition of Electronic Evidence as Evidence in Criminal Cases in the CIS Member States

As was noted, the legal status and procedures for recognition of electronic documents as evidence in criminal proceedings depend on the state's belonging to a particular legal system.

Criminal procedural legislation of the CIS member states, based on the continental system of law, is characterized by a high degree of elaboration of legal concepts, terms and, accordingly, of classification of means of proof.

In addition, the normative provisions of the Codes of Criminal Procedure of the CIS member states on evidence and proof in criminal proceedings are based on the Model Code of Criminal Procedure for the member states of the Commonwealth of Independent States, as well as on similar criminal procedure law scientific doctrines.[2]

---

[1] О.В. Качалова, Ю.А. Цветков, *Электронное уголовное дело — инструмент модернизации уголовного судопроизводства* [Electronic criminal case as an instrument of modernizing criminal proceedings]. URL: http://www.iuaj.net/node/1761.

[2] С.П. Щерба, И.В. Чащина, *Использование электронных доказательств в уголовном процессе государств — участников СНГ: сборник научных трудов* [The use of electronic evidence in the criminal process of the CIS member states: collection of scholarly works], in Проблемы укрепления законности и правопорядка: наука, практика, тенденции. Выпуск 13 (Минск, 2020), pp. 294–301; Е.А. Архипова, *"Правовой статус и процедура признания электронных документов в качестве доказательств в уголовном процессе иностранных государств"* [The legal status and procedure for recognizing electronic documents as evidence in the criminal process of foreign states], in Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев (Екатеринбург: Уральский государственный юридический университет, 2021), pp. 389–400.

In particular, in the Model Code of Criminal Procedure, in relation to the subject of this work, the following definition of evidence is given. In accordance with art. 142 of the Model Code of Criminal Procedure, evidence is any communications lawfully received by the court or a party, as well as documents and other items, the use of which is lawful for the establishment of circumstances that are relevant to the proceedings in the case.

The CIS member states have developed a common understanding of evidence in terms of its content, despite the differences in the established definitions (CPCs of the CIS member states define any information or factual data as evidence).

Electronic information is not singled out as a stand-alone source of evidence and, as a rule, is referred to as "other documents". Electronic media is not defined as a separate type of evidence and is considered material evidence.

1. Depending on the method of formalization of electronic information, other documents may too be classified as electronic evidence in accordance with the provisions of the RF CPC, since its art. 84 provides that documents may contain information recorded both in writing and in another form. The law includes into them photo, audio and video recording materials, as well as filming and other types of information that is received, requested or provided in the manner prescribed by art. 86 RF CPC. When these documents possess the features specified in art. 81(1) RF CPC, they can be recognized as material evidence by virtue of art. 84(4) RF CPC.

2. In accordance with the provisions of art. 135 of the Criminal Procedure Code of the Republic of Azerbaijan of 2000 (hereinafter referred to as CPC of Azerbaijan), electronic information is classified as documents. Documents, in turn, are recognized as paper, electronic and other materials bearing information which may be of importance to the prosecution, in the form of letters, numbers, graphics or other signs (art. 135 CPC of Azerbaijan). The legal owner of the document has the right to make a copy of it (art. 136 CPC of Azerbaijan).

The course and results of procedural actions in a criminal case are reflected on electronic media (art. 51 CPC of Azerbaijan).

Photographs, films and other media obtained in the course of investigative actions are attached to the protocol (arts. 237, 241,

247, 252 and 258 CPC of Azerbaijan) and are considered an integral part of it.

During the court session, the use of photo, audio, film, video, computer and other technical devices is allowed only with the consent of the presiding judge (art. 310 CPC of Azerbaijan).

Thus, the criminal procedural legislation of the Republic of Azerbaijan defines electronic information as an electronic document. An electronic information carrier does not constitute a separate type of evidence. However, the CPC of Azerbaijan does not outline special rules governing the storage and evaluation of electronic information.

3. The Criminal Procedure Code of the Republic of Armenia of 2021 (hereinafter referred to as CPC of Armenia) introduced a special article providing for mandatory recording of the process and results of all procedural actions performed within the framework of criminal proceedings (art. 8 CPC of Armenia). Procedural actions are recorded in a protocol, which is drawn up electronically.

At the same time, if it is impossible to record the process and results of a particular procedural action electronically, then it shall be done on paper — on a computer, and if this is not possible either, then by a protocol drawn up in handwritten form. If a video recording was made during the procedural action, then the carrier with such a recording is attached to the protocol.

The form and content of electronic documents (procedural acts, protocols, instructions, objections, motions, recusals, complaints, etc.) are subject to the requirements established by the CPC of Armenia for paper documents *mutatis mutandis*.

The materials of criminal proceedings recorded electronically are stored in an electronic system (electronic criminal proceedings or electronic criminal case), and documents prepared with the use of a computer or handwritten shall also be stored in a paper version.

Documents prepared with the use of a computer or handwritten, as well as the content of electronic media, are uploaded into the electronic system. Items and other materials are stored as an integral part of the electronic proceedings materials, and their photographs are uploaded to the electronic system. A list of these items and materials is also uploaded on to the electronic system.

The rules for the operation and security of such electronic system are established by the Government of the Republic of Armenia separately.

Nonetheless, the CPC of Armenia directly provides for the written submission of a complaint, objection and instruction both on paper with a handwritten signature and on electronic media with an electronic signature (art. 6 CPC of Armenia).

In addition, non-procedural documents, such as a record in the form of words, numbers, drawings or other symbols containing data on facts relevant to the criminal proceedings that were formed outside the framework of the criminal proceedings, can be made on paper, on a magnetic, electronic or other medium. Such documents, in accordance with art. 96 CPC of Armenia are attached to the materials of criminal proceedings.

In accordance with art. 200 CPC of Armenia, upon a written application of a person getting familiarized with the materials of the case, he/she shall be given an electronic version of the case file materials.

The CPC of Armenia introduced a new search format, a digital one, which consists in searching for digital data contained in electronic devices or on media. In the course of a digital search, data relevant to the proceedings are seized by copying them to another medium, ensuring the integrity thereof and copies made of them.

Analyzing the legal regulation of the use of electronic information and electronic media in the criminal proceedings of the Republic of Armenia, the following features can be distinguished: (1) electronic medium is a type of evidence; (2) the legal status of an electronic protocol is defined; (3) a special procedure for collecting electronic media is laid down.

4. The Criminal Procedure Code of the Republic of Belarus of 1999 (hereinafter referred to as CPC of Belarus) clearly distinguishes evidence (factual data) from sources of evidence. The CPC of Belarus singles out relevance, admissibility, credibility and sufficiency as criteria for evaluating sources of evidence, noting in art. 105(3) that admissibility extends precisely to the sources of evidence. Evidence is defined by the legislator as "any factual data obtained in the manner prescribed by law" (art. 88(1) CPC of Belarus).

Sources of evidence (art. 88(2) CPC of Belarus) include testimony of a suspect, accused, victim, witness or an expert opinion, documents and other media obtained in the manner prescribed by the CPC of Belarus. The law does not contain a definition of proof, but only sets out the elements of the process of proving a case, defining its goals.

So, art. 102(1) CPC of Belarus notes that the proving process consists in the collection, verification and evaluation of evidence in order to establish circumstances that are relevant for lawful, well-founded and fair resolution of a criminal case.

In accordance with art. 103 CPC of Belarus, the collection of evidence is carried out by conducting investigative actions, presenting objects and documents that are relevant for the case, as well as by performing examinations by the relevant bodies and officials at the order of the criminal prosecution body or the court.

In addition, arts. 224^1 (conduct of an interrogation, confrontation, presentation for identification using videoconferencing systems) and 343^1 (conduct of an interrogation and identification using videoconferencing systems) CPC of Belarus provide for the possibility of remote collection of data at the stage of preliminary investigation and during the court investigation by using videoconferencing systems.

In relation to keeping records of investigative actions, serving as auxiliary evidence are photo, film and video recording, drawing up plans, diagrams, tables, etc., making casts from traces left on material objects.

Based on the foregoing, one can conclude that electronic information and electronic information carriers are not determined as a separate source of evidence, therefore there is no special procedure for collecting, storing, presenting and evaluating such information.[1]

On the other hand, of interest is the CPC of Belarus framework for the possibility of obtaining evidentiary information by conducting confrontations and identifications through videoconferencing.

[1] М.С. Сергеев, *Правовое регулирование применения электронной информации и электронных носителей информации в уголовном судопроизводстве: отечественный и зарубежный опыт: дис. ... канд. юрид. наук* [Legal regulation of the use of electronic information and electronic information carriers in criminal proceedings: domestic and foreign experiences: PhD in Law dissertation] (Екатеринбург, 2018), p. 72.

5. Chapter 15 of the Criminal Procedure Code of the Republic of Kazakhstan of 2014 (hereinafter referred to as CPC of Kazakhstan) establishes the following types of evidence: testimony of a suspect, victim or witness; conclusion and testimony of an expert; conclusion and testimony of a specialist; material evidence; protocols of procedural actions; as well as documents. The Code does not contain a definition of a document; however, in accordance with art. 120 CPC of Kazakhstan, documents that can be presented as a source of evidence include information recorded in writing or in any other way (computer information, photography and filming, video and sound recording).

In accordance with art. 123 CPC of Kazakhstan, factual data can be used as evidence only after they are recorded in protocols of procedural actions. Photographing, sound recording, filming and video recording may be used to secure evidence, among other things. The resulting photographs, video recordings, phonograms and films are attached to the protocol.

Art. 126 CPC of Kazakhstan regulates the use of scientific and technical means in the process of proving. Based on this rule, for example, serving as evidence can be a video recording from a car video registrator or from CCTV cameras.

The CPC of Kazakhstan also provides for the institution of deposition of testimony and the possibility of remote interrogation.

According to art. 217 CPC of Kazakhstan, participants in proceedings have the right to file a request for an interrogation by an investigating judge, if there are grounds to believe that a later interrogation might turn out to be impossible.

The official conducting the pre-trial investigation shall have the right to send an application to the public prosecutor for filing a request for deposition of testimony with an investigating judge. In addition, art. 213 CPC of Kazakhstan provides for remote interrogation of a victim or witness, which can be carried out using scientific and technical means in the video conference mode.[1]

---

[1] С.П. Щерба, Е.А. Архипова, *Применение видеоконференцсвязи в уголовном судопроизводстве России и зарубежных стран: опыт, проблемы, перспективы: монография* [The use of videoconferencing in criminal proceedings in Russia and foreign countries: experiences, problems, prospects: monograph] / под общ и науч. ред. профессора С.П. Щербы (М.: Юрлитинформ, 2016), pp. 87–88.

The CPC of Kazakhstan does not regulate in detail the concept of electronic proceedings in a criminal case, it only touches upon the possibility of its existence and specifies a list of procedural documents and types of evidence, which may have an electronic format. At the same time, the legislator has granted the Prosecutor General of the Republic of Kazakhstan the authority to adopt legal acts, binding on all criminal prosecution bodies, related to the conduct of criminal proceedings in electronic format (art. 58(6) CPC of Kazakhstan). The Instruction on Conducting Criminal Proceedings in Electronic Format (hereinafter referred to as the Instruction) was approved by the Prosecutor General of the Republic of Kazakhstan on 3 January 2018.

Based on the Instruction, the information system "Unified Register of Pre-Trial Investigations" has been introduced for the purposes of electronic proceedings in the Republic of Kazakhstan. This information system has additional functionality, a module called "Electronic Criminal Case" (module e-CC), designed to organize the preparation, maintenance, sending, receiving and storing electronic criminal cases. The Register also features "SMS-notification" functionality, which allows sending text messages to participants in criminal proceedings via mobile communication and/or e-mail to notify them or for them to appear before the official conducting the criminal process, as well as the "Public Sector" functionality, which allows participants of the criminal process to receive remote access to the materials of electronic criminal cases, and to file complaints and petitions.

In the absence of the possibility of remote access, the participants in the criminal process can get acquainted with the materials of the criminal case by obtaining their electronic copy made by the official in charge of the criminal process (para. 26 of the Instruction).

An official of a criminal prosecution body gets access to administering an electronic criminal case in the Register after passing certain authorization and authentication processes through the use of an electronic digital signature issued by the National Certification Center of the Republic of Kazakhstan, of a personal identification number-code assigned by the state body carrying out within its competence statistical activities in the field of legal statistics and

special records, or of the identification with the use of a biometric reader (para. 9 of the Instruction).

During the conduct of preliminary investigation by an investigative or investigative operational team, members of the team carrying out such investigation get access to the electronic criminal case through the e-CC module (para. 31 of the Instruction). First electronic documents are automatically generated in the Register even before the start of criminal proceedings: those are a report on the registration of a crime in a record book, a report of crime, notification to the public prosecutor of the start of a pre-trial investigation.

A decision to choose the electronic format of a criminal case is made by an official in charge of the preliminary investigation, when taking charge of the proceedings (para. 10 of the Instruction), on which a reasoned order is drawn up (art. 42-1(2) CPC of Kazakhstan). After the issuance of the order, the e-CC module generates an automatic notification to the supervising public prosecutor within 24 hours.

Documents attached to the materials of the criminal case, created earlier on paper, after the decision to conduct the criminal case in electronic format has been taken, are scanned and enclosed in the electronic criminal case in the form of PDF documents immediately, but no later than 24 hours after an order to conduct electronic proceedings is issued (paras. 11, 14 and 16 of the Instruction). Paper documents converted into electronic format are stored by the criminal prosecution authorities and forwarded to the public prosecutor's office or court along with the electronic criminal case (para. 6 of the Instruction). Media files, which, by decision of an official conducting the criminal process, are attached to the electronic criminal case, should be input into the e-CC module (para. 13 of the Instruction). In the Register, the necessary information accounting documents are filled out, and electronic interaction with experts, specialists and the court is carried out (para. 5 of the Instruction).

At the same time, the CPC of Kazakhstan or the Instruction do not directly indicate in what way, after a decision is made to conduct a criminal case in an electronic format, the materials and documents provided by a defence counsel or other participants in the criminal case and drawn up in paper format are supposed to be attached to it, nor what the requirements are for electronic documents submit-

ted to the investigator by the participants in the proceedings, in particular, those concerning the volume of a document, quality of scanning or mandatory attributes.

It is not regulated whether an official conducting proceedings in an electronic criminal case has the right to perform investigative actions in a non-electronic format if they are carried out under conditions that preclude electronic workflow (re-inspection of the crime scene, interrogation of a witness at his location , etc.), whether it is possible to conduct investigative or other procedural actions in an electronic criminal case with the preparation of procedural documents in paper format, when there is no possibility of compiling electronic documents, but without switching to a paper format case in general.

The issue of compliance with the time limits of preliminary investigation, detention and performance of investigative and other procedural actions in the event of long-term (more than 24 hours) failures in the functioning of the Register or other emergency situations, remains open, provided that all materials of the criminal case are kept in electronic format and cannot be printed out.

6. The Criminal Procedure Code of the Kyrgyz Republic of 2021 (hereinafter referred to as CPC of Kyrgyzstan) defines the following among its main concepts:

a complaint is an objection brought either in written or electronic form (signed or certified by an electronic signature);

an electronic document is a document in which information is provided in electronic and digital form and is certified by means of an electronic signature;

an electronic case is criminal proceedings which are conducted in electronic and digital form, designating case movement, starting from registering a crime report, followed by pre-investigative verification, investigation, court proceedings and execution of the sentence, which is formed with data of the relevant agency information systems, with an option to generate procedural documents in paper form that are certified by means of an electronic signature, accumulated in the Unified Register of Crimes;

an electronic medium is an external mobile material device used for recording, storing and reproducing information processed with the use of means of computing technology (art. 5).

The CPC of Kyrgyzstan distinguishes between messages, information and comments in written or electronic form (in writing or in the form of an electronic document) (arts. 59, 91 and 311); establishes a procedure, similar to the Russian procedures, for storing material evidence in the form of electronic media, copying information from them, seizing electronic media during search and seizure, and draws a distinction between a legal owner of the seized electronic media and an owner of the information contained on them (arts. 87 and 212). Documents as a type of evidence may include photo, sound and video recording materials, as well as all types of electronic documents (art. 89). When seizing property, heads of banks and other credit institutions are obligated to provide information established by the CPC of Kyrgyzstan, including in the form of an electronic signed document (art. 121). The CPC of Kyrgyzstan also provides for the preparation of an expert opinion in the form of an electronic signed document on a par with a written opinion certified by his handwritten signature and seal (art. 193).

In accordance with art. 89 CPC of Kyrgyzstan, an electronic document is recognized as evidence that is equal in its significance to written evidence, and has the same legal effect as a document reproduced on paper and confirmed electronically. The original electronic document exists only on a machine-readable medium. All copies of an electronic document that are signed with an electronic and digital signature, recorded on a machine medium and identical to one another, constitute originals and having the same legal effect. Copies of an electronic document are created by reproducing the form of an external representation of an electronic document on paper. Electronic documents reproduced on paper must contain an indication that they are copies of the corresponding electronic document and must be certified in the manner prescribed by law for certification of copies of electronic documents on paper.

The applications of participants of criminal proceedings addressed to the investigating judge and orders of the investigating judge can be drawn up in the form of an electronic signed document. The applications may be accompanied by documents in the form of an electronic signed document, electronic document or electronic image (art. 264).

When implementing international cooperation in the field of criminal proceedings, the central authority of the Kyrgyz Republic may accept for consideration a request (commission, application) received from the requesting party via electronic, facsimile or other means of communication. The execution of such a request (commission, application) is carried out exclusively on condition of confirmation of the sending or transfer of its original version. Forwarding of the materials of the executed request (commission, application) to the competent authority of a foreign state is only possible upon receipt by the central authority of the Kyrgyz Republic of the original request (art. 510).

A request for extradition of a person present on the territory of a foreign state is sent to the foreign state in writing or in the form of an electronic signed document, unless otherwise stipulated by an international treaty (art. 522).

The CPC of Kyrgyzstan provides for the specifics of the interrogation of a victim or witness using technical means in a video-link mode (remote interrogation) at the stage of pre-trial proceedings (art. 201); interrogation of a victim, witness, expert, specialist, accused (convicted) person held in custody by videoconferencing (remote interrogation) at the trial stage (art. 290); identification of persons or objects in the videoconference mode when broadcasting from other premises (art. 209); secret audio or video control of a person or place (special investigative action) (art. 233); when inspecting material evidence located in another locality, technical means of videoconferencing may be used in the execution of a court order by a district (city) court at the location of such evidence (art. 333); when inspecting areas or premises located on the territory of other districts, technical means of videoconferencing may be used in the execution of a court order by a district (city) court at their location (art. 335).

In accordance with art. 516 CPC of Kyrgyzstan, a witness, victim, expert, as well as person held in custody on the territory of a foreign state, may be interrogated with the use of technical means in a videoconferencing mode (remote interrogation) in the manner prescribed by arts. 201 and 290 CPC of Kyrgyzstan, if such procedure is provided for by an international treaty of the Kyrgyz Republic that has entered into force. At the same time, art. 520 CPC of Kyrgyzstan

provides for the conduct of procedural actions, without specifying their range, by video-link at the request of the competent authority of both a foreign state and Kyrgyzstan in the way of international legal assistance.

Of interest are also the requirements of art. 200 CPC of Kyrgyzstan, according to which the use of sound and video recording (technical means of fixation) is mandatory in cases of interrogation of: (1) children; (2) the blind, the illiterate, the semiliterate, who are unable to read the records of their testimony as laid down in the protocol of interrogation; (3) persons interrogated through an interpreter; (4) suspects and accused in cases of especially grave crimes; (5) persons in need of examination by expert psychiatrists; (6) when confession testimony is being given by suspects or accused persons about their commission of crimes.

In our view, such expansion of the range of investigative and court actions carried out using videoconferencing systems is a positive trend in the development of criminal procedural legislation, as it increases the speed and effectiveness of the investigation of crimes, and ensures at the same time the observance of human rights in the criminal process.

7. The Criminal Procedure Code of the Republic of Moldova of 2003 (hereinafter referred to as CPC of Moldova) defines evidence as factual data obtained in the manner prescribed by law that are used to establish the presence or absence of elements of a crime, identify the perpetrator of the crime, establish the guilt or innocence of the accused, as well as determine other circumstances that are important for the proper resolution of the case (art. 93 CPC of Moldova).

Audio or video recordings, photographs, means of electronic and technical, magnetic or optic control and other carriers of electronic and technical information obtained in line with the requirements of the legislation, shall be means of evidence if they contain data or weighty indications as to the preparation or commission of a crime and if their content contributes to finding the truth in the case (art. 164 CPC of Moldova).

The CPC of Moldova regulates the procedure for conducting an electronic search and seizure of electronic information (art. 130-1), and for monitoring the online activity of Internet users based on a court decision (art. 132-11).

8. The Criminal Procedure Code of the Republic of Tajikistan of 2009 (hereinafter referred to as CPC of Tajikistan) defines evidence as factual information, based on which the court, investigator, inquirer and prosecutor establish the presence or absence of a socially dangerous act, proof or lack of proof of the commission of such act and other circumstances that might be important for the correct resolution of the case (art. 72(1) CPC of Tajikistan).

An analysis of the criminal procedural legislation of the Republic of Tajikistan allows to conclude that the law classifies electronic sources of information as documents, but does not contain rules for their application.

9. According to art. 131 of the Criminal Procedure Code of Turkmenistan of 2009 (hereinafter referred to as CPC of Turkmenistan), factual data of investigative and court actions recorded in protocols that are of practical significance for the case serve as evidence. These data can be recorded both in writing and in another form (audio and video recording, recording on computer information media).

In accordance with art. 125(1) CPC of Turkmenistan, evidence may be excluded in case of violations that can affect its credibility. This rule on the exclusion of evidence cannot be applied to material evidence obtained as a result of illegal wiretapping, illegal search or other evidently unconstitutional actions of officials, since material evidence is inherently reliable.

Of interest among the investigative actions set out in the CPC of Turkmenistan are seizure of correspondence (art. 281), interception of messages (art. 282) and wiretapping and sound recording of telephone and other conversations (arts. 283–284). These investigative actions are carried out on the basis of a decision of an inquirer or investigator sanctioned by a public prosecutor.

10. The Criminal Procedure Code of the Republic of Uzbekistan of 1994 (hereinafter referred to as CPC of Uzbekistan) defines as evidence in a criminal case any factual data, on the basis of which in the manner prescribed by law, the body of inquiry, investigators and court establish the presence or absence of a publicly dangerous act, the guilt of the person who committed it, as well as other circumstances relevant to the right resolution of the case.

Documentary materials include paper, photographic paper, video and film tape, audiotape, etc. Fixing information on them

can be carried out using letters, numbers, stenographic, telegraph and other signs, images, diagrams, etc. Particularly significant information can be recorded using various technical devices and machines (cinema and video camera, tape recorder, etc.). Materials of operational search activities can be recognized as evidence after their verification and evaluation (art. 81 CPC of Uzbekistan).

The criminal procedural legislation of the Republic of Uzbekistan does not contain special requirements for the collection, storage and evaluation of electronic media and electronic information.

Thus, in the CIS member states, including the Russian Federation, electronic information is not singled out as a separate source of evidence and, as a rule, gets classified as "other documents". Electronic information carriers are not defined as a separate type of evidence either, and are viewed as part of material evidence.

In our opinion, in accordance with art. 20 of the CIS Charter of 22 January 1993, a comprehensive and coordinated reform of the criminal procedural legislation of the CIS member states is called for.

First of all, it is necessary to determine in the codes of criminal procedure of the CIS member states the list of procedural documents that can be drawn up in electronic form in the course of criminal proceedings and to regulate the procedure for their issuance.

The interaction between the competent authorities of the CIS countries in the field of criminal proceedings should be carried out within a single virtual environment, and the exchange of information should not take place between separate databases of law enforcement agencies, as it is currently the case. This will contribute to the development of information technologies in criminal proceedings and will allow to carry out proceedings in criminal cases in an electronic format.

In addition, it is critical to organize training/retraining for law enforcement officers in the field of online forensics, which will contribute to a more effective investigation of acts committed on the Internet (credit card fraud, illegal arms and drug trafficking, human trafficking and other cross-border crimes).[1]

[1] С.П. Щерба, И.В. Чащина, *op. cit.*, p. 301.

Chapter 2

COLLECTION AND USE OF ELECTRONIC EVIDENCE IN THE FRAMEWORK OF INTERNATIONAL COOPERATION IN CRIMINAL MATTERS

(*P.A. Litvishko*)

§ 1. Legal Framework and General Rules for Collection of Electronic Evidence through International Cooperation in Criminal Matters

International treaties in force do not lay down any definitions of electronic evidence. It is defined in the following international legal documents:

Regulation of the European Parliament and of the Council of 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 defines electronic evidence as "subscriber data, traffic data or content data stored by or on behalf of a service provider, in an electronic form".[1]

Guidelines on electronic evidence in civil and administrative proceedings, adopted by the Committee of Ministers of the Council of Europe in 2019 ("Electronic evidence" means any evidence derived from data contained in or produced by any device, the functioning of which depends on a software program or data stored on or transmitted over a computer system or network").[2]

[1] 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 (art. 3).

[2] Guidelines CM(2018)169-add1final of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings (Adopted by the Committee of Ministers on 30 Jan. 2019, at the 1335th meeting of the Ministers' Deputies), Explanatory Memorandum.

Model Law on Mutual Assistance in Criminal Matters of 2007, as amended in 2022 (United Nations Office on Drugs and Crime) ("Electronic evidence means any data or information generated, stored, transmitted or otherwise processed in electronic form that may be used to prove or disprove a fact in legal proceedings").[1]

Guidelines for identification, collection, acquisition and preservation of digital evidence of 2012 (International Organization for Standardization) ("Digital evidence" means information or data, stored or transmitted in binary form, that may be relied on as evidence").[2]

Practical Guide for Requesting Electronic Evidence across Borders of 2021 (UN) in its glossary narrowly defines electronic evidence (e-evidence) as including "basic subscriber information, traffic data[3] and content data".[4]

Russian Draft United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes of 2021 ("Electronic evidence" shall mean any evidentiary information stored or transmitted in digital form (on an electronic medium").[5]

The cross-border sharing of electronic evidence may take place (1) within the well established "reactive" triad of investigation, prosecution and judicial proceedings as part of international legal (judicial) assistance, and equally (2) for the proactive purposes of preventing, detecting or disrupting crime, during criminal intelligence operations or pre-investigative examinations as part of international law enforcement (police-to-police) cooperation.

---

[1] *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) (sec. 27).

[2] ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence.

[3] Apart from traffic data, various legal acts of the European Union also distinguish among metadata (constituting a separate category along with subscriber data and content data) location data, access data and transactional data, which are generally covered by traffic data.

[4] *The Practical Guide for Requesting Electronic Evidence across Borders* (Vienna: United Nations, 2021), p. 238.

[5] URL: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home, accessed Dec. 8, 2023.

The legal framework for international cooperation of the Russian Federation in criminal matters involving crimes committed with the use of ICT or in the field of computer information, as well as in the collection of electronic evidence in cases relating to these or any other criminal offences, even where currently our country is not a party to any special criminal justice treaty on that subject, is nonetheless quite extensive.

Legal assistance in the acquisition of both stored electronic evidence and its real-time collection (interception)[1] is requested and provided by the Russian Federation under universal sectoral, regional ordinary crime and sectoral international instruments, such as the 2000 Palermo Convention (UN), 1959 European Convention and its additional protocols, 2005 Warsaw Convention (Council of Europe), 1993 Minsk Convention, 2002 Kishinev Convention (CIS), 2015 Agreement on the Procedure for Establishing and Operation of Joint Investigative and Operational Teams in the Territories of the Member States of the Commonwealth of Independent States, as well as pursuant to bilateral treaties on legal assistance and legal relations, binding UN Security Council resolutions and on the basis of the principle of reciprocity.

At the same time, such global and regional anti-crime and counter-terrorism treaties are not customized to serve the electronic evidence domain, do not cater to the needs of procuring a broad scope of electronic evidence of all kinds with regard to any criminal offences and irrespective of the stages of criminal proceedings, which may differ significantly in the states parties' legal systems.

Some of those international agreements also regulate law enforcement (police) cooperation. Exclusively law enforcement assistance, but not legal (judicial) assistance, is regulated by bilateral and multilateral (CIS, SCO, CSTO, etc.) intergovernmental and interstate agreements and arrangements:

- on cooperation in combating crime (in particular, ordinary criminal offences, ICT crimes, terrorism, extremism, corrup-

[1] Recommendation No. R (85) 10 of the Committee of Ministers to Member States concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications (Adopted by the Committee of Ministers on 28 June 1985 at the 387th meeting of the Ministers' Deputies); Technical Specification: Lawful Interception (LI); Requirements of Law Enforcement Agencies. ETSI TS 101 331 V1.8.1 (2021-07), 33 p.

tion, money laundering). The same category includes special treaties within the framework of the CIS: the 2001 Agreement on Cooperation of the Member States of the Commonwealth of Independent States in Combating Crimes in the Sphere of Computer Information (Minsk Agreement) and the 2018 Agreement on Cooperation of the Member States of the Commonwealth of Independent States in Combating Crimes in the Sphere of Information Technologies (Dushanbe Agreement), which replaces the Minsk Agreement; within the framework of the CSTO, the 2014 Protocol on Interaction of the Member States of the Collective Security Treaty Organization in Countering Criminal Activities in Information Sphere;[1]

- on cooperation in the field of ensuring international information security;
- international interagency (RF Ministry of Internal Affairs, RF Prosecutor General's Office, etc.) agreements and other arrangements.

The overwhelming majority of requests for legal assistance in criminal cases related to ICT crimes are sent to the Prosecutor General's Office of the Russian Federation from Belarus, which is primarily attributable to the location in Russia of major ICT service providers and social media hosting services popular with Belarusian users. The same circumstance is partly responsible for the relatively small number of Russian requests for legal assistance in such cases sent abroad to obtain electronic evidence, in particular from US service providers. The main offences in relation to which assistance is requested in both incoming and outgoing requests are cyber fraud (social engineering techniques), cyber extortion (including sextortion), and online child sexual exploitation and abuse (mostly self-generated child sexual abuse material). In addition, incoming requests also concern money/parcel (reshipping) mule scam and romance scam, the latter being sometimes combined with investment fraud (pig butchering scam). A big problem is created by phone

[1] In 2014, the Collective Security Treaty Organization Consultative Coordination Center for Computer Incident Response (CSTO CCC) was established in Moscow, which, among other things, exchanges notifications of contact points of the CSTO member states on malicious activity emanating from or in relation to one another's address (information) space, information resources, software vulnerabilities and information security threats.

scammers operating from foreign call centers, especially those located in Ukraine, in relation to clients of Russian banks.

The main problems in the investigation of those offences lie in the areas of preservation of electronic traces; prompt interaction with ICT service providers; encryption (particularly end-to-end encryption in instant messaging apps); decentralized messaging apps (no central server due to the applied blockchain and peer-to-peer technology, no phone number required for subscriber registration and identification); service providers' zero-log policies, peer-to-peer networks, Darknet, etc., almost all of them thus boiling down to the technological challenges of user identification and authentication, anonymization and attribution of cyber attacks. The complexity of the rapid collection of digital evidence is generally caused by the lack of a technical basis for the guaranteed identification of devices connected to the Internet and consequently their subscribers and/or end-users.

The exchange of information on computer incidents with authorized bodies of foreign states, international, international non-governmental organizations and foreign organizations operating in the field of responding to computer incidents is carried out by the National Coordination Center for Computer Incidents, except for cases where the direct exchange of such information by a subject of the critical information infrastructure with a foreign (international) organization is provided for by an international treaty of the Russian Federation.[1]

Russian federal laws obligate service providers and some other categories of data custodians to retain on the territory of the Russian Federation and provide to the Russian competent authorities subscriber/user information, communications (traffic, connections) data and content data: telecom operators (3 years, 3 years and up to 6 months respectively), organizers of information circulation on

[1] Order of the RF Federal Security Service of 24 July 2018 No. 368 "On approval of the Procedure for the exchange of information on computer incidents between the subjects of the critical information infrastructure of the Russian Federation, between the subjects of the critical information infrastructure of the Russian Federation and authorized bodies of foreign states, international, international non-governmental organizations and foreign organizations engaged in responding to computer incidents, and the Procedure for obtaining information by the subjects of the critical information infrastructure of the Russian Federation on the means and methods of conducting computer attacks and on the methods for their prevention and detection" (para. 11 of Appendix No. 1).

the Internet, including organizers of instant messaging services (1 year, 1 year and up to 6 months respectively; they are also obliged to provide the state security agency with decryption information for electronic messages); proprietors and other possessors of technological communication networks having a unique identifier of the aggregate of communication means and other technical means on the Internet (autonomous system number) (3 years for user information and traffic data, and there is no retention obligation imposed upon them for content data); and hosting providers (3 years for user information, 1 year for connections and other traffic data, and there is no retention obligation imposed upon them for content data).

To implement those federal laws, the Government of the Russian Federation has enacted a number of resolutions on the relevant obligations of ICT service providers and other custodians.[1]

[1] Federal Law of 7 July 2003 No. 126-FZ "On Communications" (arts. 53, 56^{2}(9–10) and 64); Federal Law of 27 July 2006 No. 149-FZ "On Information, Information Technologies and Information Protection" (arts. 10^{1}, $10^{2\text{-}1}$, 10^{3}–10^{7}); RF CPC (arts. 5(14^{1}, 24^{1}), 13, 29 and 185–186^{1}); Federal Law of 12 Aug. 1995 No. 144-FZ "On Operational Search Activities" (arts. 6 and 8); Rules for the interaction of telecom operators with authorized state bodies carrying out operational search activities, approved by Resolution of the RF Government of 27 Aug. 2005 No. 538; Rules for the interaction of organizers of information dissemination in the information and telecommunications network "Internet" with authorized state bodies carrying out operational search activities or ensuring the security of the Russian Federation, approved by Resolution of the RF Government of 31 July 2014 No. 743; Rules for the storage by telecom operators of text messages of users of communications services, voice information, images, sounds, video and other messages of users of communications services, approved by Resolution of the RF Government of 12 Apr. 2018 No. 445; Rules for the interaction of proprietors or other possessors of technological communication networks having a unique identifier of the aggregate of communication means and other technical means in the information and telecommunications network "Internet" with authorized state bodies carrying out operational search activities or ensuring the security of the Russian Federation, approved by Resolution of the RF Government of 29 Oct. 2019 No. 1385; Rules for the storage by organizers of information dissemination in the information and telecommunications network "Internet" of information on facts of reception, transmission, delivery and/or processing of voice information, written text, images, sounds, video or other electronic messages of users of the information and telecommunications network "Internet" and information about such users, and providing it to authorized state bodies carrying out operational search activities or ensuring the security of the Russian Federation, approved by Resolution of the RF Government of 23 Sept. 2020 No. 1526; Rules for the storage by an organizer of information dissemination in the information and telecommunications network "Internet" of text messages of users of the information and telecommunications network "Internet", voice information, images, sounds, video and other electronic

Violation of these retention and other related obligations entails administrative liability (articles of Ch. 13 (administrative offences in the field of communications and information) of the Code of Administrative Offences of the Russian Federation).

Russian law enforcement and judicial authorities normally apply the following algorithm of actions to obtain data from foreign ICT service providers (referred to in various sources as electronic (digital) evidence, which is a narrow meaning of this concept), depending on the type of data required in a criminal case, crime report examination or criminal intelligence case, as well as to execute or otherwise process respective foreign requests.

1. The ephemeral and transient nature of e-evidence causes law enforcement's race against time for laying their hands on it.

Where it is necessary to obtain information on communications that have already taken place (historical records), first of all immediately send a request asking to preserve the data of interest, since the periods of their storage vary significantly from country

messages of users of the information and telecommunications network "Internet", approved by Resolution of the RF Government of 26 Feb. 2022 No. 256; Rules for the identification of users of the information and telecommunications network "Internet" by an organizer of an instant messaging service, approved by Resolution of the RF Government of 20 Oct. 2021 No. 1801; Rules for the storage in the territory of the Russian Federation of information about facts of reception, transmission, delivery and (or) processing of voice information, text messages, images, sounds, video or other electronic messages, as well as other information about interaction of users of information systems and (or) programs for electronic computing machines functioning in technological communication networks, whose proprietors or other possessors have an autonomous system number, and information about these users, and its provision to authorized state bodies carrying out operational search activities or ensuring the security of the Russian Federation, approved by Resolution of the RF Government of 1 Sept. 2023. No. 1441; Rules for the interaction of hosting providers with authorized state bodies carrying out operational search activities or ensuring the security of the Russian Federation, approved by Resolution of the RF Government of 22 Nov. 2023 No. 1952; Rules for passing the identification and (or) authentication by persons who have applied to a hosting provider for the purpose of obtaining computing capacity for placing information in an information system permanently connected to the information and telecommunications network "Internet", approved by Resolution of the RF Government of 29 Nov. 2023 No. 2011; Requirements for computing capacity used by a hosting provider, for the performance by authorized state bodies carrying out operational search activities or ensuring the security of the Russian Federation, in cases established by federal laws, of measures for the purpose of fulfillment of tasks entrusted to them, approved by Order of the RF Ministry of Digital Development, Communications and Mass Media of 1 Nov. 2023 No. 935 (para. 9 of Annex No. 1).

to country and from provider to provider, and can be very short or not at all established by the legislation of the country or the rules of the provider.[1] Otherwise, the initiators of requests for legal or law enforcement assistance are likely to receive, after a long time, replies about the absence of the requested data, which leads to useless waste of resources of both investigative authorities and foreign counterparts on the knowingly unattainable purposes.

Such a request for data preservation is usually sent via the following one or simultaneously several channels:

(1) directly to a foreign service provider, in particular, the one providing services on the territory of the Russian Federation, if in their officially published policy they declare the possibility of their interacting directly with foreign law enforcement and judicial authorities, and possibly maintain the Russian language version of their portal for relevant applications in electronic form. The request may also be addressed to a branch or a representative office of a foreign person operating on the Internet on the territory of the Russian Federation, or to a Russian legal entity established by a foreign person operating on the Internet on the territory of the Russian Federation, pursuant to art. 7 of Federal Law of 1 July 2021 No. 236-FZ "On the Activities of Foreign Persons on the Information and Telecommunications Network "Internet" in the Territory of the Russian Federation";

[1] For example, such retention periods are not established in the legislation of the United States, which is considered the principal recipient of the relevant requests. See also on the latest developments in EU law in this area: Data retention developments in Europe. Overview of rulings of the Court of Justice of the European Union related to data retention for the purposes of prevention and prosecution of crime, in *Cybercrime Judicial Monitor*, Issue 6 — May 2021 (The Hague: Eurojust, 2021), pp. 19–33; Judgment of the Court of Justice of the EU (Grand Chamber) of 21 Dec. 2016 in Joined Cases C-203/15 and C-698/15; Judgments of the Court of Justice of the EU of 6 Oct. 2020 in Case C-623/17 and in Joined Cases C-511/18, C-512/18 and C-520/18; Court of Justice of the European Union, PRESS RELEASE No 123/20, Luxembourg, 6 Oct. 2020 (The Court of Justice confirms that EU law precludes national legislation requiring a provider of electronic communications services to carry out the general and indiscriminate transmission or retention of traffic data and location data for the purpose of combating crime in general or of safeguarding national security). URL: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123en.pdf; Judgment of the Court of Justice of the EU (Grand Chamber) of 20 Sept. 2022 in Joined Cases C-793/19 and C-794/19; *SIRIUS EU Digital Evidence Situation Report 2022*, pp. 53–56.

(2) through the channels of law enforcement (police-to-police) cooperation, i.e. through I-24/7 INTERPOL communications network (through the INTERPOL NCB of the RF Ministry of Internal Affairs and its regional branches), or through other similar networks; directly to a foreign law enforcement or judicial authority on the basis of international treaties of the Russian Federation,[1] interagency agreements or based on the principle of reciprocity; to police or other law enforcement or judicial liaison officers posted at an embassy or consular post of the relevant foreign state in Russia.

Thereafter, when forwarding requests for the production of the following types of electronic evidence in relation to historical communications, one should include in such requests an indication as to the implemented preservation, reflecting the identification reference number, code or other attributes of the saved material reported by the service provider.

2. A request to provide data on the subscriber/user, the equipment used by him or her, his or her correspondence with the provider's technical support service can be sent directly to the foreign provider or through the channels of law enforcement (police-to-police) assistance in the manner described above. However, many countries and providers require that these data be obtained only through the use of legal assistance procedures, especially if they concern the identification of users of dynamic IP addresses, therefore in such cases, the request must be sent to the competent authorities of a foreign state in accordance with art. 453 of the Criminal Procedure Code of the Russian Federation of 2001 (with further amendments, hereinafter referred to as RF CPC).

3. A request for legal assistance in obtaining retrospective information on completed connections between subscribers and/or subscriber devices (historical traffic data, including GPS or cell

[1] These are mainly bilateral and multilateral intergovernmental and interstate agreements on cooperation in the field of combating crime and/or on cooperation in the field of ensuring international information security, which regulate the sending and execution of requests for law enforcement assistance, but do not concern requests for legal assistance.

See also: К.К. Клевцов, "Переписка в мессенджерах как доказательство. Способы получения и оформления" [Correspondence in messengers as evidence. Methods of obtaining and registration], *Уголовный процесс* 10 (2020), pp. 42–45.

site location tracking data (cellular tower and triangulation data))[1] pursuant to art. 186[1] RF CPC, is sent to the competent authorities of a foreign state in accordance with art. 453 RF CPC, to which attached is a relevant decision of a Russian court or its certified copy. By virtue of art. 455 RF CPC and the RF legislation on secrecy of communication, the mutual legal assistance procedure must also be observed in cases where a foreign state unilaterally allows receiving from them of this type of data under the aforementioned simplified law enforcement assistance procedure.[2]

4. A request for legal assistance to obtain historical content data, including the inspection and seizure of electronic messages or other messages transmitted over telecommunications networks, as provided for in art. 185(7) RF CPC, is sent to the competent authorities of a foreign state in accordance with art. 453 RF CPC, to which comes attached a relevant decision of a Russian court or a certified copy thereof.

It should be noted that the concept of content may differ from country to country. For instance, geolocation data and profile pictures (avatars) are considered content data in the United States.[3]

One should also take account of the differences in the scope of the concepts of personal privacy and secrecy of communication depending on the country.[4]

In the United States, communications which a customer has not accessed (unretrieved communications, i.e. where he or she has not logged on, opened, viewed, read or listened to them) for up to 180 days from the moment of their delivery, and which are stored on a

---

[1] А.М. Багмет, В.В. Бычков, С.Ю. Скобелин, Н.Н. Ильин, *Цифровые следы преступлений: монография* [Digital traces of crimes: monograph] (М.: Проспект, 2021), 168 p.

[2] See, e.g.: *Request for Mutual Legal Assistance in Criminal Matters: Guidelines for Authorities outside of the United Kingdom* (London: Home Office, March 2022), pp. 33–37; Agreement between the Government of the Russian Federation and the Government of the United Kingdom of Great Britain and Northern Ireland on Co-operation in Fighting Crime of 6 Oct. 1997.

[3] *The Practical Guide for Requesting Electronic Evidence across Borders* (Vienna: United Nations, 2021), p. 35.

[4] For information on the Russian approaches, see, e.g.: *Способы получения доказательств и информации в связи с обнаружением (возможностью обнаружения) электронных носителей: учебное пособие* [Methods of obtaining evidence and information in connection with discovery (possibility of discovery) of electronic media: study aid] / В.Ф. Васюков, Б.Я. Гаврилов, А.А. Кузнецов [и др.]; под общ. ред. Б.Я. Гаврилова (М.: Проспект, 2017), pp. 57 and 71.

provider's server, have the highest level of protection necessitating that law enforcement authorities meet the most stringent procedural requirements to receive them from a provider, as compared to communications which the subscriber has accessed, or which are stored on the provider's server being "unclaimed" by the subscriber for more than 180 days.[1] Such rules have their origin in the concept of reasonable expectation of privacy.

The Czech legislation and practice proceed on the understanding that the secrecy of communication (unlike the general privacy and personal secret), being subject to disclosure through court proceedings, only extends to communications which are in the process of their transmission by an ICT service provider to the addressee, or which, though they had been delivered to the addressee, he has not had the opportunity to familiarize himself with due to objective reasons beyond his control (for instance, in case of having been taken into custody); which arrive to the person's device after its seizure by law enforcement (in this case, a judicial authorization for wiretapping, monitoring and recording of conversations is required); which are stored not in the memory of the seized device (for instance, in a cloud storage), but which can be accessed from that device.[2]

5. A request for legal assistance for monitoring and recording of conversations or other messages, as well as obtaining information on connections between subscribers and/or subscriber devices in real time, including prospective (real-time) GPS or cell site and triangulation tracking data, pursuant to arts. 186–186[1] RF CPC, is sent to the competent authorities of a foreign state in accordance with art. 453 RF CPC, to which enclosed is a relevant decision of a Russian court or a certified copy thereof.

6. If certain operational search measures, provided for by the Federal Law "On Operational Search Activities" and related to obtaining prospective information on subscriber connections or the content of messages (control of communications, wiretapping, capturing information from technical communications channels and obtaining computer information) are to be undertaken abroad, a request for assistance in conducting them can be forwarded to

[1] *Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors* (Washington, DC: U.S. Department of Justice, 2007), 81 p.

[2] *Elektronické důkazy v trestním řízení* [Electronic evidence in criminal proceedings] / R. Polčák, F. Púry, J. Harašta a kolektiv. 1. vydání (Brno: Masarykova univerzita, 2015), s. 122–126, 184–185, 210–216.

the competent authorities of a foreign state in accordance with a treaty of the Russian Federation,[1] especially if the foreign state conducts parallel investigations or proceedings in respect of the same circumstances.

However, most countries require such measures to be requested exclusively as part of legal assistance, and not law enforcement assistance,[2] therefore in such cases the request must be sent to the competent authorities of a foreign state in accordance with art. 453 RF CPC.

In this context, it is also worth noting that the Federal Law "On Operational Search Activities" (arts. 7(6) and 14(3)) regulates the execution of requests of international law enforcement organizations, law enforcement agencies and special services of foreign states in accordance with international treaties of the Russian Federation, but not the sending of such requests abroad by Russian authorities, nor does it mention the possibility of cooperation based on the principle of reciprocity.

When drafting a request for the preservation or provision of electronic evidence, it is necessary to ensure it contains precise and detailed technical information, including, in particular, accurate data on the time of access to an information resource on the Internet, up to a second, the time zone, the IP address of the visited resource, the name of the protocol or the port number through which the connection took place. The absence of this information or any part thereof in the request frequently renders its execution impossible, or else it may lead to the provision of data with respect to uninvolved persons or yield other erroneous data, for example, if there was a mistake in the indicated time zone with regard to dynamic addresses.

When sending requests for preservation or production of electronic evidence overseas, it is required to give special attention to

[1] For example, in accordance with the above mentioned Agreement between the Government of the Russian Federation and the Government of the United Kingdom of Great Britain and Northern Ireland on Co-operation in Fighting Crime of 6 Oct. 1997.

[2] *Special Investigative Techniques: Assessing the Need for Additional Regulation in the Council of Europe's Instruments of Legal Assistance in Criminal Matters: Discussion Paper* by Mr Pyotr Litvishko (Russian Federation), PC-OC Mod Substitute Member, Strasbourg, 19 Aug. 2021 [PC-OC/PC-OC Mod/Docs PC-OC Mod 2021/PC-OC Mod (2021)04E]; *Introductory Note to Discussion Paper* PC-OC (2021)10EN.

statement and justification therein of the requirements for confidentiality, ensuring the secrecy of investigation, or covert nature of operational search measures. For instance, in the United States, whose competent authorities execute a large number of such international requests, the files concerning judicial authorization of disclosure of communication secrecy are uploaded onto a public Internet portal of courts; service providers in turn notify, as a general rule, their customer, whose details are requested, of the receipt and/or results of consideration of the request.[1] Therefore the US counterparts need a justification of the confidentiality requirement by the requesting party, especially when the person of interest whose details constitute the subject of the request, is aware of the investigation underway in relation to him or her. Many other countries also require, in addition to such justification, the indication of a specific period within which it should be prohibited to provide notification, which is otherwise mandatory under their law, to the subscriber or user whose electronic data were collected by their competent authorities pursuant to a foreign request.

If the materials of an incoming foreign request contain information on criminal activity on the territory of the Russian Federation, which calls for a separate domestic investigation, the relevant criminal cases are initiated upon verification of such information.

In Russia, obtaining data of subscribers, including users of dynamic IP addresses, that do not contain information on connections

[1] The default notification can also take place automatically, by technical design of the provided service. See: *Data disclosure framework. General practices developed by international service providers in responding to overseas government requests for data* (Vienna: United Nations, 2021), pp. 18–19.

See also: А.Ю. Ушаков, С.В. Петраков, *Организация взаимодействия следственных органов с представителями администраций социальных сетей по вопросам своевременного предоставления и дальнейшего анализа электронной информации по уголовным делам о тяжких и особо тяжких преступлениях против личности, общественной безопасности и коррупционных преступлениях: практическое пособие* [Organization of interaction of investigative authorities with representatives of administrations of social networks on issues of timely provision and further analysis of electronic information in criminal cases of grave and especially grave crimes against the person, public security, and corruption crimes: practical manual] (СПб: Санкт-Петербургская академия Следственного комитета, 2022), pp. 24–25.

or content of messages, does not require a court decision[1] (the latest case law of the European Court of Human Rights, however, proceeds from the requirement of a court decision for certain types of subscriber data as well, such as details of the user of a dynamic Internet protocol address[2]), and consequently, in the international dimension, does not require going through a lengthy judicial assistance procedure either. Such data may be provided to foreign counterparts through INTERPOL or other police channels (among others, through law enforcement liaison officers accredited at embassies), as well as directly by the authorities conducting preliminary investigations or operational search activities. For instance, identifying foreign users of the Blue Whale Challenge and other child suicide games hosted on some Russian social media platforms (that are popular outside Russia, in Russian-speaking countries and among expat communities) and putting minors out of harm's way has been possible by way of overseas agents applying directly to Russian law enforcement, in particular the RF Investigative Committee, or through foreign police liaison officers stationed at embassies in Russia, or INTERPOL, or SPOCs, to promptly establish the potential victim's identity behind their user accounts. The Russian law enforcement also regularly and spontaneously tipped off their foreign counterparts regarding such communications.

When Russian authorities are required to produce stored data on the content of messages or on connections, to monitor and record conversations or the content of other messages, or to collect connections data in real time, or to carry out operational search measures (such as control of communications, wiretapping, capturing information from technical communications channels or obtaining computer information), as a result of which one gathers historical or prospective connections data (including cell site and triangula-

[1] Resolutions of the RF Supreme Court of 30 Mar. 2016 No. 82-АД16-1, of 11 Oct. 2016 No. 82-АД16-5.

[2] *Benedik v. Slovenia,* no. 62357/14, 24 Apr. 2018, ECHR; *Conditions for obtaining subscriber information in relation to dynamic versus static IP addresses: overview of relevant court decisions and developments. Discussion paper prepared by the Secretariat in cooperation with T-CY members of the Protocol Drafting Group.* Strasbourg, Version 25 Oct. 2018, T-CY (2018)26. See also: Directive (EU) 2019/713 of the European Parliament and of the Council of 17 Apr. 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA.

tion data) or content data, in compliance with the requirements of Russian law for the permissibility of these actions depending on the category of a criminal offence,[1] foreign authorities should send a request for legal assistance asking to carry out such investigative or other procedural actions or operational search measures, and if it is prescribed or permitted by law of their state, attach to such a

[1] In Russia, threshold values of categories of crimes (which are not below the medium gravity, and therefore fall within the conventional concept of a "serious crime" by virtue of art. 15 of the RF Criminal Code, art. 2 of the Palermo Convention, and other conventions) are used in relation to real-time collection (interception) of data on the content of communications, i.e. monitoring and recording conversations (art. 186 RF CPC), wiretapping of telephone or other conversations, and operational experiment (art. 8 of the Federal Law "On Operational Search Activities").

The assessment of intrusiveness and permissible thresholds of encroaching on personal privacy and secrecy of communication for law enforcement purposes varies widely throughout states, and consequently, ideally, seriousness/gravity of an offence cannot be taken to represent a one-size-fits-all attribute with respect to (electronic) evidence collection.

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. URL: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home, accessed Apr. 14, 2023; В.Ф. Васюков, "Процедуры получения сведений о содержании электронных сообщений при расследовании преступлений в уголовно-процессуальном законодательстве Российской Федерации и Республики Казахстан" [Procedures for obtaining information on the content of electronic messages during the investigation of crimes in the criminal procedure legislation of the Russian Federation and the Republic of Kazakhstan], *Расследование преступлений: проблемы и пути их решения* 4(14) (2016), pp. 124–129; В.Ф. Васюков, "Осмотр, выемка электронных сообщений и получение компьютерной информации" [Inspection, seizure of electronic messages and obtaining computer information], *Уголовный процесс* 10 (2016), pp. 64–67; С.Б. Миронов, *"О необходимости конкретизации оперативно-розыскного мероприятия снятие информации с технических каналов связи и объединения тождественных оперативно-розыскных мероприятий в единое оперативно-розыскное мероприятие"* [On the need to specify the operational search measure in the form of capturing information from technical communications channels and combine the equivalent operational search measures into a single operational search measure], in Уголовный процесс и криминалистика: теория, практика, дидактика (Конфликты и конфликтные ситуации в досудебном производстве по уголовному делу и в суде; Особенности преподавания уголовного процесса и современная уголовно-процессуальная практика): Сб. матер. всерос. науч.-практ. конференции (57-е криминалистические чтения) (М.: Академия управления МВД России, 2016), pp. 710–716.

request the respective decision of a foreign court or other competent judicial authority.

Incoming foreign requests for the (reactive) preservation of traffic or content data get processed taking into account the maximum allowable periods of the (proactive) retention of these data established by the legislation of the Russian Federation, and that after their expiry the data are automatically deleted.[1] Currently, there is a need for establishing in the Russian legislation the right, power and obligation of telecom operators, organizers of information dissemination on the Internet, proprietors or other possessors of technological communication networks having a unique identifier of the aggregate of communication means and other technical means on the Internet (autonomous system number) and hosting providers to preserve electronic evidence, as well as specific permissible time limits for such preservation, at the request of a competent authority of a foreign state related to the investigation or judicial proceedings in a criminal case, in excess of the retention periods under the current law, in cases of expiration of the latter, as well as establishing administrative liability for violation of such an obligation.[2] This actually also applies to data preservation by Russian service providers at requests of Russian law enforcement and judicial authorities. In addition, such preservation constitutes an international legal obligation that is to be implemented in domestic law.[3]

As a general rule, neither a foreign request for legal assistance nor a foreign court or equivalent judicial decision would be required where an investigator transfers the above mentioned data abroad under art. 161 RF CPC on his own initiative (spontaneous information) or otherwise decides to disclose data from his criminal case file at his discretion, or where the data are transferred within an international joint investigative team as part of its activities.

---

[1] See, e.g.: Resolution of the RF Government of 12 Apr. 2018 No. 445 "On approval of the Rules for the storage by telecom operators of text messages of users of communications services, voice information, images, sounds, video and other messages of users of communications services" (para. 8).

[2] Such preservation period is usually 90 days, with the possibility of its extension (e.g., under the US legislation and the Budapest Convention).

[3] Agreement on Cooperation of the Member States of the Commonwealth of Independent States in Combating Crimes in the Sphere of Information Technologies of 28 Sept. 2018 (art. 5(и)); Draft United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.

Due to the fact that traffic and content data are covered by secrecy of communication, and their receipt in accordance with international treaties is considered a coercive measure, normally requiring a court decision or in a number of countries, a decision of a public prosecutor, the simplified expedited procedures for direct communications between the competent state authorities in sending and executing MLA requests provided for by treaties, are generally not applicable to the requests for legal assistance at issue, in particular due to the respective declarations and reservations of the Russian Federation to the treaties (for example, to the 2001 Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters). Communications on these types of legal and law enforcement assistance are ordinarily carried out through the RF Prosecutor General's Office as a central authority.

No coercive or compulsory measures may be used in executing foreign requests for legal assistance in cases of criminal offences under foreign law that are qualified by Russian law as administrative offences or constitute neither a criminal nor an administrative offence (the absence of dual criminality). For instance, there is a large number of Belarusian requests for legal assistance in criminal cases of computer fraud, which, under Russian law, is considered petty theft (an administrative offence). Such requests, on the instructions of the RF Prosecutor General's Office, are executed in accordance with art. 29.1.5 of the RF Code of Administrative Offences of the Russian Federation by the authorities handling cases on administrative offences, including the warning of participants of requested procedural actions of administrative responsibility under arts. 17.7, 17.9 and 19.26 of the RF Code of Administrative Offences and, where required by the requestor, also under their country's criminal law, but not under Russian criminal law.[1] In exceptional cases, such requests for assistance in criminal cases can, nonetheless, be executed by criminal investigation authorities, in particular on the instructions of the public prosecutor, in accordance with art. 457 RF CPC, including interrogations of suspects or accused persons, provided that the measures of procedural coercion set out in RF CPC are not applied, and without warning the participants of the

[1] Apprising of the criminal liability for refusal to testify, knowingly false testimony (perjury), false accusation and unauthorized disclosure of the investigative information.

requested actions about the above mentioned responsibility under the criminal law of the requested state.

Those two categories of requests must not allow the conduct of requested investigative or other procedural actions or operational search measures interfering with the fundamental human rights and freedoms (coercive measures), which, as a general rule, depending on the country, require a decision of a court, judge or public prosecutor (human rights criterion). In the Russian Federation, such intrusive actions restricting the constitutional rights of an individual and a citizen and requiring a court sanction are enumerated in arts. 12–13 and 29 RF CPC and arts. 8–9 of the Federal Law "On Operational Search Activities".

Thus, a request for international assistance may only be executed insofar as the requested measure is allowed under the domestic law of the requested state, where appropriate subject to judicial authorization or its equivalent, hence a default ground for refusal of assistance would be the sought measure's inapplicability in a similar domestic case or that it is contrary to the requested state's domestic law, for example, where the investigated offence lacks dual criminality.[1]

The counter-terrorism and other sectoral conventions, which lay down the obligations of their parties to establish responsibility for the offences or unlawful acts they define, at the same time oblige the parties to provide each other assistance only in criminal matters. Meanwhile, the corporate liability for the offences prescribed by these conventions may be criminal, civil or administrative. This alternative formula is included in most contemporary multilateral

[1] The respective treaty ground for refusal of assistance is discretionary and may be applied in each individual case either formally by the central authority or, factually, by a court denying authorization for the requested action. See: UN Convention against Transnational Organized Crime (art. 18(21)(c)); UN Convention against Corruption (art. 46(9, 21(c)); Explanatory Report to the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism. Warsaw, 16.V.2005, p. 35, para. 224; *UNODC Revised Manual on the Model Treaty on Mutual Assistance in Criminal Matters*, p. 89, para. 88; G. Vermeulen, W. De Bondt and C. Ryckman, *Rethinking international cooperation in criminal matters in the EU. Moving beyond actors, bringing logic back, footed in reality* (Antwerpen-Apeldoorn-Portland: Maklu, 2012), pp. 140–145; Directive 2014/41/EU of the European Parliament and of the Council of 3 Apr. 2014 regarding the European Investigation Order in criminal matters ("in a similar domestic case").

global and regional (in particular, the Council of Europe) anti-crime treaties. Such administrative liability of legal persons for criminal offences (crimes) is also prescribed by the Convention on Cybercrime (art. 12), therefore, such substantive conventional provisions can serve as the basis for the application of procedural provisions of these treaties concerning the obligations of the parties to cooperate in criminal matters, equally in respect of cases on administrative offences against legal persons charged with the commission of acts covered by the convention.

It should be taken into account that terminological designations (and even more so the translations thereof) of categories of offences cannot serve *per se* as a criterion for the applicability of treaties or domestic legislation on administrative offences, since they differ from country to country; they should be distinguished from criminal offences or crimes (felonies and misdemeanors) based on by which law (criminal or administrative) of the requesting or requested state they are proscribed. The most unambiguous in this regard are authentic texts drawn up in one language, of treaties between countries having common legal traditions and systems, for example, those concluded within the Commonwealth of Independent States. For instance, the 2018 Agreement on Cooperation of the CIS Member States in Combating Crimes in the Sphere of Information Technologies (arts. 2–3 and 5) uses the concepts of a "criminally punishable act" and a "crime", providing for specific forms of cooperation, including in the prevention of these crimes, which may also cover the interaction of the parties in cases of administrative offences.[1]

Specific forms of cooperation in the fight against both crimes and administrative offences are set forth in treaties on international information security,[2] which either contain a direct indication as to the interaction in the field of administrative offences, or use the

[1] When ratifying the Agreement, the Russian Federation made a reservation to the effect that it reserves the right to consider the acts proscribed by particular provisions of art. 3 of the Agreement (criminally punishable acts), both as criminally punishable in accordance with the RF Criminal Code, and as administratively punishable in accordance with the RF Code of Administrative Offences (Federal Law of 1 July 2021 No. 237-FZ "On ratification of the Agreement on Cooperation of the Member States of the Commonwealth of Independent States in Combating Crimes in the Sphere of Information Technologies").

[2] See, e.g.: the Agreement between the Government of the Russian Federation and the Government of Turkmenistan on cooperation in the field of ensuring international information security of 5 Apr. 2019.

concept of an "offence" (sometimes in tandem of "crimes and other offences"), covering both criminal and administrative offences, and also, less often, deal with cooperation of the parties in the law enforcement field in general, countering illegal activities, ensuring public order, law and order, and security.

Judicial and extrajudicial removal of content or other restrictions imposed on access to information resources provided for by the legislation of the Russian Federation can also be undertaken on the basis of eligible foreign requests and communications to block relevant information, given that they comply with the provisions of the Russian law.

As was mentioned above, identification of the device which accessed the Internet may not always be possible due to the Internet provider lacking the technical capability to do it. Using the software that conceals or disguises/substitutes the user's IP address (Tor and other proxy servers, anonymizers, VPNs with zero-log policy, etc.) can make his or her identification challenging, but basically it remains possible, which is also the case when one uses pools of IP addresses distributed by NAT (Network Address Translation) technology, where the same external IP address can be simultaneously allocated to many subscribers.[1]

[1] A variation of CGNAT (LSN) (Carrier-Grade NAT), in which one public IP address in the fourth version of the Internet Protocol (IPv4) is used to provide access to the Internet for a random (dynamic) list of internal IP addresses of subscribers. The use of this technology is primarily caused by the exhaustion of IPv4 addresses and the insufficient implementation of the sixth version of the Internet Protocol (IPv6), which significantly expands the number of IP addresses. Since this technology selects dynamically which internal IP addresses of subscribers will use the public IP address, several hundred and even thousands of subscribers/end-users can simultaneously be logged at this IP address. Therefore, to determine the specific internal IP address of the subscriber/end-user that used the public IP address, it is necessary to know the precise time of the subscriber/end-user's access session and connections, the IP address and the source port of this access. However, the source port number information required for subscriber identification is not logged at internet-facing servers or retained by a lot of service providers, which makes attribution difficult or impossible based on the lists of hundreds or thousands of subscribers. See: *Common challenges in combating cybercrime. As identified by Eurojust and Europol. Joint Report*. June 2019, pp. 6–8.

In accordance with the Rules for the interaction of telecom operators with authorized state bodies carrying out operational search activities, approved by Resolution of the RF Government of 27 Aug. 2005 No. 538 (para. 13), data on NAT transmissions are transferred by a telecom operator directly to the equipment of the control points of the national security agencies, without the telecom operator

When executing a foreign request to establish a subscriber's dynamic IP address, if the request does not contain indispensable accurate data on the time of access to an information resource on the Internet, up to a second, including information on the time zone, the IP address of the visited resource, the protocol name or port number through which the connection was made, service providers usually produce very large sets of subscriber data, a priori collaterally scooping up dragnets of personal data pertaining to dozens of uninvolved or otherwise irrelevant citizens (data mining), the permissibility of transferring which to foreign requestors for their own subsequent filtering, collation, matching and further analysis is evaluated in each specific case, taking account of the practical possibility for the foreign initiator to specify or narrow down their request, the necessity and proportionality of the cross-border transfer of such personal data, based on the provisions of the Federal Law of 27 July 2006 No. 152-FZ "On Personal Data", in particular its art. 12 (cross-border transfer of personal data). Otherwise, such across-the-board, indiscriminate and excessive personal data normally cannot be shared with foreign counterparts.

Some countries explicitly prohibit foreign requests to search for evidence (fishing expedition) in their territory, for example, information about whether a person holds any bank accounts in the requested state.[1]

If there exist relevant legal grounds, anonymization of participants of the requested proceedings (art. 166(9) RF CPC) can be applied if it is necessary to ensure their safety, especially where they turn out to be fully uninvolved in any illicit activities; their personal and other identifying data may be excluded (deleted altogether or blacked out) from the files prepared to be transferred abroad, including by editing pre-made copies of records of interrogation and other records.[2] This approach is consistent with the principles of proportionality and necessity and data protection requirements.

themselves having either access to the relevant information system or technical capability of establishing to what specific subscribers the sessions of a certain IP address relate.

[1] *Die internationale Rechtshilfe in Strafsachen: Wegleitung* [International legal assistance in criminal matters: Guidance]: 9. Aufl. 2009 (Rechtsprechung Stand Mai 2010) (Bern: Bundesamt für Justiz, Fachbereich Rechtshilfe, 2009): Ziff. 2.1.3, S. 17.

[2] A similar procedure is prescribed by art. 2 of the Regulation of the Federal Council of the Swiss Confederation on International Legal Assistance in Criminal

In many cases, the subscriber is registered under fictitious personal data, and the address indicated by him or her either does not exist, or the person of interest does not reside there; or the criminals use unwitting people's compromised bank or personal data for cover (identity thefts), or the equipment or device of the user being investigated for possible involvement in the offence had been infected with malware, or the persons who cashed out or transferred the stolen money or goods are just "mules". To fill in evidence gaps in such cases, one carries out questionings of witnesses and suspects, confrontations, seizure of equipment and computer forensic examinations.[1]

If the citizens concerned are persons who provide or provided confidential assistance to the authorities engaged in operational search activities, this is explicitly communicated to the RF central authority for international legal and law enforcement assistance in the manner established by law (art. 21 of the Federal Law "On operational search activities"). At the same time, for example, if such persons provided their personal data or bank details for the commission of crimes, their actions may contain elements of crimes, for instance, proscribed by art. 174 of the RF Criminal Code.

If, in the course of consideration or execution of a foreign request by Russian authorities, one discovers the elements of a crime falling under the jurisdiction of the Russian Federation (arts. 11–12 of the RF Criminal Code), in particular, if there is information about the presence of a person involved in the crime on the territory of the Russian Federation, Russian authorities normally initiate the transfer to Russia from the requesting foreign authority of copies of materials of the relevant foreign criminal case file, including statements or other crime reports, documentary evidence of damage to victims (bank statements, etc.), computer forensic expert opinions, samples of malicious software, by way of legal or law enforcement assistance,

Matters of 24 Feb. 1982 (IRSV) ("Removal of data"): If a document contains data that may not be transferred abroad, the executing authority shall make a copy or a photocopy from which the data to be kept secret have been omitted. It notes the fact, the place and the reason for the omission on the document and certifies that the document otherwise corresponds in all parts to the original. The same applies *mutatis mutandis* to other information carriers.

[1] *Methodological recommendations for exercising prosecutorial supervision over the execution of laws in the investigation of crimes in the field of computer information* (Moscow: Prosecutor General's Office of the Russian Federation, 2013), 25 p.

in order to resolve the issue of instituting criminal proceedings and/or initiating a criminal intelligence case in the Russian Federation, and, especially if the Russian Federation refuses to extradite the accused to the foreign state, it is expedient to initiate the transfer of his or her criminal prosecution to the Russian Federation.[1]

When organizing domestic pre-investigation probes and investigations into such facts, only on the basis of an initial foreign request for the conduct of certain procedural actions, it should be carefully weighed, to what extent the performance of actions not requested by foreign partners, for example, an interrogation of a suspect, within those own domestic investigations, would contradict the interests of a foreign investigation and the requirements for confidentiality of the fact of existence and substance of a foreign request, where possible, also by way of coordination, preliminary consultations and approvals with the foreign initiators of the request.

In 2021, the second edition of the Practical Guide for Requesting Electronic Evidence across Borders, jointly prepared by the UN Office on Drugs and Crime, the UN Security Council's Counter-Terrorism Committee Executive Directorate and the International Association of Prosecutors in cooperation with a number of structures of the European Union, was released (for law enforcement and judicial use only), representing to date the most comprehensive guidebook for law enforcers and judiciary, containing the algorithm of collecting electronic evidence in international cooperation, detailed information on national and international legal frameworks in force in this field, rules of key ICT service providers concerning their processing of requests from foreign competent authorities for preservation and production of electronic evidence, including their voluntary and emergency disclosure without a request for international legal assistance, the legal capacities of countries for fulfilling foreign requests for monitoring and recording (real-time interception[2]) of communications. Information regarding the modes

[1] Recommendation No. R (85) 10 of the Committee of Ministers to Member States concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications (Adopted by the Committee of Ministers on 28 June 1985 at the 387th meeting of the Ministers' Deputies) (para. 5).

[2] See also: Recommendation No. R (85) 10 of the Committee of Ministers to Member States concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the

of data preservation and production established by states and/or providers is periodically updated and supplemented. The Guide also highlights some challenges and practical solutions concerning the admissibility of e-evidence, its presentation in court, encryption, "cloud jurisdiction", virtual private and peer-to-peer networks, proxy servers, the quasi-judicial role of service providers, human rights aspects of the circulation of electronic evidence, provides templates and model request forms.[1]

The extensive EU country material on electronic evidence, including the regimes for its retention and preservation, receipt and provision from abroad, is contained in "Fiches Belges" database, a tool of the European Judicial Network.[2]

In 2019, the Committee of Ministers of the Council of Europe adopted Guidelines on electronic evidence in civil and administrative proceedings, which are also relevant for use in criminal proceedings.[3]

§ 2. Cross-Border Access to Information Systems, Information and Telecommunications Networks and Data for the Purpose of Gathering Electronic Evidence. International Information Security

Cyberspace includes a number of levels (layers), the central of which is the logical (virtual, digital) level that has no material geographic boundaries. At the same time, the physical, technological substrate (carrier) of cyberspace is comprised of the ICT infrastructure, hardware and software, geographically localized within particular states, which includes, among others, the equipment of end-users (they, in turn, constitute the social layer), as well as ICT

interception of telecommunications (Adopted by the Committee of Ministers on 28 June 1985 at the 387th meeting of the Ministers' Deputies).

[1] *The Practical Guide for Requesting Electronic Evidence across Borders* (Vienna: United Nations, 2021), 241 p.

[2] Fiche Belge on electronic evidence. URL: https://www.ejnforum.eu/cp/e-evidence-fiche/223/0, accessed Dec. 12, 2023.

[3] Guidelines CM(2018)169-add1final of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings (Adopted by the Committee of Ministers on 30 Jan. 2019, at the 1335th meeting of the Ministers' Deputies), Explanatory Memorandum.

service providers and other data custodians having the concrete "nationality".[1]

The exercise of extraterritorial jurisdiction to enforce in cyberspace is associated with the need to comply with the fundamental international legal principles in it.[2]

State sovereignty and international norms and principles that flow from sovereignty (such as non-intervention or non-interference in the internal affairs of other States) apply to State conduct of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory.[3]

Apart from the jurisdictional criterion of the location of information infrastructure objects (information systems and information and telecommunications networks) in the internal geographic space of the state, there also exist grounds for establishing and exercising prescriptive and enforcement state jurisdiction in the information

---

[1] See also: Д.В. Красиков, Н.Н. Липкина, *Принцип территориального суверенитета и концепция делимитации юрисдикций государств в киберпространстве: монография* [The principle of territorial sovereignty and the concept of delimitation of states' jurisdictions in cyberspace: monograph] (Саратов: ИЦ «Наука», 2021), 153 p.; J. Wasilewski, *Cyberprzestępczość — wybrane aspekty prawnokarne i kryminalistyczne: praca doktorska* [Cybercrime: selected criminal law and criminalistics aspects: doctoral thesis] (Białystok: Uniwersytet w Białymstoku, 2017), 428 s.

[2] See in more detail: П.А. Литвишко, *"Трансграничные оперативно-разыскные мероприятия и следственные действия в свете последних изменений антитеррористического законодательства России"* [Cross-border operational search measures and investigative actions in the light of recent changes in the counter-terrorism legislation of Russia], in Оптимизация деятельности органов предварительного следствия и дознания: правовые, управленческие и криминалистические проблемы: сборник научных статей Международной научно-практической конференции / под ред. И.П. Можаевой (М.: Академия управления МВД России, 2017), pp. 352–358.

[3] UN General Assembly Resolution 73/27 of 5 Dec. 2018 "Developments in the field of information and telecommunications in the context of international security" reaffirming the set of international rules, norms and principles of responsible behaviour of States, enshrined in the reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, concerning the applicability of international law to State use of ICTs.

See also: Е. Зиновьева, С. Шитьков, "Цифровой суверенитет в практике международных отношений" [Digital sovereignty in the practice of international relations], *Международная жизнь* 3 (2023), pp. 38–51; С.В. Коростелёв, "Проблема определения объема суверенных полномочий государства в цифровую эпоху" [The problem of determining the scope of sovereign powers of the state in the digital era], *Управленческое консультирование* 6 (2020), pp. 41–49.

space with respect to computer data stored, transmitted or otherwise processed using information systems (servers) and communications networks located in other countries. These grounds can be the following: the "targeting criterion", that is the orientation of such information resources towards the territory of the state (which may be inferred from the language, payment currency, options offered for delivering goods or providing services, domain name, etc. used on these resources), interactivity of the portal (website), factual consequences of its operator's intentional actions from abroad that unfold on the territory of the state, as well as the accessibility of these information resources from the territory of the state (the last one *per se*, as a rule, is not recognized as sufficient). These criteria, in addition to the geographical criterion, were developed mainly by international and national private law,[1] and are reflected in the materials of the interpretation of the 2001 Budapest Convention on Cybercrime.[2]

The main legal acts that determine the jurisdiction of the Russian Federation (both substantive (prescriptive) and procedural (enforcement)) in the information space, are the following.

The definition of the information infrastructure of the Russian Federation is given by the strategic planning document, Decree of the President of the Russian Federation of 5 December 2016 No. 646 "On Approval of the Doctrine of Information Security of the Russian Federation" (para. 2), as "a combination of informatization objects, information systems, Internet websites and communication networks located in the territory of the Russian Federation, as well as in the territories under the jurisdiction of the Russian Federation or

[1] J. Worona, *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy: rozprawa doktorska* [Cyberspace and international law. Status quo and prospects: doctoral dissertation] (Białystok: Uniwersytet w Białymstoku, 2017), s. 80, 84, 97–99, 104–106, 137–138; J. Worona, *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy* [Cyberspace and international law. Status quo and prospects: doctoral dissertation] (Warszawa: Wolters Kluwer, 2020), 488 s.

[2] 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). This 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.

used under international treaties to which the Russian Federation is a party".[1]

Federal Law of 31 July 2020 No. 259-FZ "On Digital Financial Assets, Digital Currency and on Amendments to Certain Legislative Acts of the Russian Federation" (art. 14) determines that the objects of the Russian information infrastructure encompass domain names and network addresses located in the Russian national domain zone, information systems, the technical means of which are located on the territory of the Russian Federation, and complexes

[1] There are a number of legal acts regulating the issue of data localization.

In accordance with para. 31 of the Decree of the President of the Russian Federation of 9 May 2017 No. 203 "On the Strategy for Development of the Information Society in the Russian Federation for 2017–2030", in order to protect data in the Russian Federation, it is necessary, among others, to ensure the processing of data on Russian servers with electronic interaction of persons located on the territory of the Russian Federation, as well as the transfer of such data on the territory of the Russian Federation using communication networks of Russian operators.

According to art. 18 of Federal Law of 27 July 2006 No. 152-FZ "On personal data", when collecting personal data, including through the use of the Internet, the operator is obliged, as a general rule, to ensure recording, systematization, accumulation, storage, clarification (update, change), and extraction of personal data of citizens of the Russian Federation with the use of databases located on the territory of the Russian Federation. The RF Code of Administrative Offences (art. 13.11(8) (violation of the legislation of the Russian Federation in the field of personal data)) establishes administrative liability for failure by the operator to fulfill this obligation.

According to art. 13 of Federal Law of 27July 2006 No. 149-FZ "On information, information technologies and information protection", technical means of information systems used by state bodies must be located on the territory of the Russian Federation. Operators of state information systems should not allow, when operating information systems, to use databases and technical means situated outside the territory of the Russian Federation that are not part of such information systems; when operating information systems, they are obligated to use computing capacities of a hosting provider who deploys technical means used for providing computing capacity to place information in the information system permanently connected to the Internet, on the territory of the Russian Federation. In addition, operators of state information systems, when creating or operating information systems, as well as interacting in an electronic form, inter alia, with citizens (natural persons) and organizations, are not entitled to use information systems and/or programs for electronic computing machines functioning through the use of the Internet, that belong to foreign legal persons and/or foreign nationals, except for cases established by the RF Government. Violation of said obligation entails administrative liability (art. 13.27.1 (Violation of the requirement to place technical means of information systems on the territory of the Russian Federation) of the RF Code of Administrative Offences).

of software and hardware means located on the territory of the Russian Federation; user equipment located on the territory of the Russian Federation.

For the purposes of art. 5 (state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation) of the Federal Law of 26 July 2017 No. 187-FZ "On the Security of the Critical Information Infrastructure of the Russian Federation", "information resources of the Russian Federation" are comprised of "information systems, information and telecommunication networks and automated control systems located on the territory of the Russian Federation, in diplomatic missions and (or) consular posts of the Russian Federation".[1]

Federal Law of 1 July 2021 No. 236-FZ "On the Activities of Foreign Persons on the Information and Telecommunications Network "Internet" in the Territory of the Russian Federation" (informally, the law on "landing" of foreign IT companies in Russia) (art. 4), regulating the problem of localization of data,[2] gives a definition of a foreign person operating on the Internet in the territory of the Russian Federation, against whom compulsory enforcement measures may be applied to make it comply with the requirements of the legislation of the Russian Federation.

Laws and by-laws in the field of communications and information referred to in this work establish the relevant obligations of foreign organizations and foreign citizens, who are determined based on the criterion of their services or other activities being directed at the target audience in the Russian Federation; some of those duties consist in identification and authentication of users and storage of information exclusively in the territory of the Russian Federation (data localization) (for example, arts. 10^{1}, $10^{2\text{-}1}$, 10^{3}–10^{7} (obligations of

[1] The Law contains the incomplete list of state foreign missions (only diplomatic missions and consular posts). See, e.g.: the Federal Law "On the Public Prosecutor's Office of the Russian Federation" (art. 39^{1}), which contains a complete list of state foreign missions of the Russian Federation ("diplomatic missions and consular posts of the Russian Federation, missions of the Russian Federation to international organizations, other official representations of the Russian Federation and representations of federal executive bodies located outside the territory of the Russian Federation").

[2] Counter-Terrorism Committee Executive Directorate (CTED). *The State of International Cooperation for Lawful Access to Digital Evidence: Research Perspectives. CTED Trends Report.* January 2022, 33 p.

the organizer of information dissemination on the Internet, hosting provider and some other custodians) of the Federal Law of 27July 2006 No. 149-FZ "On information, information technologies and information protection"), and the corresponding liability for their violation (Ch. 13 (administrative offences in the field of communications and information) of the RF Code of Administrative Offences).[1]

The substantive jurisdiction of states in relation to relevant acts in the information space (in particular, the establishment of mandatory territorial jurisdiction based on the criteria of the physical presence of the offender in the country's territory or the use of the information system in the country's territory when committing an offence) is regulated by particular provisions of the sources of European law: the directives of the European Parliament and Council of the European Union of 2019 on Combating Fraud and Counterfeiting of Non-Cash Means of Payment,[2] of 2015 (as amended in 2018) on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing,[3] of 2013 on Attacks

[1] See on the Belgian court ruling regarding the Skype messenger located in Luxembourg: *Cybercrime Judicial Monitor*. Issue 5 — December 2019 (The Hague: Eurojust, 2019), pp. 6–8; *The Practical Guide for Requesting Electronic Evidence across Borders* (Vienna: United Nations, 2021), p. 78.

The essence of the decisions of the Supreme Court of Belgium regarding "Yahoo!" on requests for subscriber information (2015) and regarding "Skype" on requests for content data (2019) was subsequently reflected in the provisions of the Belgian Criminal Procedure Code on the obligations of providers rendering services in Belgian territory to comply with Belgian warrants for the production of evidence.

See, e.g.: "Facebook погасил в России штрафы на 17 млн рублей" [Facebook paid out its 17 million rubles fines in Russia], *Ведомости*, 19 Dec. 2021. URL: https://www.vedomosti.ru/business/news/2021/12/19/901441-facebook, accessed Mar. 6, 2022.

[2] Directive (EU) 2019/713 of the European Parliament and of the Council of 17 Apr. 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA (art. 12).

The preparatory materials for this directive (Procedure 2017/0226/COD) reflect the process of resolving the problem of a positive conflict of territorial jurisdictions of the EU countries based on the criteria of the physical presence of the offender in the country's territory or use of the information system in the country's territory when committing an offence.

[3] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/

against Information Systems,[1] as well as the Council Framework Decision of 2008 on Combating Certain Forms and Expressions of Racism and Xenophobia by means of Criminal Law.[2]

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.

At the persistent requests of the Russian delegation's members at the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, who also participated in the work on the said UNODC Model Law, this formula for determining a requested "touchpoint state",[3] in a somewhat reduced form, along with the criterion of data storage location (location of the ICT device, computer system in the territory of the requested state), was included into the draft convention articles dedicated to international cooperation.[4]

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

EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Consolidated text with EEA relevance).

[1] Directive 2013/40/EU of the European Parliament and of the Council of 12 Aug. 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (art. 12).

[2] Council Framework Decision 2008/913/JHA of 28 Nov. 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law (art. 9).

[3] "A touchpoint describes the connection of a service provider with its users. Therefore, if a subscriber's registration information or IP address resolves to a specific State, this means that State is the touchpoint." (*The Practical Guide for Requesting Electronic Evidence across Borders* (Vienna: United Nations, 2021), p. 241.)

[4] 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. URL: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home, accessed Apr. 14, 2023.

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.[1]

The location of data (servers) is actually of lesser value than the location of a service provider/data custodian having possession, control or custody of the sought data, or of the provider's operations (storing, transmitting or otherwise processing the data) in the cloud computing environment, where it is normally hard or altogether unfeasible even for the service provider themselves to identify the exact location of data flows (the "loss of location" problem). Therefore, the way for determining a requested state party solely based on the data storage location is misplaced and not consistent with the current national practices of requesting this type of judicial assistance from states, whose "nationality" the relevant data custodian has. A requesting authority is almost never in a position to know where the service provider may store or otherwise process their data, on what servers, that may be situated anywhere all over the world.

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 the 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 pass.

Substantive criminal jurisdiction of the Russian Federation in respect of offences at hand can be asserted only if they fall under the provisions of arts. 11–12 of the RF Criminal Code, and its procedural criminal jurisdiction can be exercised only if there are grounds enshrined in arts. 2–3 RF CPC.[2] Determined on a general basis are

[1] 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.

[2] See also: *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* / Ed. by M.N. Schmitt, L. Vihul (Cambridge: Cambridge University Press, 2017), pp. 51–78.

also territorial investigative and court jurisdictions (arts. 32 and 152 RF CPC).

Contrary to the popular belief that there are no statutory impediments to direct transborder communications, including via telecommunications, between criminal investigators and private individuals (potential witnesses etc.) who are abroad on a voluntary basis and which do not involve any procedural actions, in reality, such contacts are generally not considered acceptable outside the framework of international legal or law enforcement assistance because it may be a violation of the sovereign territory of a foreign state.

Countries generally tend to regard remote "intangible" activities of representatives of a foreign state carried out from within its territory and physically reaching the persons and objects that are known to be located in those countries as activities undertaken within their own territory. Such activities include cross-border contacts via any telecommunication networks (electromagnetic systems): terrestrial (landline, cable, for example, fiber-optic communications, radio relay, tropospheric scatter and other mobile (wireless) radio communications), space (satellite) radio communications, in other words, for instance, by telephone, video conferencing, e-mail, social media, instant messaging on the Internet with persons knowingly staying and using relevant end-point equipment on the territory of the country concerned.[1]

---

[1] C.Y.M. Paulussen, *Male Captus Bene Detentus? Surrendering suspects to the International Criminal Court* (Tilburg University, Intersentia, 2010), pp. 45–47, 278–279, 403; A. Deeks, "An International Legal Framework for Surveillance", *Virginia Journal of International Law* 55:2 (2015), pp. 300 and 303–312; S. St. Vincent, "*International Law and Secret Surveillance: Binding Restrictions upon State Monitoring of Telephone and Internet Activity*", pp. 2–4, 6, Center for Democracy & Technology, 4 Sept. 2014. URL: https://cdt.org/insight/international-law-and-secret-surveillance-state-monitoring-of-telephone-and-internet-activity/; А.Г. Волеводз, *Правовое регулирование новых направлений международного сотрудничества в сфере уголовного процесса* [Legal regulation of the new directions of international cooperation in the field of criminal procedure] (М.: Юрлитинформ, 2002), p. 312; А.Г. Волеводз, *Противодействие компьютерным преступлениям: правовые основы международного сотрудничества* [Counteraction of computer crimes: legal foundations of international cooperation] (М.: Юрлитинформ, 2002), p. 240; И.М. Нурбеков, *Тактико-организационные особенности взаимодействия при расследовании преступлений международного характера: дис. ... канд. юрид. наук* [Tactical and organizational particularities of interaction in the investigation of crimes of an international character: PhD in Law dissertation] (М., 2010), pp. 223–226.

Thus, the legal fiction of the "territorialization" of cyberspace is applied.[1]

The international treaties regulating investigative and judicial cross-border hearings to obtain testimony by video or telephone conference, the parties' declarations and reservations thereto, the international legal principles of sovereign equality of states and non-interference in the internal affairs of other states imply the prohibition for carrying out these actions if the country in the territory of which their participant (interviewed, identifying, being identified, etc.) is located does not permit these actions, even in the cases when there is a relevant request or consent of the participant himself and there is no need for the assistance of an "intermediary" acting in this country (its official, or consul of the sending state, lawyer, notary, or any other private commissioner) who traditionally fulfills functions of ensuring, proving and certifying the participant's identity, the fact of his voluntary participation, and other conditions.

This approach to the physical extraterritorial effect of telecommunications[2] is reflected, for example, in art. 20 of the 2000

See also: Criminal Procedure Code of Georgia (art. 113(11–13) on cross-border interviews by electronic means of communication outside the procedure of international legal assistance with the consent of the relevant foreign state).

[1] Л.В. Терентьева, "Разграничение экстратерриториальной и территориальной юрисдикции в киберпространстве" [Delimitation of extraterritorial and territorial jurisdiction in cyberspace], *Право и цифровая экономика* 1(15) (2022), pp. 41–51.

[2] Wireless data transmission is carried out through electromagnetic radio waves which are oscillations of the electromagnetic field propagating through space which field, in turn, is one of the two forms of existence of the matter, along with the substance.

On the material nature of the electromagnetic field and related issues, see: А. Лукьянова, "Электронный официальный документ как предмет преступления, предусмотренного ст. 327 УК РФ" [An electronic official document as an object of a crime envisaged by art. 327 of the RF Criminal Code], *Уголовное право* 3 (2016), p. 59; Н.Н. Беломытцев, *"Криптовалюта как предмет хищения путем использования компьютерной техники"* [Cryptocurrency as an object of theft through the use of computer technology], in Использование криптовалют в противоправных целях и методика противодействия: материалы Международного научно-практического «круглого стола» (Москва, 25 апреля 2019 года) / под общ. ред. А.М. Багмета (М.: Московская академия Следственного комитета Российской Федерации, 2019), pp. 16–22; В.В. Бычков, С.В. Харченко, *"О понятии компьютерной преступности"* [On the concept of computer crime], in Противодействие киберпреступлениям и преступлениям в сфере высоких технологий: материалы Всероссийской научно-практической конференции (Москва, 10 декабря 2020 года) / Под общ. ред. Д.Н. Кожухарика

Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union and art. 31 of the 2014 Directive regarding the European Investigation Order in criminal matters, governing cross-border interception of telecommunications without the technical assistance of another member state whose territory is affected by the interception, by means of remote access, and providing for mandatory notification and substantial authority to the affected state to influence the progress and the results of the interception.[1]

These documents proceed from the premise that the intercepting state is or later becomes aware of the fact that the subject of the interception is, will be or has been during the interception, on the territory of the notified state, which serves as a condition for the intercepting state to notify unfailingly this other state and for the latter to have the corresponding powers.

In this regard, as well as in the context of cross-border hearings by video or telephone conference, the question arises as to the need to verify the location of the person in respect of whom these actions are planned. It may be argued that, in the absence of any indication to the contrary, and in particular if a person subject to remote questioning voluntarily declares that he or she is in the territory of the state whose authorities will conduct the questioning, the presumption of the location of the person within the territory of this state, and not abroad, should apply. Otherwise, these actions are to be carried out within the framework of international legal assistance (for example, in accordance with arts. 9–10 of the 2001 Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters) or unilaterally in agreement with a foreign state, where the person is staying, if the state in question allows such proceedings to be carried out outside the legal assis-

(М.: Московская академия Следственного комитета Российской Федерации, 2021), pp. 26–30.

[1] Explanatory report on the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union (comment on Title III); *Zasady obrotu prawnego z zagranicą w sprawach karnych w postępowaniu przygotowawczym* [Principles of legal interaction with foreign countries in criminal matters in preparatory proceedings] / pod red. E. Zalewskiego, K. Karsznickiego, A. Wiśniewskiej, C. Michalczuka (Warszawa: Prokuratura Krajowa, 2009), s. 22–25; Zákon ze dne 20. března 2013 č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních [Law on international judicial cooperation in criminal matters] (§§ 62–63).

tance procedure.[1](The legislation of the Russian Federation does not provide for such a possibility.)

There are proxy servers, VPN, TOR, SSL software technologies that allow to change the IP address of an Internet user, create dynamic and unrecognizable IP addresses, technologies for substituting (changing) a subscriber number or a unique identification code using SIP telephony, complicating or making the above-mentioned verification[2] impossible, which is why the requirement for its unconditional implementation in all cases seems unjustified.

If, upon the performance of a proceeding, it is discovered that the person in respect of whom it had been carried out, was in the territory of a foreign state during its conduct, this should not adversely affect the admissibility of the evidence thus obtained for the state that performed such a proceeding as the ultimate user in accordance with its national legislation, since it cannot be imputed to it that it committed a violation of the peremptory norms of international law — the principles of sovereign equality of states, non-interference in domestic affairs of another state, or the commission of any other internationally wrongful act.

It is obvious that apart from the interception of telecommunications, where the subscriber/end-user to be approached and interacted with or the terminal (but, of course, not "transit"[3])

---

[1] See, e.g.: art. 113(11-13) of the Criminal Procedure Code of Georgia (Interview procedure) ("A public prosecutor, or an investigator with the consent of a public prosecutor, shall be authorised to interview, remotely with the use of electronic means, a person staying within the territory of a foreign state without sending a request for legal assistance if interviewing a person using such procedure is permitted by a relevant international treaty of Georgia, the law of the state where this person is present, or/and by the clearly formed practice of this state. A person may not be interviewed in this manner if the person to be interviewed has not expressed a direct and explicit consent to be interviewed. A person may be questioned in this manner at the investigation stage as well").

[2] Since 2021, the RF Code of Administrative Offences has the dedicated art. 13.2.1 for this (Non-compliance by a telecom operator with the obligations relating to the transmission of a subscriber number and (or) a unique identification code in an unchanged form, to the termination of the provision of communications services and (or) traffic transit services and failure to connect to the system for ensuring compliance by telecom operators with the requirements for the provision of communications services and traffic transmission services in a public communications network).

[3] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* / Ed. by M.N. Schmitt, L. Vihul (Cambridge: Cambridge University Press, 2017), pp. 33–34 and 55–56 (data stored (at rest) v. data transmitted (in transit)).

equipment to be accessed is knowingly located on foreign soil, the same restrictions from the point of view of international law apply to all other possible cross-border online covert special investigative techniques (criminal intelligence operations) (in relation to Russia, such activities are listed in art. 6 of the Federal Law "On Operational Search Activities"),[1] involving interaction with the user or access to equipment, for example, a test purchase, infiltration, operational experiment (sting operation), use of persons providing confidential assistance to authorities carrying out operational search activities, special technical measures,[2] measures to lure the implicated user from abroad, while taking account of the circumstance that actual observance of such international legal limitations for domestic investigations is hardly practicable in a highly virtualized and mobile environment.

Such covert special investigative techniques, as cross-border observations or covert investigations, are associated with enhanced risks of unauthorized intrusion into the sovereign space of the requested state, therefore, when ratifying the 2001 Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, the Russian Federation made a reservation on the use of the right not to accept arts. 17 and 19 of the Protocol regulating these actions. Similar restrictions apply, under certain conditions, to the use of the Russian ICT infrastructure for the purpose of carrying out such actions.

However, the mentioned covert actions can, if necessary, be carried out within the framework of another type of legal assistance — joint investigations (art. 20 of the Protocol), as well as based on the provisions of many other international treaties of the Russian

[1] Special Investigative Techniques: Assessing the Need for Additional Regulation in the Council of Europe's Instruments of Legal Assistance in Criminal Matters: Discussion Paper by Mr Pyotr Litvishko (Russian Federation), PC-OC Mod Substitute Member, Strasbourg, 19 Aug. 2021 [PC-OC/PC-OC Mod/Docs PC-OC Mod 2021/PC-OC Mod (2021)04E]; Introductory Note to Discussion Paper PC-OC (2021)10EN.

[2] E.g., in virtual investigations by "government hacking", using loggers, such as IP Grabber (Grabify IP Logger), hardware and software keystroke loggers, sniffers, compromising electromagnetic emanations, or embedding exploits (backdoors).

Сбор и анализ цифровых следов преступления: практическое пособие [Collection and analysis of digital traces of a crime: practical manual] / С.В. Петраков, М.А. Гудкова, Д.П. Бащук, А.А. Тимофеев, Д.Н. Пигильдин, И.С. Бедеров, Д.О. Сорокин, А.В. Пытайло (СПб: Изд-во Санкт-Петербургской академии Следственного комитета, 2023), 96 p.

Federation, such as the Palermo (art. 20) and Merida (art. 50) conventions on special investigative techniques, including electronic surveillance and undercover operations, numerous agreements on law enforcement assistance in carrying out operational search activities (criminal intelligence operations), among which the most specialized are the 2018 Agreement on Cooperation of the CIS Member States in Combating Crimes in the Sphere of Information Technologies and the 2014 Protocol on Interaction of the CSTO Member States in Countering Criminal Activities in Information Sphere.[1]

In 2022, the 2007 UNODC Model Law on Mutual Assistance in Criminal Matters was updated with provisions on electronic evidence and supplemented with a special investigative technique "electronic surveillance", whose definition mentions "manipulation of messages, data or signals" and "any covert engagement in electronic communications with suspects involving undercover measures", which may include the use of online infiltrated agents and confidential informants.[2]

In 2021, the Council of Europe Cybercrime Convention Committee approved the terms of reference[3] for its new Working group on undercover investigations by means of computer systems and extension of searches.[4]

---

[1] See also on criminal intelligence cyber operations: Resolution of the Parliamentary Assembly of the Collective Security Treaty Organization of 19 Dec. 2023 No. 16-7.3 "On the Draft Model Guidance of the Competent Authorities of the CSTO Member States in the Sphere of Ensuring the Collective Security by Operational Search Activities".

[2] 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) (sec. 27).

[3] Terms of reference (document T-CY (2021)19 of 15 Nov. 2021) for the T-CY Working group on undercover investigations by means of computer systems and extension of searches.

[4] As applied to the Russian legislation on criminal proceedings and operational search activities in force, in a general sense, by a search in information systems and telecommunications networks should be understood not a search in some premises or other physical objects, or inspection of premises, but other investigative actions or operational search measures, namely inspection and seizure (with copying onto a medium) of electronic messages or other communications transmitted over telecommunications networks, capturing information from technical communications channels or obtaining computer information.

One should also distinguish between two types of a remote search: extended search, associated with extending an inspection from the initial ICT device onto other devices connected via network with that initial device, on the one hand, and

Taking into account international practice and the convergence of the institutions of preliminary investigation and operational search activities (reflected, in particular, in the 2001 Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters), and for the purpose of ensuring the admissibility of evidence collected in this manner, it is recommended that, when there is an initiated criminal case (criminal proceedings, as opposed to criminal intelligence operations), requests for the conduct of these covert activities should be sent through the use of legal (judicial), and not law enforcement (police-to-police) assistance.

At the 74th session of the UN General Assembly (2019), the UN Secretary-General presented a report on the challenges faced by Member States in countering the use of information and communications technologies for criminal purposes. According to the report, a number of states parties to the Budapest Convention on Cybercrime keep voicing concerns about unilateral direct cross-border access by states to data that are not in the public domain.[1]

Nevertheless, the current case law of individual European countries shows that their high courts tend to view as not contrary to international law and to the territorial sovereignty of other states, lawful online searches in relation to computer data stored on servers or in cloud storage facilities abroad.[2]

Significant attention to restrictions and prohibitions on cross-border access to persons, information systems and data, including

a remote search (where there is a connected "remote workstation" in the searched place, Remote Desktop Protocol (RDP) brute forcing, etc.), that is generally carried out in a covert manner, without the participation of the owner of the ICT device concerned and without physical access to that device ("government hacking"), on the other.

See: J. Wasilewski, *Cyberprzestępczość — wybrane aspekty prawnokarne i kryminalistyczne: praca doktorska* [Cybercrime: selected criminal law and criminalistics aspects: doctoral thesis] (Białystok: Uniwersytet w Białymstoku, 2017), s. 372–402; *Способы получения доказательств и информации в связи с обнаружением (возможностью обнаружения) электронных носителей: учебное пособие* [Methods of obtaining evidence and information in connection with discovery (possibility of discovery) of electronic media: study aid] / В.Ф. Васюков, Б.Я. Гаврилов, А.А. Кузнецов [и др.]; под общ. ред. Б.Я. Гаврилова (М.: Проспект, 2017), pp. 77–79.

[1] *Countering the use of information and communications technologies for criminal purposes: Report of the Secretary-General* (UN Doc. A/74/130 of 30 July 2019).

[2] *Cybercrime Judicial Monitor.* Issue 5 — December 2019 (The Hague: Eurojust, 2019), pp. 19–20 and 23.

cross-border searches, is dedicated in the Online Investigative Principles for Federal Law Enforcement Agents published in 1999 by the US Department of Justice.[1]

Indicative of different approaches of the states concerned to the legality of cross-border searches and seizures of data in information systems and networks is the well-known criminal case of the early 2000s of the United States against hackers A. Ivanov and V. Gorshkov, who were lured by US agents from Russia to the United States by way of an undercover action on the Internet, where, as part of another sting operation, they gave away access to their Russian information resources; whereupon these resources were subjected to unilateral cross-border search and seizure. Ivanov and Gorshkov were convicted and sentenced in the United States, and the Russian investigative authorities, in turn, initiated a criminal case against the US special agent, who carried out the said search and seizure, on the charges of illegal access to computer information committed by a person using his official position.[2]

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

---

[1] *Online Investigative Principles for Federal Law Enforcement Agents*. Prepared by the Online Investigations Working Group. Final Version (November 1999), 93 p. URL: https://info.publicintelligence.net/DoJ-OnlineInvestigations.pdf.

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

See in more detail: S.W. Brenner, "Law, Dissonance, and Remote Computer Searches", *North Carolina Journal of Law & Technology*, vol. 14, issue 1 (2012), pp. 43–92; Ph. Attfield, *"United States v Gorshkov Detailed Forensics and Case Study; Expert Witness Perspective"*, in Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05) (2005), 22 p.; N. Seitz, "Transborder Search: A New Perspective in Law Enforcement?", *Yale Journal of Law & Technology* 7 (2004–2005), pp. 23–50; J.L. Goldsmith, "The Internet and the Legitimacy of Remote Cross-Border Searches", *University of Chicago Public Law & Legal Theory Working Paper* 16 (2001); *Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers": Discussion paper*, prepared by Joseph J. Schwerha, Strasbourg, 15 January 2010, Project on Cybercrime www.coe.int/cybercrime; *United States v. Ivanov*. UNODC Sherloc Case Law Database. URL: https://sherloc.unodc.org/cld/en/case-law-doc/cybercrimecrimetype/usa/2001/united_states_v._ivanov.html, accessed Dec. 14, 2023.

the grounds of the victim's citizenship, direction of the act against the interests of the state).[1]

For the purpose of preventing unilateral cross-border covert cyber operations by establishing precise requirements for filing an international request for legal or law enforcement assistance to carry them out, for the content of such a request, as well as for its execution, at the initiative of the Prosecutor General's Office of the Russian Federation, the Russian Federation has introduced a dedicated article into the draft comprehensive international convention on countering the use of information and communications technologies for criminal purposes,[2] designed to provide granular and self-contained regulation for deploying covert special investigative

[1] See on US courts determining the jurisdiction according to the location of the damage caused through crimes committed abroad and the extraterritorial effect of the US criminal law with regard to the relevant corpora delicti: D.L. Buresh, "The Computer Crimes of Vasiliy Gorshkov and Alexey Ivanov", *Journal of Advanced Forensic Sciences*, vol. 1, issue 2 (2022), pp. 27–32.

See also: *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* / Ed. by M.N. Schmitt, L. Vihul (Cambridge: Cambridge University Press, 2017), pp. 11–29 and 51–78.

[2] Modelled on the relevant provisions of the UNTOC and UNCAC as well as the 2007 UNODC Model Law on Mutual Assistance in Criminal Matters as amended in 2022.

"Article […] Special investigative techniques

1. For the purpose of effectively combating offences covered by this Convention, identifying and tracing instrumentalities and proceeds of such offences, or property the value of which corresponds to such proceeds, each State Party shall, to the extent permitted by the fundamental principles of its domestic legal system and under the conditions prescribed by its domestic law, take the necessary measures to allow for the use of covert special investigative techniques, such as electronic or other forms of surveillance, online undercover operations or extended searches by its competent authorities in its territory or in the territory under its jurisdiction, and to ensure that the evidence collected through the use of such measures is admissible in judicial proceedings.

2. If there are reasonable grounds to believe that a serious offence covered by this Convention has been, is being or is likely to be committed, a State Party shall, within its possibilities and under the conditions prescribed by its domestic law, at the request of another State Party for legal or law enforcement assistance, and where necessary jointly with the competent authorities of that other State Party, carry out covert special investigative techniques, such as electronic or other forms of surveillance, online undercover operations or extended searches by its competent authorities in its territory or in the territory under its jurisdiction, and provide the evidence collected through the use of such measures to the requesting State Party.

3. A request made in accordance with paragraph 2 of this article shall specify:

(a) Particular individuals, entities, locations or devices, instrumentalities, proceeds or property subject to the requested measure;

techniques, as compared to the non-self-executing régime envisaged by the Palermo and Merida Conventions framework (arts. 20 and 50 respectively, that generally apply by reference to other international agreements and arrangements). The Russian Federation pointed out the need to prevent — through the provisions of this article — unilateral cross-border surreptitious cyber operations, which aim to bypass the bilateral coordination, risk generating blue-on-blue undercover activities, abuses of human rights, tensions between states because of them undertaking unilateral cyber operations of this kind, and generally run counter to international law. Otherwise this field also risks to remain a grey zone in international law enforcement.

It is the highly anonymous and obfuscated nature of cyberspace that makes the proactive deployment of cross-border online undercover operations indispensable for law enforcement to be able to identify international perpetrators of child abuse, drug or arms trafficking and many others, collect electronic evidence of their misdeeds and bring them to justice. Undercover operations represent a separate tool for collecting evidence for criminal justice purposes, among others, and cannot be conflated with just one type of electronic surveillance in the form of covert real-time interception of telecommunications or joint investigations.[1]

(b) Particular network access, equipment or service level identifiers subject to the requested measure;

(c) Where that person(s), entity or equipment, instrumentalities, proceeds or property are, or are suspected to be, located in the requested State or any relevant service provider is located or established in, or, through data processing activities, otherwise operates from the requested State;

(d) The type of covert special investigative technique for which the assistance is sought, and the persons, service providers or entities that may be required to assist in its implementation;

(e) The duration for which the assistance is sought;

(f) The nature of the data or information that is expected to be collected, and specifically the links to serious crime investigated in the requesting State, as well as justification of the prosecution."

[1] 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. URL: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home, accessed Apr. 14, 2023.

Still, such attempts to establish minimum global rules of the game hit a roadblock of resistance on the part of some cyber powers, who are allegedly interested in keeping their unilateral proactive cross-border cyber operations of "government hacking" in a legal grey zone.

In order 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, the Prosecutor General's Office of the Russian Federation has presented a draft "blocking" (see more on this term below) federal law which was filed with the State Duma of the Federal Assembly of the Russian Federation in 2023.[1] If the law is ad-

[1] Draft 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.

"Article 294[1]. Unlawful performance of investigative, other procedural actions and operational search measures in the territory of the Russian Federation

The conduct by a foreign official or an official of a public international organization (international authority), in which the Russian Federation does not participate, of an action in the territory of the Russian Federation that in accordance with the legislation of the Russian Federation constitutes an investigative or other procedural action, or operational search measure, in the interests of a foreign state, public international organization (international authority), in which the Russian Federation does not participate, including through the use of video conferencing systems or other means of communication with a person who is present in the territory of the Russian Federation, in violation of the procedure for interaction with foreign and international law enforcement and judicial authorities provided for by an international treaty and (or) the legislation of the Russian Federation, and for purposes contrary to the interests of the Russian Federation, in the absence of elements of crimes envisaged in articles 276 and 284[3] of the present Code, — shall be punished by a fine in the amount from five hundred thousand to two million rubles or by deprivation of liberty for a term of up to five years."

The objects of the acts stipulated by draft art. 294[1], on the one hand, and arts. 276 (espionage) and 284[3] (provision of assistance in executing decisions of international organizations, in which the Russian Federation does not participate, or foreign state authorities) of the RF Criminal Code, aimed mainly at countering the intelligence activities of special services of foreign states, on the other hand, differ significantly. The corpus delicti provided for by draft art. 294[1] of the RF Criminal Code constitutes a publicly dangerous violation of the international

legal procedure for interaction between law enforcement and judicial authorities, specified in an international treaty and (or) the legislation of the Russian Federation (the RF Criminal Procedure Code and Federal Law of 12 Aug. 1995 No. 144-FZ "On Operational Search Activities"), when carrying out relevant actions or measures on the territory of the Russian Federation for purposes contrary to the interests of the Russian Federation; and the purpose of causing damage to national security may not necessarily be pursued. The objects of draft art. 294^1 of the RF Criminal Code are public relations aimed at protecting the interests of the Russian Federation from interference in its internal affairs in the field of administration of justice and pre-trial proceedings, from violation of the procedure for interstate interaction in this area, of territorial sovereignty as a component of the foundations of the constitutional system of the Russian Federation.

The subjects of the crime envisaged by the draft are the relevant officials, regardless of their citizenship.

The interests of the Russian Federation mentioned in the draft article are mainly reflected in strategic planning documents, such as the National Security Strategy of the Russian Federation, the Information Security Doctrine of the Russian Federation, the Fundamentals of the State Policy of the Russian Federation in the field of International Information Security, and the Concept of Foreign Policy of the Russian Federation, approved by decrees of the President of the Russian Federation.

At the same time, the provision of assistance by citizens of the Russian Federation in connection with the performance of actions referred to in draft Article 294^1 of the RF Criminal Code, such as transfer, including with the use of information and telecommunication networks (including the Internet), or collecting information for transfer, is covered by arts. 275 (state treason) and 275^1 (cooperation on a confidential basis with a foreign state, international or foreign organization) of the RF Criminal Code.

The legislation of foreign countries used in elaborating the draft law contains separate criminalization of espionage and unrelated unauthorized activities of representatives of foreign authorities on the territory of these countries.

(See in more detail on foreign laws used in the drafting: P.A. Litvishko, *Non-Treaty Forms of Extraterritorial Judicial and Law Enforcement Activities*, in Collection of Materials on International Cooperation of the Investigative Committee of the Russian Federation (Moscow: Prospekt, 2016), pp. 132–173; П.А. Литвишко, *"О российских инициативах по противодействию противоправному сбору доказательств в киберпространстве представителями иностранных государств и международных органов"* [On Russian initiatives for countering unlawful collection of evidence in cyberspace by representatives of foreign states and international authorities], in Проблемы противодействия киберпреступности: материалы международной научно-практической конференции (Москва, 28 апреля 2023 г.) (М.: Московская академия Следственного комитета Российской Федерации, 2023), pp. 93–101.)

As regards art. 286 (exceeding of official powers) of the RF Criminal Code, the scope of such powers and the fact of their excess by a foreign official, as a general rule, are determined by the state of the official, which can also engage the immunity of its official from foreign criminal jurisdiction.

(See in more detail: *Analytical Guide to the Work of the International Law Commission. Immunity of State officials from foreign criminal jurisdiction*. URL: https://

opted, it will criminalize and penalize, among other things, actions unacceptable to Russia, provided for in art. 32(b) of the Budapest Convention on Cybercrime.

Apart from officers of law enforcement and judicial authorities of foreign states, defendants under art. 294[1] of the RF Criminal Code could be, under certain circumstances and with due regard to their immunities under international law, consular officers and diplomatic agents of foreign states' embassies and other missions in the Russian Federation, performing a hearing, including by video or telephone conference, service of documents or other proceedings by way of consular legal assistance in criminal matters in contravention of the procedure prescribed by art. 5(j) of the 1963 Vienna Convention on Consular Relations and/or other international treaties to which the Russian Federation is a party.

It is notable that under the draft federal law, methods and instrumentalities for the commission of such an offence include the use of video conference or other means of communication with a person (in the sense of law, a natural person, including those acting on behalf and/or in the interest of a legal person) who is present on the territory of the Russian Federation. Therefore, the constituent elements of the offence are absent where the law enforcement or judicial activities undertaken from overseas consist in interacting with a device, also in an automated mode, located on Russian soil, but not with a human being there. This is explained, firstly, by the enhanced intrusiveness inherent in the cross-border interference in human rights rather than in the functioning of equipment or software, and secondly, by the circumstance that such illegal access to and interaction with hardware or software can fall within and be classified under other provisions of the criminal law, like it was in the aforementioned case of Ivanov and Gorshkov.

Such norms also serve as an additional means of challenging the admissibility of evidence obtained in the way specified therein. However, it would be erroneous to presume in all cases the automatic undermining of the admissibility of evidence collected in such an illegal way, even if it contained elements of an internationally

legal.un.org/ilc/guide/4_2.shtml, accessed Dec. 15, 2023; П.А. Литвишко, "Возбуждение и расследование уголовного дела о преступлении, совершенном должностным лицом иностранного государства" [Initiation and investigation of a criminal case on a crime committed by an official of a foreign state], *Международное уголовное право и международная юстиция* 3 (2014), pp. 5–8.)

wrongful act, since the admissibility is determined by the interested ultimate user of this evidence, especially if they apply the so-called protective norms (*Schutznorm*), which allow the admissibility of evidence to be preserved in case of breach of international law, provided that the fundamental rights of the suspect or accused are not violated (prohibition of torture, right to defence, fair trial).[1]

The prevailing opinion in international law at the moment is that said cross-border remote access, search and seizure of data without the consent of the state in which this data is located, expressed in an international treaty or on a case-by-case basis, contravene the principles of territorial sovereignty (in particular, through interference with or usurpation of an inherently governmental function exclusively reserved to the territorial state under international law)[2] and non-interference in the internal affairs of another state, constitute an internationally wrongful act and may entail the inadmissibility of evidence collected in this way.[3] However, at the same time , there is an ongoing discussion about the need to reach international agreements on the legalization of such unilateral actions, as well as about the existence of situations that preclude their wrongfulness, when the fundamental principle of territoriality cannot be observed, for instance, where there is "loss of location" of the data when using cloud computing and anonymizing techniques, or law enforcers are mistaken in good

---

[1] B.-J. Koops and M. Goodwin, *Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities of International Law*, in Tilburg Law School Legal Studies Research Paper Series, No. 05/2016, p. 75.

See also on judicial evaluation of electronic evidence gathered abroad: *Cybercrime Judicial Monitor*. Issue 8 — June 2023 (The Hague: Eurojust, 2023) pp. 11–14.

[2] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / Ed. by M.N. Schmitt, L. Vihul (Cambridge: Cambridge University Press, 2017), pp. 11–29 and 51–78.

[3] Д.В. Красиков, *Территориальный суверенитет и делимитация юрисдикций в киберпространстве* [Territorial sovereignty and delimitation of jurisdictions in cyberspace], in Государство и право в новой информационной реальности: Сб. науч. тр. / РАН. ИНИОН. Центр социал. науч.-информ. исслед. Отд. правоведения; Рос. гос. ун-т правосудия. Каф. информационного права, информатики и математики; Отв. ред. Алферова Е.В., Ловцов Д.А. (М., 2018), pp. 99–111; Д.В. Красиков, "Экстратерриториальный доступ к информации: проблемы международного и внутригосударственного правового регулирования" [Extraterritorial access to information: problems of international and domestic legal regulation], *Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер.* 4: *Государство и право* 4 (2018), pp. 97–102.

faith as to the actual location of data, or under the "principle of ubiquity" of data.[1]

As regards the possibility of reaching international arrangements on said unilateral actions of a normative (treaty) rather than ad hoc character, it appears to be nonrealistic in the short and medium term, especially in a multilateral format. At the global level, the work on draft UN Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes in 2023 evidenced the lack of support with the majority of member states for inclusion of both an article analogous to art. 32(b) of the Budapest Convention, and even an article, which is actually classic for universal conventions, on covert special investigative techniques in cyberspace that were not, moreover, of a unilateral nature as drafted.

In the regional (2022 Second Additional Protocol to the Council of Europe Convention on Cybercrime) and even integrative European areas of trust (2023 EU Regulation on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings and Directive 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), the highest attainable level of cooperation comes down to allowing limited direct contacts of states parties with a foreign private sector of service providers to obtain data of interest.

This is also true for the most advanced level of bilateral arrangements in this field — executive agreements concluded pursuant to the US CLOUD Act.

Hence, any recognition and development as a treaty norm of states' rights and powers for a covert cross-border unilateral direct access to the data themselves stored or transmitted in information systems or networks of service providers, let alone in user ICT devices, seem to be a nonstarter in the short and medium terms.

---

[1] A.-M. Osula, *Remote search and seizure of extraterritorial data: PhD in law dissertation* (Tartu: University of Tartu Press, 2017), 96 p.; A.-M. Osula and M. Zoetekouw, "The Notification Requirement in Transborder Remote Search and Seizure: Domestic and International Law Perspectives", *Masaryk University Journal of Law and Technology*, vol. 11, No. 1 (2017), pp. 103–127; B.-J. Koops and M. Goodwin, *Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities of International Law*, in Tilburg Law School Legal Studies Research Paper Series, No. 05/2016, 102 p.

On the contrary, in order to prevent the situations at stake, starting from 2022, the Russian Federation has been introducing a relevant norm into bilateral intergovernmental agreements on cooperation in ensuring international information security. 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 (art. 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."[1]

When developing the documents for the Convention on Cybercrime, their authors highlighted risks of "friendly fire" for law enforcement cyber operations: "In addition to affecting individuals and third parties, transborder access could pose a risk to domestic and international law enforcement operations. Investigations often rely on secrecy and the cooperation of third parties. Transborder access could create situations where a law enforcement entity of another State fails to coordinate, data becomes unavailable to domestic law enforcement entities, or a suspect is notified of an investigation. As has occasionally happened, law enforcement entities within a State or from different countries could find themselves investigating each other because they mistake legitimate law enforcement activities for criminal activities."[2]

18 U.S. Code § 1952 criminalizes the use of the mail or any facility in interstate or foreign commerce in aid of racketeering enterprises. Under the UK criminal law (introduced in 1998) on conspiracy to commit offences outside England and Wales, any act done by means

[1] 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).

[2] *Transborder access and jurisdiction: What are the options? Report of the Transborder Group* adopted by the T-CY on 6 Dec. 2012. Strasbourg, 6 Dec. 2012, T-CY (2012)3, p. 16, para. 2.3.6; pp. 29–31, para. 4 (Scenarios of transborder access).

of a message (however communicated) is to be treated for the purposes of the condition of territoriality as done in England and Wales if the message is sent or received in England and Wales.[1]

At the same time, criminal jurisdiction claimed by the legislation of individual countries in respect of transit of communications passing through these countries, is assessed by lawyers as unjustifiably broad.[2]

Pursuant to the Home Office's Guidelines for authorities outside of the United Kingdom on Requests for Mutual Legal Assistance in Criminal Matters of 2012, "subject to the provisions of relevant bilateral or other international instruments, contact may be made with witnesses in the UK directly by letter, fax or telephone without informing the central authorities".[3] The later editions of these Guidelines fully reversed that provision: "Witnesses, victims, suspects and defendants [in the UK], must not be contacted directly [by letter, fax or telephone] unless UK law enforcement agencies have first been informed, except where that contact is direct service of process.[4] Once UK law enforcement has been notified and consented, the witness can be contacted directly".[5]

In 2015, in connection with the Litvinenko inquiry, the Ministry of Foreign Affairs of the Russian Federation issued an official statement to the effect that "…This is not the first time the British "public inquiry" has demonstrated such disregard for international and Russian law: it transpired during the hearings that its secretariat, in order to make enquires, repeatedly via means of communication contacted potential witnesses located in the Russian Federation without giving advance notice to the Russian authorities. Thereby they extended enforcement jurisdiction of a foreign State to the ter-

[1] Criminal Law Act 1977 (S. 1A inserted (4.9.1998) by 1998 c. 40, s. 5(1)).

[2] S.W. Brenner and B.-J. Koops, "Approaches to Cybercrime Jurisdiction", *Journal of High Technology Law*, vol. IV, No. 1 (2004), 46 p.; *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* / Ed. by M.N. Schmitt, L. Vihul (Cambridge: Cambridge University Press, 2017), pp. 33–34, 55–56 (data stored (at rest) v. data transmitted (in transit)).

[3] *Guidelines for authorities outside of the United Kingdom on Requests for Mutual Legal Assistance in Criminal Matters* of 14 Sept. 2012 (10th Ed.), p. 35.

[4] That is, a summons, judgment or other procedural documents.

[5] *Requests for Mutual Legal Assistance in Criminal Matters: Guidelines for Authorities Outside of the United Kingdom* of 23 Mar. 2015 (12th Ed.), p. 18; *Request for Mutual Legal Assistance in Criminal Matters: Guidelines for Authorities outside of the United Kingdom* (London: Home Office, March 2022), p. 23.

ritory of Russia without the latter's consent, violated its sovereignty and the fundamental international principle of non-interference in internal affairs. By the way, the same legal norms are also in force in the United Kingdom. Witnesses located in the UK must not be contacted directly by means of communication unless UK law enforcement agencies have first been informed".[1]

International treaties on legal assistance regulating the service of summonses and other procedural documents, their direct cross-border postal transmittal, declarations and reservations of states parties to them, and national rules (for example, in Switzerland) prohibit, by implication, such transmissions specifically and exclusively by post (as a rule, requiring documentary confirmation of physical personal service by hand), if the respective addressee country does not permit them. However, the same prohibition is presumed with regard to transmissions sent to addressees, who are known to the sender to be permanently present abroad, via SMS messages or e-mail, since this flows from the international legal principles of sovereign equality of states and non-interference in the internal affairs of other states. In addition, such unauthorized methods of service should result in the fact that the delivery will not have legal effect and will not entail any binding legal consequences for the recipients.

At the same time, it is reasonable to assume an acceptable exception to such a ban in cases where the addressee who stays abroad, irrespective of his or her citizenship, has in advance given his or her voluntary, informed and documented consent to the cross-border receipt of specific procedural correspondence (including summonses advising of the negative consequences of failure to appear) by such means of communication, except for post, since it is not associated with any coercive measures taken by the sending state in the territory of the receiving state. In such cases, it should not matter whether the phone number of the participant of the proceedings belongs to a telephone numbering range assigned to a Russian or foreign telecom operator, whether the email account belongs to a Russian or foreign provider, whether it is hosted by

[1] "Deputy Director of the Information and Press Department, MFA of Russia, A.M. Bikantov's answer to the media question on the 'Litvinenko case'", official website of the *RF MFA*, 31 July 2015, accessed July 31, 2015, http://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/1629306.

Russian or foreign servers, particularly since foreign operators and providers may offer these services in the territory of the Russian Federation, which is especially obvious in relation to the widespread use of foreign e-mail accounts by Russian nationals.

However, Russian laws and regulations approach such remote cross-border communications with the utmost caution in terms of non-violation of foreign jurisdiction: for example, Russian courts may send SMS notifications only to a mobile phone number of a cellular communication operator functioning on the territory of the Russian Federation;[1] in criminal proceedings, copies of a court decision made in the form of an electronic document, a summons or notification in electronic form are sent only within the limits of the Russian information systems enumerated in the law.[2]

The extraterritorial effect of telecommunications is reflected at length in international instruments, documents and methodological papers of the United Nations[3] and regional organizations, in particular the Council of Europe, on the subject of cybercrime. These have focused on the exercise of prescriptive and enforcement jurisdiction in cyberspace[4] and the need to observe international law

[1] Order of the Judicial Department at the RF Supreme Court of 25 Dec. 2013 No. 257 "On approval of the Regulations for organizing notifications to participants of proceedings by SMS messages" (para. 2.3 of the Regulations).

[2] RF CPC (arts. 474^1(5–6) and 474^2).

[3] *Comprehensive Study on Cybercrime* (New York: United Nations, 2013), pp. 183–185, 187–188 and 216–223; *The 2013 Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector: Executive summary* (UN Doc. UNODC/CCPCJ/EG.4/2013/2), paras. 29 and 35(c). URL: https://www.unodc.org/unodc/en/organized-crime/expert-group-to-conduct-study-cybercrime-feb-2013.html; C.S.D. Brown, "Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice", *International Journal of Cyber Criminology*, vol. 9, issue 1 (2015), pp. 61, 71, 77–79 and 98.

[4] See also: *Council of the European Union conclusions on improving criminal justice in cyberspace* of 9 June 2016; В.О. Калятин, "Проблемы установления юрисдикции в Интернете" [Problems of establishing jurisdiction on the Internet], *Законодательство* 5 (2001); А.И. Халиуллин, "Место совершения преступления как признак состава преступления в сфере компьютерной информации" [Place of commission of a crime as an element of corpus delicti in the field of computer information], *Актуальные проблемы экономики и права* 1 (2012), pp. 291–294; Л.В. Терентьева, "Территориальный аспект юрисдикции и суверенитета государства в киберпространстве" [Territorial aspect of jurisdiction and sovereignty of a state in cyberspace], *Lex russica* 4 (2019), pp. 139–150; Л.В. Терентьева, "Принципы установления территориальной юрисдикции государства в киберпространстве" [Principles of establishing territorial jurisdic-

principles such as respecting the territorial sovereignty of another state and non-intervention in its domestic affairs.

In cases of aforementioned actions and communications performed without informing the authorities of the state on whose territory the information system used by their addressee is located, they can be regarded as violating international legal principles of the sovereign equality of states, non-interference in the internal affairs of another state, viewed as constituting a crime or other offence or internationally wrongful act.[1] This fully applies to transnational relations with ICT service providers, including of virtual assets. Therefore, states nowadays strive to elaborate and approve international rules for mutual lawful conduct of such kind.

---

tion of a state in cyberspace], *Lex russica* 7 (2019), pp. 119–129; А.И. Москаленко, "Смарт-контракты как "умные" информационные активы в системе интеллектуальной собственности" [Smart contracts as "smart" information assets in the intellectual property system], *Международное публичное и частное право* 3 (2021), pp. 17–21; В.А. Батырь, *Международное территориальное право* [International territorial law] (М.: Международные отношения, 2021), p. 431; J. Worona, *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy: rozprawa doktorska* [Cyberspace and international law. Status quo and prospects] (Białystok: Uniwersytet w Białymstoku, 2017), s. 108–150; Resolution of the Plenum of the RF Supreme Court of 15 Dec. 2022 No. 37 "On some issues of court practice in criminal cases of crimes in the sphere of computer information, as well as other crimes committed with the use of electronic or information and telecommunications networks, including the Internet network" (para. 19).

[1] In accordance with Decree of the President of the Russian Federation of 12 Apr. 2021 No. 213 "On approval of the Fundamentals of the state policy of the Russian Federation in the field of international information security" (para. 8 of the Fundamentals), the use of ICTs to interfere in the internal affairs of sovereign states is one of the main threats to international information security.

In accordance with the updated Concept of Foreign Policy of the Russian Federation approved by Decree of the President of the Russian Federation of 31 Mar. 2023 No. 229 (paras. 15, 17–18 and 30), in view of the long-term trends in the development of the situation in the world, the national interests of the Russian Federation in the foreign policy domain include the protection of the sovereignty of the Russian Federation against any destructive foreign influence; strengthening the legal foundations of international relations; development of safe information space. The system of international relations should be based on the principles of sovereign equality of states, non-interference in internal affairs, and the rule of international law in regulating international relations. In order to ensure international information security and strengthen Russian sovereignty in the global information space, the Russian Federation intends to give priority attention to, among other things, adopting measures aimed at countering the policy of unfriendly states to use information and communications technologies to interfere with the internal affairs of states.

The threat of infringement on sovereignty caused Russia not to become a party to the 2001 Convention on Cybercrime.[1]

A Cybercrime Convention Committee's 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".[2] However, the contentious art. 32(b) of the 2001 Budapest Convention on Cybercrime[3] on the right and power to

[1] Decree of the President of the Russian Federation of 15 Nov. 2005 No. 557-rp "On Signing of the Convention on Cybercrime" (repealed in 2008).

See in more detail: Т. Борисов, "Виртуальный мир закрыт. Почему мы не подписали конвенцию против киберпреступности" [The virtual world is closed. Why we didn't sign the Convention on Cybercrime], *Российская газета — Федеральный выпуск* No. 256(5335), 12 Nov. 2010; М.А. Федотов, "Конституционные ответы на вызовы киберпространства" [Constitutional responses to the challenges of cyberspace], *Lex russica* 3 (2016), pp. 164–182; B.-J. Koops and M. Goodwin, *Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities of International Law*, in Tilburg Law School Legal Studies Research Paper Series, No. 05/2016.

[2] See also on Switzerland's criminal classification under art. 271 of the Criminal Code of the Swiss Confederation of direct approaches by foreign authorities to ICT service providers in Switzerland and related issues, as well as information on the Russian Federation: *The Practical Guide for Requesting Electronic Evidence across Borders* (Vienna: United Nations, 2021), pp. 16 and 228–230.

[3] Convention on Cybercrime of 23 Nov. 2001 (arts. 31–34); Explanatory Report to the Convention on Cybercrime, paras. 292–297.

It is noteworthy that its "prototype" is para. 6 ("Transborder access to stored data not requiring legal assistance") of the Principles on transborder access to stored computer data (Annex 1 to the Communiqué of the Ministerial Conference of the G-8 Countries on combating Transnational Organized Crime (Moscow, October 19-20,1999) (UN Doc. A/54/547 of 12 Nov. 1999) ("Notwithstanding anything in these Principles, a State need not obtain authorization from another State when it is acting in accordance with its national law for the purpose of: a. accessing publicly available (open source) data, regardless of where the data is geographically located; b. accessing, searching, copying, or seizing data stored in a computer system located in another State, if acting in accordance with the lawful and voluntary consent of a person who has the lawful authority to disclose to it that data. The searching State should consider notifying the searched State, if such notification is permitted by national law and the data reveals a violation of criminal law or otherwise appears to be of interest to the searched State.").

Provisions of art. 32 of the Budapest Convention are nearly verbatim reproduced in art. 40 of the Arab Convention on Combating Information Technology Offences of 21 Dec. 2010 concluded within the League of Arab States.

When necessary to immediately preserve data held by Russian ICT service providers and make preliminary inquiries about the availability of such data in

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 part of inspection of the (cooperative) suspect's device with an open mailbox, whose data is located in another state party to the Convention, and other scenarios of an unlimited scope, wherever and whenever the person in question is located[1]), in its official interpretation given by the said guidance note, 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".[2]

Nonetheless, this paragraph, initially intended to prevent cross-border searches and seizures of non-public data without the consent of their owners, due to the wording employed in it, is prone to extensive interpretation when assessing compliance with the criteria of lawfulness and voluntariness. There is no legal certainty as to whose law and by whom will be assessed and applied[3] (whether at

Russia, foreign authorities can use the INTERPOL I-24/7 network to contact the NCB of INTERPOL of the RF Ministry of Internal Affairs for this purpose.

[1] If the person providing the consent is located not abroad, but on the territory of the state whose foreign authority is obtaining access to the data, the provisions of art. 32(b) of the Budapest Convention will largely coincide with the provisions of art. 18(1)(a) of this Convention, against which the Russian Federation raised no objections.

[2] *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) // Guidance Notes. URL: https://www.coe.int/en/web/cybercrime/guidance-notes.

[3] For example, in the Russian Federation such actions may constitute crimes under art. 272 (illegal access to computer information committed by a person with the use of his official position), art. 273 (use of malicious computer programs committed by a person with the use of his official position) of the RF Criminal Code. See also draft art. 294[1] above; 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. URL: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home, accessed Apr. 14, 2023.

the location of the foreign authority retrieving the data,[1] the data subject, the operator (controller) of personal data, service provider, server, terminal user equipment). At the same time, guidance notes to the Convention, although being the official source of its interpretation, nonetheless, are not binding on its states parties. In addition, ICT service providers, contrary to the guidance note, are usually personal data controllers who determine the purposes and means of their processing (in Russia, this concept is covered by the term "operator"). The case law of the Federal Supreme Court of Switzerland indicates that service providers do have such a lawful authority to transfer data to local and foreign law enforcement and judicial agencies, if they have stipulated the possibility thereof among the terms and conditions of use of their services accepted by the client. (The papers on the implementation of the Budapest Convention contain an opposite view).[2]

The provisions of art. 32(b) of the Budapest Convention do not contain any mechanisms for resolving possible withdrawals of the given consent by the authorized person, a requirement that such consent be not only voluntary but also informed, jurisdictional and other clauses as to the basic procedure for challenging by the persons

[1] The drafters of subsequent documents to the Budapest Convention leaned towards this option. See: *Transborder access and jurisdiction: What are the options? Report of the Transborder Group* adopted by the T-CY on 6 Dec. 2012. Strasbourg, 6 Dec. 2012, T-CY (2012)3, p. 22, para. 3.2.3.4; *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), p. 7, para. 3.5.

[2] Bundesgericht, Urteil der I. öffentlich-rechtlichen Abteilung i.S. Oberstaatsanwaltschaft des Kantons Zürich gegen Unbekannt (Beschwerde in Strafsachen) 1B_344/2014 vom 14. Januar 2015. See the opposite opinion: *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), p. 7, para. 3.4; *Transborder access and jurisdiction: What are the options? Report of the Transborder Group* adopted by the T-CY on 6 Dec. 2012. Strasbourg, 6 Dec. 2012, T-CY (2012)3. P. 21–23, paras. 3.2.3.3, 3.2.3.5.

Country-specific information on the implementation in national legislation and practical application (including issues of admissibility of evidence) by the EU member states of the provisions of arts. 18 and 32 of the Budapest Convention is published annually (in varying scope) in a joint publication of Eurojust, Europol and EJN: *SIRIUS EU Digital Evidence Situation Report. 2nd Annual Report.* 2020. 68 p.

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

concerned of direct accesses to and retrievals of data sanctioned by the Convention, establishment and enforcement of other essential legal remedies for data subjects, either.

According to the results of UNODC research published in 2013 and remaining relevant at the present time, direct cross-border access to computer systems and data, including in the cloud, without prior authorization of the state where they are located, is deemed impermissible by the majority of "host countries" which ordinarily require that legal assistance processes are observed for these purposes. There is a similar attitude with respect to foreign law enforcement directly and remotely approaching service providers situated in those countries for subscriber, traffic or content data. In turn, service providers themselves also tend to adhere to the international legal assistance channels for disclosing the said data, with some exceptions where a foreign judicial or other relevant order of the requesting party is sufficient.[1] Voluntary disclosure of data (subscriber information, traffic and sometimes content data) to foreign authorities, in particular in emergency situations, is currently established, to the best of our knowledge, only by service providers in the United States and Canada in accordance with domestic legislation of these countries.[2] For European service providers this is not typical even in case of an emergency.

Legislation, policy (including the foreign policy line under the coordinating role of the Ministry of Foreign Affairs[3]) or practice of the Russian Federation do not provide for the possibility of direct

---

[1] *Comprehensive Study on Cybercrime* (New York: United Nations, 2013), pp. 218–222; А.П. Рыжаков, *Комментарий к статье 2 Федерального закона от 6 июля 2016 года № 375-ФЗ* [Commentary on article 2 of the Federal Law of 6 July 2016 No. 375-FZ], СПС КонсультантПлюс (2016).

[2] 18 U.S. Code § 2702 — Voluntary disclosure of customer communications or records.

[3] The principles of sovereignty and non-interference in the internal affairs of another state are not duly respected by some norms of EU law in the field of processing personal data for law enforcement, judicial and penitentiary purposes. Directive 2016/680 establishes a unilateral transfer of personal data directly to recipients in third countries, bypassing their competent authorities (Directive (EU) 2016/680 of the European Parliament and of the Council of 27 Apr. 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, preamble para. 73, art. 39).

access of foreign law enforcement and judicial authorities with any requests (including requests for data preservation,[1] voluntary disclosure of data in emergency situations, also with the consent of the user) to Russian ICT providers (the so-called asymmetric (diagonal) cooperation), reserving such contacts exclusively to the purview of Russian authorities (the "State-in-the-middle" approach). The required urgency of the request and of its processing must be secured by 24/7 interagency communication networks, such as INTERPOL's I-24/7, provided that their functioning is uninterrupted and otherwise fully reliable.

At the same time, unlike, for instance, Switzerland, which criminalized any unauthorized actions on behalf of and in the interests of foreign states in its territory (art. 271 of the Swiss Criminal Code),[2] so far the Russian Federation has not enacted any "blocking statutes",[3] that would restrict, prohibit and penalize the actions of both Russian ICT service providers fulfilling foreign requests received by them directly from abroad (whereas there are pieces of such legislation adopted in relation to other subjects),[4] and of foreign officials forwarding such requests.

See also on the assumed permissibility of extraterritorial direct warning in cases of danger of violation of the right to life and in other exceptional cases (duty to warn): *Investigation of, accountability for and prevention of intentional State killings of human rights defenders, journalists and prominent dissidents: Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions* (UN Doc. A/HRC/41/36 of 4 Oct. 2019), para. 67; *Annex to the Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions: Investigation into the unlawful death of Mr. Jamal Khashoggi* (UN Doc. A/HRC/41/CRP.1 of 19 June 2019), para. 368.

[1] The service provider's reaction to such requests already involves their disclosure of information that confirms or refutes the availability or absence of the data that are to be preserved.

[2] *The Practical Guide for Requesting Electronic Evidence across Borders* (Vienna: United Nations, 2021), p. 230.

[3] *Transborder access and jurisdiction: What are the options? Report of the Transborder Group* adopted by the T-CY on 6 Dec. 2012. Strasbourg, 6 Dec. 2012, T-CY (2012)3, p. 22, para. 3.2.3.4; P.A. Litvishko, *Non-Treaty Forms of Extraterritorial Judicial and Law Enforcement Activities*, in Collection of Materials on International Cooperation of the Investigative Committee of the Russian Federation (Moscow: Prospekt, 2016), pp. 132–173; Л.В. Головко, *Государство и его уголовное судопроизводство: монография* [State and its criminal proceedings: monograph] (М.: Издательский Дом «Городец», 2022), pp. 43–72 and 442–443.

[4] Federal Law of 1 May 2022 No. 125-FZ "On amendment to the Federal Law "On measures to influence (counter) unfriendly actions of the United States of America and other foreign states""; Federal Law of 28 June 2014 No. 173-FZ "On the specificities of performing financial transactions with foreign citizens and legal entities,

Draft article 294[1] of the RF Criminal Code discussed above is also aimed at filling in this gap.

On the other hand, with regard to outgoing requests from Russian law enforcement, investigative and judicial authorities for voluntary preservation of electronic evidence or provision of subscriber information, transmitted directly to foreign service providers (mainly operating under US law) and related to the services provided by them in Russia, these are considered admissible insofar as they are envisaged by guidances or other instructions of these service providers for foreign law enforcement and judiciary, officially published on their portals and thus denoting the express consent, implicit approval or acquiescence of the state of the service provider to such way of cross-border communications.[1]

In addition, these requests may be addressed directly to service providers "localized" ("landed") in the Russian Federation in accordance with Federal Law of 1 July 2021 No. 236-FZ "On the Activities of Foreign Persons on the Information and Telecommunications Network "Internet" in the Territory of the Russian Federation".

It should be borne in mind that in cases of such voluntary asymmetric cooperation, many service providers by default, unless being

on amending the Code of Administrative Offences of the Russian Federation and repealing certain provisions of legislative acts of the Russian Federation"; Decree of the President of the Russian Federation of 11 Sept. 2012 No. 1285 "On measures to protect the interests of the Russian Federation in the conduct of foreign economic activities by Russian legal entities"; RF Criminal Code arts. 275 (state treason), 275[1] (cooperation on a confidential basis with a foreign state, international or foreign organization), 276 (espionage), and 284[3] (provision of assistance in executing decisions of international organizations, in which the Russian Federation does not participate, or foreign state authorities).

[1] Some countries have enshrined this approach at the legislative level. For example, in 2018, Georgia introduced an international production order, which empowers a Georgian judge to issue a production order in respect of persons or entities outside of the territorial jurisdiction of Georgia if the following conditions are met, cumulatively: agreement of the person who is the subject of the order with the voluntary disclosure of electronic data; and permission from the host country of the foreign entity for such disclosure through its laws or executive policies. Such orders must be obtained from a court by the prosecutor and must be transmitted through an official who is authorized by the attorney general. Non-compliance with such orders does not entail any legal liability. In accordance with article 18 of the Council of Europe Convention on Cybercrime, Georgia has used international production orders in respect of Facebook and other international service providers in connection with services offered in Georgia. (*Countering the use of information and communications technologies for criminal purposes: Report of the Secretary-General* (UN Doc. A/74/130 of 30 July 2019), para. 109.)

given (justified) confidentiality instructions in the request or a gag order attached to the request, normally notify[1] the customer, whose data is requested, of the receipt and results of consideration of the request. They can also immediately send a copy of it to the customer concerned, as well as demand reimbursement of the costs of processing the request, of ensuring the preservation and provision of data in response to it.[2]

Article 18 of the Budapest Convention laid down the foundations for 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, including their possible dispersal over the territories of different countries, the circumstance that the user's device is in roaming mode, or "loss of location" of data, as well as any other parameters.[3]

---

[1] Default notification can also occur in an automatic mode, by technical design of the provided service. See: *Data disclosure framework. General practices developed by international service providers in responding to overseas government requests for data* (Vienna: United Nations, 2021), pp. 18–19.

[2] See, e.g.: *Pinterest Law enforcement guidelines*, URL: https://help.pinterest.com/en/article/law-enforcement-guidelines.

[3] *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). Strasbourg, 3 Dec. 2014, T-CY (2014)16, pp. 10–14 and 16–20; *Transborder access and jurisdiction: What are the options? Report of the Transborder Group* adopted by the T-CY on 6 Dec. 2012. Strasbourg, 6 Dec. 2012, T-CY (2012)3; *Criminal justice access to data in the cloud: challenges, Discussion paper* of 26 May 2015 prepared by the T-CY Cloud Evidence Group; *Criminal justice access to data in the cloud: Cooperation with "foreign" service providers, Background paper* of 3 May 2016 prepared by the T-CY Cloud Evidence Group; *Criminal justice access to electronic evidence in the cloud — Informal summary of issues and options under consideration by the Cloud Evidence Group* of 17 Feb. 2016; *Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY: Final report of the T-CY Cloud Evidence Group* (T-CY (2016)5 of 16 Sept. 2016); *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) (issuing a production order for subscriber information with regard to ICT service providers located abroad, but offering their services in the territory of

A provision identical to art. 18 of the Budapest Convention is contained in art. 27 of the current draft UN Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.

In Russia, orders for such information from service providers offering their services in its territory are presented and executed with due regard to the requirements of Federal Law of 1 July 2021 No. 236-FZ "On the Activities of Foreign Persons on the Information and Telecommunications Network "Internet" in the Territory of the Russian Federation".

In turn, for the purposes of the Budapest Convention, "it is understood that a communication is in a Party's territory if one of the communicating parties (human beings or computers) is located in the territory or if the computer or telecommunication equipment through which the communication passes is located on the territory".[1]

In the interpretation of the Federal Supreme Court of Switzerland, the norm of art. 18 of the Budapest Convention applies only to domestic, and not foreign service providers, or subsidiaries or partner firms of foreign providers located in the state exercising jurisdiction, that store data in the territory of this state, for example, by operating server farms.[2]

In 2018, the United States adopted the CLOUD Act, which provides for a mutual regime of forwarding direct orders for producing all types of data to ICT service providers, their branches and subsidiaries (including those of US service providers) located in states, with which the United States has entered into relevant executive

---

the Party issuing the order). Guidance Notes. URL: https://www.coe.int/en/web/cybercrime/guidance-notes.

[1] *Explanatory Report to the Convention on Cybercrime.* Budapest, 23.XI.2001, para. 222.

[2] Bundesgericht, Urteil der I. öffentlich-rechtlichen Abteilung i.S. Oberstaatsanwaltschaft des Kantons Zürich gegen Unbekannt (Beschwerde in Strafsachen) 1B_344/2014 vom 14. Januar 2015.

This decision, however, was taken prior to the issuance of the guidance note to art. 18 of the Budapest Convention (*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) (issuing a production order for subscriber information with regard to ICT service providers located abroad, but offering their services in the territory of the Party issuing the order)).

agreements. At the same time, the orders of the other contracting party to the agreement sent to the US service providers may not intentionally target data of US persons or persons located in the United States. (The first such agreement was concluded in 2019 with the United Kingdom, which also passed the relevant law).[1]

United States legal practice precludes prospective real-time collection of content solely on behalf of foreign governments. Two exceptions to this rule exist, however. If there is a parallel or joint investigation conducted by United States law enforcement, the United States authorities may be permitted to share the product with overseas law enforcement. Real-time content is available also to countries with a bilateral CLOUD Act executive agreement with the United States.[2]

In 2022, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence was adopted, which regulates: direct disclosure by domain name registrars and ICT service providers, located in the territory of a state party to the Protocol (this is a mandatory territorial condition), 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 aspects, 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; the use of video conferencing for taking of testimony or a statement, other hearings and proceedings, including for the purposes of identifying persons or objects, audio conferences; joint investigation teams and joint investigations; protection of personal data.[3]

---

[1] Clarifying Lawful Overseas Use of Data Act (CLOUD Act) of 2018; Crime (Overseas Production Orders) Act 2019.

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

[3] Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, Explanatory Report thereto.

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[1] apply to the issuance by an authority of a EU Member State of an order commanding a service provider offering services in the Union and established in another EU Member State, or, if not established, represented by a legal representative in another EU Member State (thus "localized" for the purposes of the Regulation and some other instruments indicated in the Directive), to produce or to preserve electronic evidence regardless of the location of the data constituting the relevant electronic evidence. The irrelevance of the data storage location is also reflected in the Regulation's provisions concerning the procedures for considering a conflicting obligation of a service provider under the law of a third country.

The Regulation applies to the issuance of orders in respect of data pertaining to services offered only within the EU. Therefore, for instance, in cases of a Russian provider offering their services there (which, in turn, requires that they designate their establishments or appoint legal representatives in one or more EU Member States), it can be ordered to yield exclusively this kind of data. The Regulation does not lay down any obligation for service providers to decrypt data, and prescribes the imposition of turnover pecuniary penalties on them for infringing its provisions.

[1] 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. See: E-evidence — cross-border access to electronic evidence. URL: https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en, accessed Dec. 17, 2023.

Determining whether a service provider offers services in the Union requires an assessment as to whether the service provider enables natural or legal persons in one or more Member States to use its services. However, the mere accessibility of an online interface in the Union, such as for instance the accessibility of a website or an email address or other contact details of a service provider or an intermediary, taken in isolation, should be considered insufficient to determine that a service provider offers services in the Union. A substantial connection to the Union should also be relevant to determining whether a service provider offers services in the Union. Such a substantial connection to the Union should be considered to exist where the service provider has an establishment in the Union. In the absence of such an establishment, the criterion of a substantial connection should be based on specific factual criteria such as the existence of a significant number of users in one or more Member States, or the targeting of activities towards one or more Member States. The targeting of activities towards one or more Member States should be determined on the basis of all relevant circumstances, including factors such as the use of a language or a currency generally used in that Member State, or the possibility of ordering goods or services. The targeting of activities towards a Member State could also be derived from the availability of an application ('app') in the relevant national app store, from the provision of local advertising or advertising in the language generally used in that Member State, or from the handling of customer relations, such as by the provision of customer service in the language generally used in that Member State. These two cumulative conditions (enabling persons to use the services at issue and the substantial connection) are set forth in the definitions of offering services in the Union and on the territory of a Member State used in the Regulation and Directive.

Orders are addressed for execution directly to a designated establishment or to a legal representative of the service provider concerned in the relevant EU Member State (enforcing State). Where an order is issued to obtain traffic or content data, the issuing authority should notify the competent authority in the enforcing State of such an order at the same time as it transmits this order to the addressee, in particular for the purpose of checking the existence of grounds for it to refuse the provision of the data concerned. However, where such an order is issued to obtain electronic evidence in criminal proceedings with substantial and strong links to the issuing State,

no notification to the enforcing authority is required. Such links should be assumed where, at the time of issuing the order, the issuing authority has reasonable grounds to believe that the offence has been committed, is being committed or is likely to be committed in the issuing State, and where the person whose data are requested resides in the issuing State (a cumulative condition). The Regulation sets forth rather broad criteria for assuming and determining the jurisdiction of the place of the commission of the offence and the place of residence of the person.

The Regulation lays down a special procedure of judicial review, with the participation of the service provider, issuing and enforcing States, for cases where the service provider at hand objects to the execution of an order coming from abroad within the EU on the grounds that compliance with the order would lead to the breach of their conflicting legal obligation under the applicable law of a third country. At the end of the procedure, a court of the issuing State has the final say as to the enforceability of the order and unilaterally overcoming the third country's legal prohibition of the disclosure of the data concerned, which cannot be regarded as compatible with the ensuring of comity in respect of the sovereign interests of third countries declared in the Regulation. The said objection may not be based on the sole fact that the data are stored in a third country; among other factors, the said court assesses the degree of connection between the service provider and the third country in question, and in this context, the data storage location alone shall not suffice for the purpose of establishing a substantial degree of connection.

Judicial authorities empowered to issue or validate orders, are, with regard to orders to obtain traffic or content data, exclusively a judge, a court or an investigating judge (orders issued by an investigating authority are subject to validation by such judges or courts), with regard to orders to obtain subscriber data or data, including traffic data, requested for the sole purpose of identifying the user, as well as orders to preserve data of any category, they also include public prosecutors in addition to such judges or courts (orders issued by an investigating authority are subject to validation by such judges, courts or public prosecutors); the Regulation sets out a special procedure for the issuance and *ex post* (as opposed to prior) validation of orders to obtain subscriber data or data requested for the sole purpose of identifying the user, as well as orders to preserve data, in emergency cases defined in the Regulation.

For secure digital communication and data exchange between issuing and enforcing authorities and service providers, the Regulation provides for the use of a dedicated decentralised IT system, some of whose components are based on the e-CODEX system,[1] the Regulation also provides for the legal effect and admissibility of electronic documents, use of electronic signatures and seals.

However, even within the EU, there is significant criticism of such outsourcing of functions of judicial authorities, with their safeguards and personal data protection standards, in favor of such cross-border public-private partnerships, privatization of public functions, and some point out the insufficiency of notifications to the competent authorities of the state of the service provider.[2]

Thus, one can observe a steady course towards the development of legal frameworks to meet the growing demand of law enforcement and judicial practice for immediate cross-border actions, which are essentially unilateral in nature, and aimed at obtaining electronic intelligence and evidence directly from foreign service providers and other actors outside the international legal (judicial) assistance or law enforcement (police-to-police) cooperation, which excludes the activation and engagement of their mechanisms for assessing and refusing assistance, imposing conditions for its provision in order to protect the public interest, personal data, privacy, and other human rights, immunities and privileges (including electronic ones), establishing authenticity of communications, etc. In turn, the service providers are in no position to evaluate all these parameters themselves (in particular, assess eventual prejudice to the states' sovereignty, security or other essential interests, risks of political persecution or other human rights abuses by the requesting state), nor are they able to conclude whether the sought data is indeed relevant, proportionate and necessary in a democratic society, or the standard of proof is met.

---

[1] Regulation (EU) 2022/850 of the European Parliament and of the Council of 30 May 2022 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system), and amending Regulation (EU) 2018/1726 (Text with EEA relevance).

[2] *Cross-border data access in criminal proceedings and the future of digital justice. Navigating the current legal framework and exploring ways forward within the EU and across the Atlantic. Report of a CEPS and QMUL Task Force* / Carrera S., Stefan M., Mitsilegas V. (Brussels: Centre for European Policy Studies (CEPS), 2020), 99 p.

One witnesses a gradual partial dismantling of the architecture of inter-State interaction. On the whole, modern aspirations for decentralization and world order without intermediaries, be it states or other corporate structures, are characteristic of many spheres of human life, especially in the context of its progressing virtualization. This centrifugal trend also expresses itself in the development of peer-to-peer networks, blockchain, smart contracts, decentralized autonomous organizations, 5G broadband technology, Metaverse and Web 3.0 with their decentralized configuration, uberization, etc. Such technological categories have now moved into the realm of ideological ones.

In 2021, the Open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime presented their report on the outcome of this study with conclusions and recommendations for consideration by the Commission on Crime Prevention and Criminal Justice.[1]

The problems of combating cybercrime are inextricably linked with the issues of ensuring international information security and are related respectively as a part and a whole.

Resolution 73/27 "Developments in the field of information and telecommunications in the context of international security", adopted by the UN General Assembly on 5 December 2018 on the Russian initiative, reaffirmed the set of international rules, norms and principles of responsible behaviour of States, enshrined in the reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, concerning the applicability of international law to State use of ICTs, in particular, the following:

State sovereignty and international norms and principles that flow from sovereignty (such as non-intervention or non-interference in the internal affairs of other States[2]) apply to State conduct of ICT-

[1] Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 6 to 8 April 2021 (UN Doc. UNODC/CCPCJ/EG.4/2021/2).

[2] Many sources distinguish between the concepts of intervention, which requires a constituent element of coercion, and interference, which does not have a coercive character. See: *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* / Ed. by M.N. Schmitt, L. Vihul (Cambridge: Cambridge University Press, 2017), pp. 24 and 312–325; *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy* (ed. K. Ziolkowski) (Tallinn: NATO CCD COE, 2013), pp. 162–165, 186 and 189–238.

related activities and to their jurisdiction over ICT infrastructure within their territory;

States must meet their international obligations regarding internationally wrongful acts attributable to them under international law. However, the indication that an ICT activity was launched or otherwise originates from the territory or objects of the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State. Accusations of organizing and implementing wrongful acts brought against States should be substantiated;

States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs. States must not use proxies to commit internationally wrongful acts using ICTs and should seek to ensure that their territory is not used by non-State actors to commit such acts;

States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.[1]

In 2021, the UN General Assembly called upon Member States to be guided in their use of information and communications technologies by two consensus final reports (of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security[2] and of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security[3]).[4]

In its Resolution 75/240 "Developments in the field of information and telecommunications in the context of international security" of

[1] See also: International code of conduct for information security: Annex to the letter dated 9 Jan. 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General (UN Doc. A/69/723), paras. 1–3; *Применение международного права в киберпространстве* [Application of international law in cyberspace], Индекс безопасности, No. 4(115), T. 21 (2015), pp. 99–116.

[2] UN doc. A/75/816 of 18 Mar. 2021.

[3] UN doc. A/76/135 of 14 July 2021.

[4] Resolution 76/19 "Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies" adopted by the UN General Assembly on 6 Dec. 2021.

31 December 2020 adopted on the Russian initiative, the UN General Assembly, decided to convene, starting from 2021, under the auspices of the United Nations, a new open-ended working group on security of and in the use of information and communications technologies 2021–2025, acting on a consensus basis, to continue, as a priority, to further develop the rules, norms and principles of responsible behaviour of States and the ways for their implementation and, if necessary, to introduce changes to them or elaborate additional rules of behaviour; to consider initiatives of States aimed at ensuring security in the use of information and communications technologies; to establish, under the auspices of the United Nations, regular institutional dialogue with the broad participation of States; to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security, inter alia, data security, and possible cooperative measures to prevent and counter such threats, and how international law applies to the use of information and communications technologies by States, as well as confidence-building measures and capacity-building; and to submit, for adoption by consensus, annual progress reports and a final report on the results of its work to the General Assembly at its eightieth session.

Multilateral and bilateral interstate and intergovernmental agreements of the Russian Federation on cooperation in the field of ensuring international information security stipulate, among other things, the fight against cybercrime, exchange of information for law enforcement and judicial purposes as the main areas of cooperation. It should be borne in mind, however, that like multilateral and bilateral interstate and intergovernmental agreements of the Russian Federation on law enforcement (police-to-police) cooperation in the field of combating crime, as well as international interagency arrangements, envisaging the mutual assistance of the parties in combating computer crimes, the said agreements in the field of international information security, of course, do not regulate the rendering of legal assistance in the field of criminal justice, that is, obtaining evidence in criminal cases.

It is necessary to keep in mind the possible use for criminal justice purposes of intelligence gathered by national security agencies,

which requires compliance with certain standards and criminal procedural guarantees, including, in certain cases, judicial review.[1]

In 2006, the ECtHR found that carrying out the strategic monitoring of international wireless telecommunications, that is, telecommunications which are not effected via fixed telephone lines but, for example, via satellite or radio relay links, and using data thus obtained, does not illegally interfere with the territorial sovereignty of the foreign states in which the persons being monitored reside and therefore is not contrary to public international law (In that case, signals emitted from foreign countries were monitored by interception sites situated on German soil and the data collected were used in Germany.)[2]

After the global surveillance programs "PRISM", "ECHELON", "Upstream", "Boundless Informant" systems and some other telecommunications intercept programs operated by the US NSA, UK Government Communications Headquarters and other countries' special services providing signals intelligence and united in the Five Eyes Signals Intelligence Alliance were leaked in 2013, it revived discussion about whether transit countries' engaging in the strategic mass surveillance of transit "external" bulk communications (where at least one party is outside the transit country) passing through their territory via cable (mostly submarine communications fibre-optic cables) and wireless systems (such as satellite and radio-relay links) was consistent with international law. In addition, questions arose over obtaining these content and metadata from telecommunications service providers incorporated or located in those countries. In 2021, the ECtHR resolved a number of long-standing cases concerning these issues by developing a set of human rights criteria for compatibility with the European Convention on Human Rights of mass interception of communications (both external and internal) and the reception and transmission of such intercept products between foreign intelligence services.[3]

---

[1] G. Vermeulen, W. De Bondt and C. Ryckman, *Rethinking international cooperation in criminal matters in the EU. Moving beyond actors, bringing logic back, footed in reality* (Antwerpen-Apeldoorn-Portland: Maklu, 2012), pp. 95–100 and 533–535.

[2] *Weber and Saravia v. Germany* (dec.), no. 54934/00, 29 June 2006, ECHR, paras. 26, 66, 81, 83 and 86–88.

[3] *Big Brother Watch and Others v. the United Kingdom* [GC], nos. 58170/13, 62322/14 and 24960/15, 25 May 2021, ECHR; *Centrum för rättvisa v. Sweden* [GC], no. 35252/08, 25 May 2021, ECHR; *New technologies. Factsheet*, European Court of

There still exist legal challenges relating to the covert use of geolocation, GPS/GLONASS tracking devices, etc. on the vehicles of suspects and other objects crossing the border of another state. This measure constitutes a special investigative technique under art. 20 of the Palermo Convention, namely electronic surveillance, and other treaties (and qualifies as an operational search measure "surveillance" under art. 6 of the Federal Law "On Operational Search Activities"), represents a particular type of international cooperation and requires an advance approval by the state into whose territory the vehicle or other object equipped with such a device is expected to arrive, or a prompt notification to the state concerned of the said object approaching its border if this was not initially anticipated and was established during the monitoring. In addition to that, some countries' laws regard these types of actions as procedural (judicial) ones requiring the international mutual legal assistance process rather than law enforcement cooperation for their conduct.[1]

Human Rights, July 2023; *Mass surveillance. Factsheet*, European Court of Human Rights, September 2022.

For information on obtaining telecommunications data from satellite and the so-called space theory (Weltraum-Theorie) applied in operations of German special services, see: A. Frischholz, "BND-Skandal. Überwachung und Spionage am rechtlichen Abgrund", *Computer Base*, 13 Nov. 2015, URL: http://www.computerbase.de/2015-11/bnd-skandal-ueberwachung-und-spionage-am-rechtlichen-abgrund/, accessed Dec. 18, 2023.

[1] *Judicial collaboration versus police collaboration. Subject submitted for discussion in the PC-OC at its 43rd meeting in 2001 by Mr M. Knaapen (Netherlands).* Strasbourg, 30 Jan. 2013 [PC-OC\Docs 2001\20Erev]; art. 134.3 of the Criminal Procedure Code of the Republic of Moldova on a special search measure "locating or tracking via the Global Positioning System (GPS)"; Zákon ze dne 20. března 2013 č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních [Law on international judicial cooperation in criminal matters] (§§ 62–63); А.А. Хайдаров, "Получение информации о местонахождении лица, транспортного средства и иного объекта как новое следственное действие" [Obtaining information about the location of a person, vehicle or other object as a new investigative action], *Вестник Академии Генеральной прокуратуры Российской Федерации* 4(60) (2017), pp. 103–108; *Die internationale Rechtshilfe in Strafsachen: Wegleitung* [International legal assistance in criminal matters: Guidance]: 9. Aufl. 2009 (Rechtsprechung Stand Mai 2010) (Bern: Bundesamt für Justiz, Fachbereich Rechtshilfe, 2009): Ziff. 3.6.3, S. 76–77.

See also: Proposal by Switzerland regarding regulation by the convention of the use of technical recording devices in the territory of another state party: *Draft Third Additional Protocol to the European Convention on Mutual Assistance in Criminal*

§ 3. Special Investigative Techniques: Assessing the Need for Developing the Regional Frameworks

I. Introduction[1]

The importance and timeliness of raising the subject of special investigative techniques (hereinafter referred to as "SIT(s)") can hardly be overestimated. The new reality characterized by such major factors as virtualization, anonymization and pseudonymization leaves the judicial and law enforcement communities no option, calling for equally surreptitious means and methods of their work. The employment of stealthy operations is more than ever gaining on relevance, especially in the online environment, compared to the physical world often being the only way to collect admissible evidence, expose criminals, disrupt and dismantle transnational criminal networks.[2]

This chapter explores the nature of SITs, the international global (UN, FATF) and regional (CoE, CIS, SCO and CSTO) as well as domestic legal frameworks, and addresses the challenges of their desig-

Matters: Document prepared by the Secretariat, Strasbourg, 8 September 2023 [PC-OC/(2023)07E], p. 5.

[1] This chapter was originally published as papers of the Council of Europe's (CoE) Committee of Experts on the Operation of European Conventions on Co-operation in Criminal Matters (PC-OC): Special Investigative Techniques: Assessing the Need for Additional Regulation in the Council of Europe's Instruments of Legal Assistance in Criminal Matters: Discussion Paper by Mr Pyotr Litvishko (Russian Federation), PC-OC Mod Substitute Member, Strasbourg, 19 August 2021 [PC-OC/PC-OC Mod/Docs PC-OC Mod 2021/ PC-OC Mod (2021)04E]; Introductory Note to Discussion Paper PC-OC (2021)10EN.

[2] Cf.: para. 24 of the 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) states that "[t]he drafters also considered other measures which, after thorough discussion, were not retained in this Protocol. Two of these provisions, namely, "undercover investigations by means of a computer system" and "extension of searches", were of high interest to the Parties but were found to require additional work, time and consultations with stakeholders."; Terms of reference (document T-CY (2021)19 of 15 Nov. 2021) for the T-CY Working group on undercover investigations by means of computer systems and extension of searches; 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. URL: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home, accessed Apr. 14, 2023.

nation and definitions. It identifies the problems of their coverage in the treaties, and relationships and differences in interpretation and application. The chapter concludes with the proposals for the required CoE regulations.

II. Designation/Definition Challenge. Council of Europe Framework: National vs. International SITs

It is common knowledge that names are too often just arbitrary labels which do not reflect intrinsic qualities of things they are attached to. Shakespeare's "What's in a name?" is of relevance when one starts talking about SITs.

For the most part, SITs are associated with law enforcement intelligence[1] which, in turn, is considered an outgrowth of military and national security intelligence that dates back to ancient times;[2] references to it can be found in ancient Chinese writings (Sun Tzu, fl. 4th century BC) and the Bible (Numbers 13).[3]

The methods to transform the product of SITs (the biblical "fruit of the land") into evidence and adduce it in court, as well as the evidential value allocated to materials derived from the deployment of SITs, are different in the existing legal systems.

Various sources generally distinguish the following types of covert SITs:[4]

---

[1] Law enforcement intelligence mainly represents information gathered surreptitiously to prevent, identify and combat criminal offences. SITs can be deployed either for intelligence-gathering or evidential purposes.

Unlike the definitions in the Council Framework Decision 2006/960/JHA of 18 Dec. 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union (art. 2), the term "criminal (law enforcement) intelligence operation" as used in this chapter is a synonym for a SIT and encompasses the stages both of a criminal intelligence operation *per se* and a criminal investigation, i.e., both proactive and reactive types of investigations.

[2] M. Peterson, *Intelligence-Led Policing: The New Intelligence Architecture* (Washington, DC: U.S. Department of Justice, 2005), p. 5.

[3] "The LORD said to Moses, "Send men to reconnoiter (in other translations, "search", "explore", or "spy out") the land of Canaan". The men conducted covert observation and sampling, procuring "the fruit of the land". In the end, they presented a misinformative description ("a bad report") of the outcome of their covert investigations.

[4] See, e.g.: *Mutual Legal Assistance Manual* (Belgrade: Council of Europe Office in Belgrade, 2013), pp. 33–36 and 101–109; *Model Legislative Provisions against Organized Crime. Second Edition* (Vienna: United Nations, 2021), pp. 59–87; *Model legislation on money laundering and financing of terrorism* (United Nations Office

- interception of communications;
- controlled deliveries;
- surveillance (observation);[1]
- (virtual) covert investigations (undercover operations), network investigative techniques,[2] such as:
  infiltration, i.e., the use of undercover officers,[3] assumed (false) identities (covers, legends, backstories);

---

on Drugs and Crime, International Monetary Fund, 2005); *Technical Guide to the United Nations Convention against Corruption* (New York: United Nations, 2009), pp. 182–187; Recommendations on Special Investigative Techniques and other Critical Measures for Combating Organized Crime and Terrorism. Meeting of G8 Justice and Home Affairs Ministers, Washington — May 11, 2004.

[1] "Surveillance" is either physical (conventional) (tailing, stakeout, shoulder surfing, aerial covert surveillance using unmanned aircraft (drones) etc.; it may also extend to monitoring bank accounts in financial investigations, monitoring computer activities in cyber investigations (equipment interference)) or technical (electronic). The latter is more intrusive than the former and includes audio, visual, tracking and data surveillance, may be directed (in a public place) or intrusive (involving the installing and using of a covert listening or recording device (wireless transmitter) in residential premises or private vehicles).

"Surveillance" may also be used as an umbrella term for various kinds of SITs. See: *Current practices in electronic surveillance in the investigation of serious and organized crime* (New York: United Nations, 2009), p. 2.

Under the UNODC 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) (sec. 27), electronic surveillance means: (a) the monitoring, interception, copying or manipulation of messages, data or signals that have been stored or transmitted, or are in the process of being transmitted, by electronic means; and (b) the monitoring or recording of activities by electronic means, and any covert engagement in electronic communications with suspects involving undercover measures.

[2] E.g., in virtual investigations by "government hacking", using loggers, such as IP Grabber (Grabify IP Logger), hardware and software keystroke loggers, sniffers, compromising electromagnetic emanations, or embedding exploits (backdoors) and other spyware.

See in more detail on watering hole attacks and other types of network investigative techniques: *Digest of cyber organized crime. Second edition* (Vienna: United Nations, 2022), pp. 32, 111–118, 123–124.

[3] They include undercover online operatives. Techniques employed by them may include various kinds of misrepresenting their identities, e.g., communicating through the online identity of a cooperating witness (with consent) or appropriating online identity, or lure, or using products of private persons' "digilantism" (Internet vigilantism, or sousveillance) (e.g., those derived from proactive impersonation of a child or of a facilitator of child exploitation online or compromising information systems used for the purposes of child pornography), other online and offline subterfuges, ruses, traps and enticements.

staging (imitation) of criminal offences, or (reverse) sting operations, like a storefront or other (online) undercover facility, pseudo-purchases (test buys) and sales, other simulated transactions, and other pseudo offences, while as a general rule no entrapments (police incitement) or agents provocateurs are permitted;
integrity testing (simulation of bribery);
financial transaction monitoring, including the setting up of undercover virtual asset wallets;

- deployment of covert human intelligence sources, i.e., confidential informants; in some legal systems, the latter are subsumed under the notion of "undercover (police or intelligence) officers (undercover agents, police operatives)", thus encompassing both handlers and their assets;
- covert obtainment of samples (DNA from a fingerprint, lip smear or other objects, voiceprints, video footage, or malware specimens);
- (transborder) remote search in information systems and networks, use of remote (digital) forensics (e.g., in forensic virtual asset investigations).

The term of art "SIT" originates in the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime of 1990. Pursuant to art. 4.2 ("Special investigative powers and techniques"), "[e]ach Party shall consider adopting such legislative and other measures as may be necessary to enable it to use special investigative techniques facilitating the identification and tracing of proceeds and the gathering of evidence related thereto. Such techniques may include monitoring orders, observation, interception of telecommunications, access to computer systems and orders to produce specific documents."

The Explanatory Report to the 1990 Convention (para. 30) indicates that "[p]aragraph 2 of the article was drafted to make States aware of new investigative techniques which are common practice

See, e.g.: Guide for the thematic discussion on strengthening the use of digital evidence in criminal justice and countering cybercrime, including the abuse and exploitation of minors in illegal activities with the use of the Internet. Note by the Secretariat. Commission on Crime Prevention and Criminal Justice, thirty-first session, Vienna, 16–20 May 2022 (UN Doc. E/CN.15/2022/6 of 4 Mar. 2022), paras. 20–24, 67.

in some States but which are not yet implemented in other States. The paragraph imposes an obligation on States at least to consider the introduction of new techniques which in some States, while safeguarding fundamental human rights, have proved successful in combating serious crime. Such techniques could then also be used for the purposes of international cooperation. In such cases, Chapter III, Section 2, would apply. The enumeration of the techniques is not exhaustive."

As one can see, SITs were initially conceived as a mixture of judicial/law enforcement intelligence measures, not necessarily of a surreptitious nature, including such patently overt judicial measure as a production order.

The Explanatory Report to the 1990 Convention may be held to elucidate what was, is and will always be "special" about SITs in art. 4 (also, in comparison with "ordinary" "Investigative measures" in art. 3) and in any other document applying the inseparable words of the term since then — they were "new" and not "common" to all States. (However, it is difficult to accept the novelty (or comprehend how they can otherwise be uncommon or special) of such old-timers as physical surveillance, undercover activities, use of informants, production orders (subpoenas, warrants) and other classical police and criminal justice tools.)

The Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism of 2005 largely reproduces the wording of the 1990 Convention in relation to SITs, and its Explanatory Report (para. 85) again, in 15 years, calls them "new" and not "common" to all States. Currently, after a lapse of another 15 years, in the CoE Member States this is definitely not the case anymore.

It is therefore clear that presently the adjective "special" has no added value, failing to convey its meaning, and the term "SIT" as a whole may be perceived as a misnomer, as vague and lacking legal certainty as it was over 30 years ago encapsulating its "zero-day" vulnerability.

The terminological deficiencies and lack of a uniform concept of SITs also result in the divergent scopes of the relevant measures and inconsistent usage throughout various documents, primarily

either equating them with only covert actions[1] or, as was discussed above, including some overt activities in them as well.

In addition, as will be shown further, some countries' legislation distinguishes between covert and overt criminal intelligence measures (the latter include inspection of premises, vehicles and objects, identification (lineups, identity parades etc.), sampling, interviews etc.), which should be taken into account when developing a definition of a SIT that would be acceptable to those countries, by underscoring the covert type, and its denomination to import secretness in and of itself, which is not the case with the current designation of a SIT.

At present, there is no universally recognized definition of the legal phenomenon of SITs.

The Legislative Guide to the 2000 Organized Crime Convention defines SITs as "techniques for gathering information in such a way as not to alert the target persons, applied by law enforcement officials for the purpose of detecting and investigating crimes and suspects."[2]

The authors of a 2022 UNODC publication venture their own, admittedly overly broad and multifaceted, rendering of the definition and concept claiming that "[t]he [special investigative] techniques are labelled "special" because their use is often costly and complicated, requiring specialized expertise and sometimes advanced technological knowledge and instruments. Their use may in some cases pose ethical problems, while in others it may endanger the operators. It is important to keep in mind that the use of special investigative techniques may infringe on fundamental individual rights (e.g., the right to privacy)".[3]

---

[1] See, e.g.: Good practices in special investigative techniques. Background paper by the Secretariat. Conference of the Parties to the United Nations Convention against Transnational Organized Crime, Working Group on the Smuggling of Migrants, Vienna, 11-13 Nov. 2013 (UN Doc. CTOC/COP/WG.7/2013/2 of 7 Aug. 2013), para. 8 ("Special investigative techniques, also known as "covert investigation techniques" differ from routine investigation methods, and include both covert techniques and the use of technology").

[2] *Legislative guide for the implementation of the United Nations Convention against Transnational Organized Crime* (New York: United Nations, 2004), paras. 442–455.

[3] *Digest of cyber organized crime. Second edition* (Vienna: United Nations, 2022), pp. 32, 111–118, 123–124.

A 2023 UNOCT and INTERPOL joint publication states that "[s]pecial investigative techniques are typically characterized as operational resources that can be deployed both preemptively and reactively in the context of detecting and investigating serious crimes and suspects, with the aim of gathering information in such a way as not to alert the target persons. The use of SITs may also involve a degree of deception."[1]

A regional CoE definition of SITs was introduced in 2005 and is currently reproduced in the Recommendation of the Committee of Ministers of the Council of Europe to Member States on "special investigation techniques" in relation to serious crimes including acts of terrorism of 2017 (hereinafter referred to as "the 2017 Recommendation"),[2] which defines SITs as "techniques applied by the competent authorities in the context of criminal investigations for the purpose of preventing, detecting, investigating, prosecuting and suppressing serious crimes, aiming at gathering information in such a way as not to alert the target persons". "Competent authorities" means judicial, prosecuting and investigating authorities involved in deciding, supervising or using SITs in the context of criminal investigations in accordance with national legislation. SITs are applied both in a judicial context and for purposes of intelligence gathering outside of a judicial context. The scope of this Recommendation is only the application of SITs in a judicial context, including for the purposes of financial or cyber investigations.

The Explanatory Memorandum to the 2017 Recommendation gives a non-exhaustive list of SITs: for the purpose of this Recommendation, SITs may include undercover operations (including

[1] *Cybersecurity and New Technologies. Guide for Human-Rights Based Approach to Countering Use of New Technologies for Terrorist Purposes* (New York: United Nations Office of Counter-Terrorism (UNOCT), 2023), pp. 18–19, 40–42 and 69.

[2] Recommendation CM/Rec(2017)6 of the Committee of Ministers to member States on "special investigation techniques" in relation to serious crimes including acts of terrorism (Adopted by the Committee of Ministers on 5 July 2017 at the 1291st meeting of the Ministers' Deputies), Explanatory Memorandum thereto. It has replaced Recommendation Rec (2005)10 of the same name (hereinafter referred to as "the 2005 Recommendation"), which was the first to establish a SIT definition. As a precursor thereto, one can regard Recommendation Rec (2001)11 concerning guiding principles on the fight against organised crime, which in para. 19 gives national-level examples of "investigative measures (techniques)" (surveillance, interception of communications, undercover operations, controlled deliveries and the use of informants).

covert investigations); front store operations (e.g. undercover company); informants; controlled delivery; observation (including cross-border observation); electronic surveillance of specific targets; interception of communications; cross-border (hot) pursuits; pseudo-purchases or other "pseudo-offences", covert monitoring of financial transactions and web traffic as they are defined in national legislation.

This definition may be said to also include purely judicial actions that cannot be considered as such techniques due to their overt character, like examining people other than the subject himself or seizing documents while taking basic precautions not to alert the target through imposing various forms of non-disclosure obligations upon the persons directly involved in those actions, issuing gagging orders, for example, in the legal process preventing default notification by telecom service providers to subscribers whose data are subject of a preservation or production order; or such measures as remote sensing, gathering open source intelligence, especially through the use of "cold computers" unlinked to any government IP address, "dummy" social media accounts to anonymously search open and public information (i.e., not engaging in undercover work per se, but for viewing purposes), consensual monitoring or trash runs (dumpster diving); facial recognition and any other type of algorithmic profiling technologies applied in specific intelligence-led policing or predictive policing.[1]

The CoE's AML/CFT framework (the 1990 Convention (arts. 3, 4, 7 and 8) and the 2005 Convention (arts. 2, 4, 7, 15 and 16)) regulates

[1] At the same time, some other parts of these documents do point, although not consistently, to the covert nature of SITs. According to the 2017 Recommendation (preamble), "special investigation techniques are numerous, varied and constantly evolving, and […] their common characteristics are their covert nature and the fact that their application could interfere with fundamental rights and freedoms; […] the use of special investigation techniques in criminal investigations requires confidentiality and […] any efforts to pursue the commission of serious crime, including acts of terrorism, should where appropriate be thwarted with secured covert means of operation". The Explanatory Memorandum to the 2017 Recommendation (paras. 17 and 31) sets out that "SIT are particular techniques because of their covert nature"; "SIT are *often* (italics mine) of a covert nature, which is present where an attempt is made to conceal the on-going criminal investigations". The 2005 Recommendation (preamble) and the Explanatory Report thereto (paras. 17 and 27) contain the same provisions but for the language, using the words "secret" and "secrecy" in place of the "covert (nature)" in the respective parts of the text.

SITs at the national level only and the international assistance in broad terms with respect to instrumentalities, proceeds and other property.

Other CoE conventions providing (explicitly in their texts or implicitly through their explanatory reports with examples) for domestic-level, but not international-level SITs, are the 1999 Criminal Law Convention on Corruption,[1] the 2011 Convention on the counterfeiting of medical products and similar crimes involving threats to public health[2], and the 2015 Convention against Trafficking in Human Organs.[3]

The next section will focus on the CoE core treaties — the European Convention on Mutual Assistance in Criminal Matters of 1959 (hereinafter referred to as "the 1959 Convention" or "mother Convention") and its two additional protocols — that do not actually use the term "SIT", but, as distinct from the instruments discussed above, are not sectoral and ordinarily apply to all kinds of criminal offences.

III. To What Extent Are SITs Covered in the 1959 Convention and Its Protocols? Domestic vs. Cross-Border SITs

The Contracting Parties' undertaking under art. 1.1 of the 1959 Convention to afford each other "the widest measure of mutual assistance" is not a self-standing and unqualified clause; it only operates through art. 3.1 and in conjunction with the rest of the Convention's articles governing concrete forms of this assistance, which on their own do not provide for covert SITs.

---

[1] Art. 23 ("Measures to facilitate the gathering of evidence and the confiscation of proceeds"), Explanatory Report (para.114) ("this provision includes an obligation for the Parties to permit the use of "special investigative techniques". No list of these techniques is included but the drafters of the Convention were referring in particular to the use of under-cover agents, wire-tapping, bugging, interception of telecommunications, access to computer systems and so on.")

[2] Art. 16 ("Criminal investigations"), Explanatory Report (para. 109) ("Effective investigation" is further described as including financial investigations, covert operations, controlled delivery and other special investigative techniques. These could encompass electronic and other forms of surveillance as well as infiltration operations.")

[3] Art. 16 ("Criminal investigations"), Explanatory Report (para. 102) ("The negotiators noted that conducting effective criminal investigations may imply the use of special investigation techniques in accordance with the domestic law of the Party in question, such as financial investigations, covert operations, and controlled delivery.")

In accordance with art. 3.1 of the 1959 Convention, "[t]he requested Party shall execute in the manner provided for by its law any letters rogatory relating to a criminal matter and addressed to it by the judicial authorities of the requesting Party for the purpose of procuring evidence or transmitting articles to be produced in evidence, records or documents."

To ascertain the purpose of the document and properly interpret its authors' intentions, one should refer, among others, to its *travaux préparatoires*.

Pursuant to the Explanatory Report to the 1959 Convention (commentary on art. 3), "[t]he expression "procuring evidence" refers, inter alia, to the hearing of witnesses, experts or accused persons, the transport involved *[sic]* as well as search and seizure."

In addition, among its general considerations, the Explanatory Report states that "it was agreed that assistance should be granted in the case of minor offences and that as a general rule the offence need not be an offence under the law of both countries", which is rather incompatible with the overall intrusive and covert nature of SITs.

Down the road, the state of affairs and new developments in crime and in combating criminal offences called for the adoption of the Recommendation of the Council of Europe's Committee of Ministers to Member States concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications of 1985[1] (hereinafter referred to as "the 1985 Recommendation") and then the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters of 2001 (hereinafter referred to as "the 2001 Protocol"), respectively, to read into the 1959 Convention's scope and further to expressly envisage in the 2001 Protocol, a limited number of covert forms of cooperation as well.

Notwithstanding the presence of the phrase *"inter alia"*, it appears evident that initially, in principle just procedural actions of a public, or overt nature were meant to be included in the scope of the 1959 Convention, since there was no mention of a single clandes-

[1] Recommendation No. R (85)10 of the Committee of Ministers to Member States concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications (Adopted by the Committee of Ministers on 28 June 1985 at the 387th meeting of the Ministers' Deputies).

tine operation to exemplify the inclusion thereof, although at least some of them were undoubtedly existent at the time and could have hardly escaped the drafters' scrutiny. As discussed elsewhere in this chapter, it was only in 1990 that the CoE Anti-Money Laundering Convention introduced SITs, labelling them "new". The 1978 and 2001 Protocols changed nothing as regards the "SITless" scope of art. 3 of the mother Convention.

Additionally, the Explanatory Report to the 2001 Protocol in the commentaries on articles concerning SITs states that "the purpose of the drafters when taking account of [the respective covert measures] in this Protocol was not to include police or other forms of non-judicial co-operation within the scope of this Protocol, but rather to take in [those measures] as a form of mutual legal assistance". Similar attempts at justification are absent in the Explanatory Report to the 1959 Convention, which, again, allows to argue that covert SITs, domestic or let alone cross-border, were not intended to be covered by the mother Convention.

The distinction between cross-border (transnational) and domestic (internal) SITs drawn in this chapter is meant to make it clear that the former are carried out in the territories of at least two countries, i.e. of the requesting and the requested States, and/or as inherently joint operations by both States' competent authorities (e.g., controlled deliveries etc.), or else as actions of the requesting or notifying State's authorities which they conduct on their own and which are carried out on or otherwise involve, only the territory of the other concerned (requested or notified) State, therefore requiring the latter's consent (e.g., where they conduct covert investigations on foreign soil themselves, or transborder telecommunications interception, remote search in information systems and networks); whereas the latter are only conducted within the requested State's boundaries solely by its domestic authorities in behalf of the requesting State (as an exception and if permitted by the requested State, also in the presence of the requesting State's officials pursuant to art. 4 of the 1959 Convention).

A CoE publication asserts that "[a]lthough the *European Convention on Mutual Assistance in Criminal Matters* does not specifically address special investigative techniques as a measure of assistance, it is quite clear that co-operation of such measures was envisaged within the context of assistance (See Recommendation No. R (85) 10 sets out fairly detailed rules in relation to requests for intercep-

tion of communications under the European Convention on Mutual Assistance in Criminal Matters) and subsequently set out in *The 2nd Additional Protocol to the European Convention on mutual assistance in criminal matters* through the following provisions: Article 18: controlled delivery; Article 19: covert investigations; Article 20: joint investigation teams."[1]

This interpretation is far-fetched as it endeavors to stretch the mother Convention out to be comprehensive, which it is not, that fact bringing about the subsequent adoption of sectoral CoE conventions on cooperation in criminal matters, including the 2001 Budapest Convention on Cybercrime, whose harbinger the 1985 Recommendation actually was. The Recommendation means only so much that the States Parties to the 1959 Convention had agreed to deem the Convention applicable to requests for domestic intercepts, and is understandably silent on any other SITs. The circumstance that the 2001 Protocol subsequently extended the mother Convention's scope to encompass some selected cross-border, but not domestic SITs, adds little or nothing to the authors' argument.

Notwithstanding its non-binding soft law character, the 1985 Recommendation has a self-contained régime, enumerating, *inter alia*, the mandatory grounds for refusal of assistance irrespective of those set out in the 1959 Convention, contents of requests, and conditions of their execution.

The 1985 Recommendation and consequently the 1959 Convention may also be considered to envisage the bulk interception of communications, communications data and sharing of their product with foreign judicial and law enforcement counterparts for further data mining, analyzing and filtering for criminal investigation purposes using tasked selectors (search terms), while observing the standards and safeguards similar to those recently determined by the ECHR in respect of intelligence services' activities.[2]

Except for interception of communications, *covert* SITs enumerated in section II of this chapter, with no cross-border components, fall outside the scope of the 1959 Convention and its two Protocols

[1] *The Deployment of Special Investigative Means* (Belgrade: Council of Europe Office in Belgrade, 2013), p. 81.

[2] *Big Brother Watch and Others v. the United Kingdom* [GC], nos. 58170/13, 62322/14 and 24960/15, 25 May 2021, ECHR; *Centrum för rättvisa v. Sweden* [GC], no. 35252/08, 25 May 2021, ECHR.

and are arguably not available to be performed in the domestic context of the requested States under them.

Unlike domestic and cross-border interceptions of telecommunications, for example, under the 2000 Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, the 1959 Convention and its Protocols' framework does not cover a cross-border interception of telecommunications, since where the 2001 Protocol does regulate the cross-border forms of assistance, it addresses them explicitly as such in the dedicated provisions, which, in turn, may normally be subject to exclusion and other reservations by Contracting States due to their significant implications for the States' sovereignty. As opposed to art. 3 regime, they are discretionary rather than mandatory and are scarcely applicable to *corpora delicti* that do not satisfy the requirement of dual criminality, non-extraditable or administrative (under art. 1.3 of the 1959 Convention as amended by the 2001 Protocol) offences. All other requested actions under arts. 3, 5 and the rest of the 1959 Convention and its Protocols are assumed, as a general rule, to be domestic (internal) in character, that is, carried out within the requested State's territory in behalf of the requesting State, unless there is a clear indication to the contrary in the texts.

Thus, the drafting history of the 1959 Convention,[1] its text and other CoE instruments and tools for their implementation as well as subsequent agreements and practice of their application which are analyzed here, attest to the 1959 Convention being regarded as not governing SITs (except for domestic intercepts).[2]

To rectify this, a new CoE document containing the express provisions to the contrary should be adopted.

---

[1] Vienna Convention on the Law of Treaties of 1969 (art. 32).

[2] This conclusion is also strongly supported by the continued process of countries submitting their relevant proposals of amendments, however fragmentary, for inclusion in the prospective third additional protocol to the 1959 Convention. See e.g. the proposal by Switzerland to introduce a new article on the use of technical recording devices in the territory of another Party (Draft Third Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters: Document prepared by the Secretariat, Strasbourg, 8 September 2023 [PC-OC/(2023)07E], p. 5).

IV. Other International and Domestic Legal Frameworks. Problems of Coverage, Relationship, and Differences in Interpretation and Application: Legal (Judicial) vs. Law Enforcement Assistance

The UN Conventions against Transnational Organized Crime of 2000 (arts. 20 and 27) and Corruption of 2003 (arts. 48 and 50) lay the universal foundations for SITs,[1] while separating them from mutual legal assistance in the dedicated articles. However, their provisions are not "self-executing" for all States as they require further international agreements or arrangements, or purely discretionary decisions on a case-by-case basis, therefore not being a sufficient source of legal authority.[2] SITs may also be

[1] It is sometimes argued that because of its art. 9, the 1988 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances may be considered to be a precursor to what would follow in other conventions in terms of introducing SITs. See: H.G. Nilsson, "Special Investigation Techniques and Developments in Mutual Legal Assistance — The Crossroads between Police Cooperation and Judicial Cooperation", in *Resource Material Series No. 65, United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders (UNAFEI)* (Fuchu, Tokyo, Japan, Mar. 2005), p. 40.

The same can be said about older treaties, especially bilateral ones, dating back to earlier decades, where their scope was framed in terms of procedural stages of combating crime, such as any assistance in preventing, detecting, disrupting, investigating, solving, prosecuting and adjudicating offences, but without explicitly naming covert means and methods. See, e.g., International Convention for the Suppression of the Circulation of and Traffic in Obscene Publications of 12 Sept. 1923 (with the Agreement for the Suppression of the Circulation of Obscene Publications of 4 May 1910), as amended by the Protocols of 1947 and 1949 respectively.

The 1990 Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders and the 1990 Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime were the earliest international treaties to expressly deal with this subject matter, and it is the latter that introduced the term "SIT" in art. 4.

At the international level, the 1988 Convention was the first multilateral agreement to endorse the investigative technique and practice of controlled delivery.

[2] In more detail, see: International cooperation involving special investigative techniques. Background paper prepared by the Secretariat. Conference of the Parties to the United Nations Convention against Transnational Organized Crime, Working Group on International Cooperation, Vienna, 7 and 8 July 2020 (UN Doc. CTOC/COP/WG.3/2020/3 of 12 May 2020), paras. 41–51; *Legislative guide for the implementation of the United Nations Convention against Corruption. Second Revised Edition 2012* (New York: United Nations, 2012), para. 650.

considered under other universal sectoral conventions, in the first place, counter-terrorism ones, as well as Security Council resolutions. However, in most cases, because of their general catchall language not expressly indicating covert SITs, they can hardly qualify to create the sufficient binding international obligations with respect to SITs.

The same is true for the FATF Recommendations (31, 37 and 40) which establish the relevant national- and international-level provisions. Under them, countries should ensure that competent authorities conducting investigations are able to use a wide range of investigative techniques suitable for the investigation of money laundering, associated predicate offences and terrorist financing. These investigative techniques include: undercover operations, intercepting communications, accessing computer systems and controlled delivery. Countries should ensure that, of the powers and investigative techniques required under Recommendation 31, and any other powers and investigative techniques available to their competent authorities are also available for use in response to requests for mutual legal assistance, and, if consistent with their domestic framework, in response to direct requests from foreign judicial or law enforcement authorities to domestic counterparts. Law enforcement authorities should also be able to use their powers, including any investigative techniques available in accordance with their domestic law, to conduct inquiries and obtain information on behalf of foreign counterparts.[1]

Still, the major deficiencies of the said UN and CoE frameworks regarding SITs stem from their sectoral character, leaving ordinary crime out.

The actions at issue are governed by a number of the European Union supranational instruments,[2] multilateral treaties concluded within other regional and sub-regional international organizations

[1] FATF (2012-2023), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation,* FATF, Paris, France, www.fatf-gafi.org/recommendations.html

[2] For the detailed analysis of the main types of SITs, see: *Study on paving the way for future policy initiatives in the field of fight against organized crime: the effectiveness of specific criminal law measures targeting organised crime. Final report, February 2015* (Luxembourg: Publications Office of the European Union, 2014), pp. 221–337.

(e.g., CIS, SCO and CSTO),[1] or bilateral interstate, intergovernmental[2] and even interagency agreements and other arrangements[3] gov-

[1] Convention on Legal Assistance and Legal Relations in Civil, Family and Criminal Matters of 7 Oct. 2002 (Kishinev Convention) (arts. 6–7, 60–61, 63, 104 and 108 ("search for persons and tracing proceeds of crime", "operational measures", "search measures" or "operational search measures", "controlled delivery", and "joint investigative and operational teams")); Agreement on Cooperation between the Governments of the Member States of the Shanghai Cooperation Organization in Fighting Crime of 11 June 2010 ("search for persons", "operational search measures", and "controlled delivery"); Agreement on Cooperation of the Member States of the Commonwealth of Independent States in Combating Crimes in the Sphere of Information Technologies of 28 Sept. 2018, Protocol on Interaction of the Member States of the Collective Security Treaty Organization in Countering Criminal Activities in Information Sphere of 23 Dec. 2014 ("operational search measures", "coordinated measures and operations for preventing, detecting, suppressing, solving and investigating crimes"); Shanghai Convention on Combating Terrorism, Separatism and Extremism of 15 June 2001 ("operational search measures"); Agreement on Cooperation of the Member States of the Commonwealth of Independent States in the Fight against Illicit Traffic in Narcotic Drugs, Psychotropic Substances and Precursors of 30 Nov. 2000 (as amended by the Protocol of 25 Oct. 2019) ("controlled deliveries", "complex coordinated or joint operational search measures, special operations", and "joint investigative and operational teams").

See also on the CSTO and CIS model legislation: Resolution of the Parliamentary Assembly of the Collective Security Treaty Organization of 19 Dec. 2023 No. 16-7.3 "On the Draft Model Guidance of the Competent Authorities of the CSTO Member States in the Sphere of Ensuring the Collective Security by Operational Search Activities"; Resolution of the Parliamentary Assembly of the Collective Security Treaty Organization of 30 Oct. 2018 No. 11-4 "On the Draft Model Agreement on Cooperation of the CSTO Member States in the Sphere of Operational Search Activities"; Resolution of the Parliamentary Assembly of the Collective Security Treaty Organization of 26 Nov. 2015 No. 8-14 "On the Draft Recommendations for the Approximation and Harmonization of Laws of the CSTO Member States on Operational Search Activities"; Model Law on Operational Search Activities, adopted by Resolution of the Interparliamentary Assembly of the CIS Member Nations of 6 Dec. 1997 No. 10-12.

[2] Agreement between the Government of the Russian Federation and the Government of the United Kingdom of Great Britain and Northern Ireland on Co-operation in Fighting Crime of 6 Oct. 1997 (art. 1; Russian "operational search measures" are translated therein as "inquiries"); Agreement between the Government of the Russian Federation and the Government of the Federal Republic of Germany on Cooperation in Fighting Especially Dangerous Crimes of 3 May 1999 (art. 3 ("coordinated operational measures for preventing, detecting, disrupting and solving crimes")).

[3] Agreement on Cooperation between the Ministries of Internal Affairs in Combating Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 21 Oct. 1992 (concluded by the MoIs of the CIS Member States and the Republic of Estonia) ("operational search measures", "incessant operational surveillance of movements

erning law enforcement assistance in combating crime, requesting and executing both domestic and cross-border operational measures. These agreements normally do not apply to legal assistance in criminal matters, and many of them explicitly state this, although they may be used to procure both leads and evidence. (Mutual legal assistance may only constitute subject matter of treaties of the interstate level.)

Conversely, in a vicious circle for Russia and many other Commonwealth of Independent States (CIS) countries, legal (judicial) assistance treaties are not applicable to SITs which are the subject matter of those law enforcement assistance agreements, either, unless the treaties themselves, and they are few, like the 2001 Protocol or the 2002 Kishinev Convention, or sources of their authentic interpretation, have provisions to the contrary. Unlike the broad language of art. 3 of the 1959 Convention, for example, bilateral treaties on legal assistance in criminal matters to which the Russian Federation is party normally employ an enumerative approach to measures that may be requested and executed under the treaty, and there are no SITs among them.

This relationship problem was already addressed briefly by the PC-OC back in 2001, mentioning in passing that "[i]t appears that the borders between judicial and police co-operation are not always clear. For example, some see the 2nd Additional Protocol as an unhappy development consisting of introducing police co-operation into the framework of the Convention on Mutual Legal Assistance. Others however welcome that same development, considering it rather as a method of controlling police activities by judicial authorities."[1]

---

of drug dealers possessing interstate connections", "coordinated measures (operations) for blocking channels of illicit movement of narcotic drugs", "controlled deliveries", and "joint groups for joint operational search measures"); Agreement on Cooperation in the Field of Special Support to Operational Search Activities of 18 Dec. 1998 (concluded by the MoIs of some CIS Member States) ("operational search measures", "operational intelligence", "surveillance subject (target)", and "special support to operational search activities for the purposes of preventing, detecting, suppressing and solving crimes").

[1] Judicial collaboration versus police collaboration. Subject submitted for discussion in the PC-OC at its 43rd meeting in 2001 by Mr M. Knaapen (Netherlands). Strasbourg, 30 Jan. 2013 [PC-OC\Docs 2001\20Erev].

As was already mentioned above, the Explanatory Report to the 2001 Protocol in the commentaries on arts. 17–19 (cross-border observations, controlled delivery and covert investigations) flags up rather inconclusively[1] that "the purpose of the drafters when taking account of [the respective covert measures] in this Protocol was not to include police or other forms of non-judicial co-operation within the scope of this Protocol, but rather to take in [those measures] as a form of mutual legal assistance".[2]

There is an exception to the above in relation to the interception of communications. In Russia and some other CIS Member States, wiretapping, "pen registers", "trap and trace devices" using existing software and hardware at the Internet service or telecommunications providers,[3] real-time collection of electronic traffic (transactional, communications) or content data in transit during criminal investigations and proceedings may take the form both of a procedural, judicial action (proceeding) and of a criminal intelligence operation, both being performed for evidentiary purposes and requiring a court warrant.[4] On the other hand, operational measures that involve covert equipment or other property interference other than that using service providers' facilities, such as electronic eavesdropping (bugging of premises, vehicles, i.e., the so-called intrusive covert surveillance, or use of a "body wired" informant to record conversations that take place within his earshot), or deployment of

[1] *Ibid.*

[2] SITs can also be carried out through another form of legal assistance envisaged in art. 20 of the 2001 Protocol (joint investigation teams).

[3] As well as production orders for their stored wire or electronic communications records, including cell tower dumps.

[4] Cf.: the Russian Federation's Criminal Procedure Code of 2001, as last amended Nov. 27, 2023, establishing the proceedings for inspection and seizure of postal or telegraphic correspondence, electronic communications or other communications transmitted through telecommunication networks (art. 185); monitoring or recording of telephone or other conversations (art. 186); and obtaining information on connections between subscribers or subscribers' devices (art. 186.1); and Federal Law no. 144-FZ, "On Operational Search Activities", of Aug. 12, 1995, as last amended Dec. 29, 2022, establishing the following operational search measures: control of postal, telegraphic or other communications; wiretapping; capturing information from technical communications channels; and obtaining computer information (art. 6).

cell-site simulators[1] fall within the exclusive domain of criminal intelligence operations.

Therefore, the application of the 1959 Convention by such countries to domestic interceptions as interpreted by the 1985 Recommendation should not face any legal difficulties. (And the Recommendation concerns the interpretation of requested domestic, but not transnational intercepts.)

Apart from that, SITs are traditionally regulated by multilateral and bilateral treaties and other instruments on mutual administrative assistance in customs matters.[2]

International assistance in operational intelligence investigations is expressly[3] or by implication[4] provided for in Status of Forces Agreements and treaties on similar overseas installations.[5]

---

[1] IMSI catchers, digital analyzers like a stingray, dirtbox or triggerfish.

[2] Recommendation of the Customs Co-operation Council on Mutual Administrative Assistance of 5 Dec. 1953 ("special watch"); International Convention on Mutual Administrative Assistance for the Prevention, Investigation and Repression of Customs Offences of 9 June 1977 ("(special) surveillance"); International Convention on Mutual Administrative Assistance in Customs Matters of 27 June 2003, Model Bilateral Agreement on Mutual Administrative Assistance in Customs Matters, as revised in June 2004 ("surveillance, controlled delivery, hot pursuit, cross-border surveillance, covert investigations, and joint control and investigation teams").

[3] Agreement between the Russian Federation and the Republic of Armenia on Jurisdiction and Mutual Legal Assistance in Matters relating to the Stationing of the Russian Military Base on the Territory of the Republic of Armenia of 29 Aug. 1997 ("search for persons", "search actions", and "operational search actions"); Agreement between the Russian Federation and the Republic of Tajikistan on Jurisdiction and Mutual Legal Assistance in Matters related to the Stay of Military Formations of the Armed Forces of the Russian Federation on the Territory of the Republic of Tajikistan of 21 Jan. 1997 ("search for persons", "search actions", and "joint operational and investigative groups (brigades)").

[4] Agreement between the Parties to the North Atlantic Treaty regarding the Status of their Forces of 19 June 1951 (art. VII.6.a ("The authorities of the receiving and sending States shall assist each other in the carrying out of all necessary investigations into offences, and in the collection and production of evidence, including the seizure and, in proper cases, the handing over of objects connected with an offence.")).

[5] Agreement between the Government of the Russian Federation and the Government of the Republic of Kazakhstan on Interaction between Law Enforcement Authorities in Ensuring Legal Order on the Territory of the Baikonur Complex of 4 Oct. 1997 ("operational search measures", "operational support of criminal cases", and "joint operational and investigative groups (brigades)").

The dedicated regional SIT-related instruments are also the Agreement on the Procedure for Establishing and Operation of Joint Investigative and Operational Teams in the Territories of the Member States of the Commonwealth of Independent States of 16 October 2015 ("operational search measures") and the Treaty on the Procedure for the Stay and Interaction of Law Enforcement Officers on the Territories of Member States of the Commonwealth of Independent States of 4 June 1999 ("operational search measures", "observation", and "hot pursuit").

Some but not all CoE countries can cooperate in the field of SITs on the basis of reciprocity. For example, the Russian Federation cannot do this, as this legal basis is not provided for in its Federal Law "On Operational Search Activities", requiring the treaty basis for executing SITs.

There have been global initiatives concerning the integration of SITs into the mutual legal assistance framework.[1]

One may assert that currently the CoE Member States have a patchwork and insufficient regulation of the subject at stake in terms of it not being streamlined in the framework of the Council's treaty law and not covering major crime area. It definitely requires the advanced harmonization in a CoE treaty.

Some CoE Member States, in particular CIS countries, have standalone laws on SITs, whose concrete denominations vary (the most common one is "On Operational Search Activities"[2]) and which are ordinarily not part of criminal procedure *sensu stricto*.[3] Nor are "op-

[1] UNODC 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).

[2] In Russian speaking countries, *operativno-razysknaya deyatel'nost'*. It is sometimes referred to as "operational investigative activities (measures)", which is not a literal translation.

[3] For instance, the Russian Federation's Federal Law "On Operational Search Activities" (art. 6) establishes the following exhaustive list of 15 covert and overt operational search measures that are common for intelligence, counterintelligence and criminal intelligence authorities: interview; enquiries; gathering samples for comparative analysis; test purchase; examination of objects or documents (a draft amendment adds computer information thereto); surveillance; identification of persons; inspection of premises, buildings, constructions, areas or vehicles; control of postal, telegraphic or other communications; wiretapping; capturing information from technical communications channels; infiltration; controlled delivery; operational experiment (i.e., a sting operation); and obtaining computer information.

erational search activities" a component of "investigative actions" in those countries, as the latter constitute proceedings, are in essence judicial. (Much of this stuff lies, of course, in the nametag terrain of the differing legal systems.) The results of the measures performed pursuant to these laws normally need to pass through a certain validation and legalization process prior to becoming admissible evidence for a criminal case. These actions can be conducted both before the institution of a criminal case and in the course of pre-trial criminal proceedings, for intelligence-gathering and evidential purposes, proactively and reactively.[1]

Thus, Russia and other countries of the CIS have generally established a special regime for disclosing and using the results of *covert* SITs in criminal proceedings different from that of ordinary, overt investigative actions. As a general rule, they constitute a State secret and are to be declassified prior to their introduction as evidence into a criminal case. This has a bearing on the international cooperation where the requested measures are covert SITs, since the resulting records and other documents should go through a declassification procedure before their transfer to the requesting foreign State or, if they cannot be declassified, the transmittal abroad can only take place if both the requesting State and the requested State are parties to special bilateral or multilateral agreements on security procedures for exchanging and protecting classified information.[2]

[1] For in-depth analyses of the CIS countries' domestic legal frameworks and practice, see: N. Kovalev and S.C. Thaman, *Special investigative techniques in post-Soviet states: the divide between preventive policing and criminal investigation*, in: J.E. Ross and S.C. Thaman (eds), *Comparative Criminal Procedure* (Cheltenham, UK; Northampton, MA, USA: Edward Elgar Publishing, 2016), pp. 453–474; *Analysis of the Legislation of the Kyrgyz Republic on Special Investigative Measures* (B.: United Nations Office on Drugs and Crime, 2014), 122 p.; L.A. McCarthy, *Trafficking Justice: How Russian Police Enforce New Laws, from Crime to Courtroom* (Ithaca and London: Cornell University Press, 2015), 276 p.

[2] See: intergovernmental agreements on mutual protection of classified information, e.g., Russia–Germany, Russia–Poland Intergovernmental Agreements on Mutual Protection of Classified Information of 2 Dec. 1999 and 8 Feb. 2008 respectively; Agreement on mutual safeguarding of classified information in the framework of the Collective Security Treaty Organization of 18 June 2004 (as of 19 Dec. 2012); Agreement between the Government of the Russian Federation and the European Union on the protection of classified information of 1 June 2010 (not yet in force); Resolution of the Government of the Russian Federation No. 973 of 2 Aug. 1997 "On Approval of the Regulations for Preparing the Transmission of Information Constituting a State Secret to Other States or International Organizations" (as of 18 Mar. 2016); RF Interagency Instructions on the Procedure

At the same time, many CoE Member States have SITs (criminal intelligence operations) incorporated in their laws on criminal procedure and statutes on international mutual legal assistance, thus there appears to be a convergence of procedural and criminal intelligence activities, on the one hand, and of legal (judicial) and law enforcement (police-to-police) international assistance,[1] on the other hand, to some extent, with treaties like the 2001 Protocol following suit.

Currently, we are witnessing the dissolution of boundaries between the procedural pre-trial (preliminary) investigation and operational investigation/intelligence activities in the countries where these institutions have long been separated. These two investigative concepts are integrating mainly due to the incorporation of operational/intelligence activities into criminal procedure.[2]

For example, as a type of procedural activities (proceedings) identical or similar to "operational search measures" *(operativno-razysknyye meropriyatiya)* in Russian law, the Code of Criminal Procedure of Ukraine of 2012 (arts. 246–275) governs the grounds and the procedure for carrying out "covert investigative (search) actions" *(негласні слідчі (розшукові) дії)*;[3] the Criminal Procedure Acts of the Czech Republic of 1961 (§§ 86–87c and 158b–158f) and Slovakia of 2005 (§§ 110–118) (with later amendments) mainly in

for Presenting Results of Operational-Search Activities to Inquiry Authority, Investigator or Court of 27 Sept. 2013 which is also applicable to the transfer of results of overt and covert operational-search activities pursuant to the requests of international law enforcement organizations and law enforcement authorities of foreign States, including the procedures for declassifying information constituting State secrecy and its media.

[1] H.G. Nilsson, *op. cit.*, pp. 39–45; 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.

[2] For the concept of "criminal justice finality", see: G. Vermeulen, W. De Bondt, C. Ryckman, *Rethinking international cooperation in criminal matters in the EU. Moving beyond actors, bringing logic back, footed in reality* (Antwerpen-Apeldoorn-Portland: Maklu, 2012), 767 p.

[3] At the same time, the Law of Ukraine "On Operational Search Activities" of 1992 (with further amendments) still regulates operational investigative, intelligence and counterintelligence activities.

Similar dual mixed regulation is contained in the respective laws of the Baltic countries. See: V.M. Turanjanin and J.V. Stanisavljević, "Special investigative actions in Baltic countries", *Strani pravni život* god. LXV, br. 4 (2021): 667–685.

Ch. "Providing Information" as distinct from the next Ch. "Proof"), while retaining the previous denomination, — "operational search means" *(operativně pátrací prostředky)*[1] *and "means of operational search activity" (prostriedky operatívno-pátracej činnosti*)[2]; the Austrian Criminal Procedure Code of 1975 (§§ 99, 118 and 129–133) governs the actions analogous to "operational search measures" in Sec. "Investigative Measures and Obtaining Evidence" *(Ermittlungsmaßnahmen und Beweisaufnahme)*; the amended German Code of Criminal Procedure of 1950 (§§ 98a–98c, 100c–101, 103, 110a–111 and 163e–163f) in the special section along with seizure, attachment of property and correspondence, and interception of telecommunications; the Swiss Criminal Procedure Code of 2007 (arts. 269–298d) in Sec. "Covert Surveillance Measures" *(geheime Überwachungsmassnahmen)*. Such regulation of the grounds and the procedure for these activities is also typical for criminal procedure laws of the States of the former Yugoslavia.[3] At the same time, for example in Poland, strict separation of "operational intelligence activities" (*czynności operacyjno-rozpoznawcze)* from procedural actions remains in force to the present day.[4]

The transposition of the relevant treaty norms into the national legislation takes various forms. For example, whereas the Act of the Czech Republic "On International Judicial Cooperation in Criminal Matters" of 2013 (§§ 59–65)[5] and the Federal Law of the Republic

[1] The Act "On the Police of the Czech Republic" of 2008 (with further amendments) (§§ 10, 72–77), in turn, regulates "supporting operational search means" (*podpůrné operativně pátrací prostředky)*.

[2] The Act of the Slovak Republic "On the Police Corps" of 1993 (with further amendments) (§§ 38a–41a) also regulates "means of operational search activity" *(prostriedky operatívno-pátracej činnosti)*, which among others includes "criminal intelligence" (kriminálne spravodajstvo).

[3] *Benchbook on Special Investigative Measures* (Sarajevo: DCAF — Geneva Centre for Security Sector Governance, 2020), 116 p.; *Special Investigative Measures. Domestic and International Practice* (Skopje: OSCE Spillover Monitor Mission to Skopje, 2010), 275 p.

[4] P. Łabuz, J. Kudła, T. Safjański, *Czynności operacyjno-rozpoznawcze polskich służb ochrony prawa w prawie krajowym i międzynarodowym* (Warszawa: Difin, 2022), 436 s.; K. Ożóg-Wróbel, "Katalog metod prowadzenia czynności operacyjno-rozpoznawczych", *Roczniki Nauk Prawnych* T. XXII nr 4 (2012), s. 113–145.

[5] The Act "On the Police of the Czech Republic" (§ 91) briefly regulates the use of "supporting operational search means" pursuant to a foreign security service's request, whereas the Act of the Slovak Republic "On the Police Corps" of 1993 (§§ 77a–77c) also regulates the use of Slovak police officers abroad and foreign police

of Austria "On Extradition and Legal Assistance in Criminal Matters" of 1979, with later amendments (§§ 59b–59c, *besondere Ermittlungsmaßnahmen* ("special investigative measures")) govern the procedure for submitting and performing requests for operational/intelligence actions and classify them as legal assistance (that is, cooperation in the field of criminal proceedings), similar special statutes of Germany and Switzerland, whose criminal procedure codes in this aspect are similar to the Czech and the Austrian ones, do not contain such provisions. At the same time, it can be assumed that in regulating the execution of these incoming requests, the Czech and Austrian competent authorities expect that the requesting party file them through the legal assistance procedure rather than within the framework of law enforcement cooperation.[1] The Ukrainian Criminal Procedure Code regulates controlled deliveries and border pursuit in Ch. "International Legal Assistance in Carrying Out Procedural Actions" (arts. 569 and 570).[2]

There is an example of a CoE country regulating the extraterritorial unilateral use of SITs. The UK Home Office Codes of Practice on Covert Surveillance and Property Interference, Equipment Interference and Covert Human Intelligence Sources provide for the applicability of authorizations and warrants under the Regulation of Investigatory Powers Act 2000 and the Investigatory Powers Act 2016 to these SITs conducted in overseas areas under the jurisdiction of the UK, such as UK Embassies, UK military bases and detention facilities.[3]

officers in Slovakia for implementing particular means of operational search activity.

[1] For tracing and interception of (tele)communications; agents, informers and infiltration; and cross-border operations, see: the European Judicial Network's practical tool for judicial cooperation "Fiches Belges", URL: https://www.ejn-crimjust.europa.eu/ejn/EJN_FichesBelges/EN/-1/-1/-1, accessed July 27, 2021.

[2] See in relation to some other countries: *Terrorism: special investigation techniques* (Strasbourg: Council of Europe Publishing, 2005), 496 p.; *Legal and Gaps Analysis: Special Investigation Techniques. CrimEx EuroMed Justice Group of Experts in Criminal Matters.* Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Palestine, Tunisia, Nov. 2017, 123 p.

[3] *Covert Surveillance and Property Interference. Revised Code of Practice* (London: Home Office, 2018), p. 12, para. 2.17; *Equipment Interference. Code of Practice* (London: Home Office, 2018), p. 19, para. 3.34; *Covert Human Intelligence Sources. Revised Code of Practice* (London: Home Office, 2022), p. 25, para. 4.27.

V. Recommendations: Filling the Gaps

1. The research of the existing frameworks and the considerations set out in the previous sections point to the need for developing the additional regulation of SITs in the CoE instruments of legal assistance in criminal matters as well as to the 1959 Convention being the most appropriate among them to accommodate that.

As the 2001 Protocol is indicative of setting the sovereignty-related thresholds for the feasible cooperation forms in the field of transnational SITs[1] and regrettably, those thresholds seem to be as relevant as they were 20 years ago, back in 2001, when the Second Protocol was adopted, presently it appears advisable to confine the express regulation of SITs to domestic ones.

Since SITs involve either compulsory (coercive) measures (in their broad sense as used in CoE instruments) or deception, decoys and other trickery, most of them are highly intrusive and invade people's privacy, they should be subjected to the restrictive regime of art. 5 of the 1959 Convention, giving the States Parties more latitude in electing or refusing to accede to them.

In view of the above considerations, it is deemed expedient to supplement art. 3 of the 1959 Convention with paragraph 4 expressly stating that *"The provisions of paragraph 1 of this article shall apply to any request for the conduct of covert special investigative techniques that do not have a cross-border character"*, and to amend paragraph

[1] Cf.: para. 24 of the 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) states that "[t]he drafters also considered other measures which, after thorough discussion, were not retained in this Protocol. Two of these provisions, namely, "undercover investigations by means of a computer system" and "extension of searches", were of high interest to the Parties but were found to require additional work, time and consultations with stakeholders, and were thus not considered feasible within the time frame set for the preparation of this Protocol. The drafters proposed that these be pursued in a different format and possibly in a separate legal instrument."; Terms of reference (document T-CY (2021)19 of 15 Nov. 2021) for the T-CY Working group on undercover investigations by means of computer systems and extension of searches; 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. URL: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home, accessed Apr. 14, 2023.

Unlike the 1990 Schengen Convention, the 2001 Protocol does not provide for such an intrusive form of cooperation as hot pursuit.

1 of art. 5 of the 1959 Convention so as to read "Any Contracting Party may, by a declaration addressed to the Secretary General of the Council of Europe, when signing this Convention or depositing its instrument of ratification or accession, reserve the right to make the execution of letters rogatory for search or seizure of property, *or for the measures provided for in paragraph 4 of Article 3* dependent on one or more of the following conditions:".

This means, that, firstly, by reference to para. 1 of art. 3, the suggested SITs are only aimed at reactive criminal investigations, prosecutions and judicial proceedings and serve evidentiary purposes, and therefore exclude those employed in secret to prevent, detect or suppress offences, i.e., proactive and disruptive investigations, to say nothing of national security (as opposed to law enforcement) intelligence operations; and, secondly, they do not comprise any individually denominated actions, means or methods.

As art. 3.1 of the 1959 Convention deals with a generic definition of judicial assistance requested and provided solely for evidential purposes, and neither the rest of the Convention nor its Protocols comprise an exhaustive or approximate list of the requested parties' concrete domestic procedural actions, means or methods for rendering that assistance, outlining only those of them that have transnational implications for the requesting parties' proceedings, the requested parties' sovereignty or other essential interests or human rights (safe conduct and other safeguards for the persons concerned etc.), the proposed paragraph 4 should follow this pattern.

The designation of a SIT should itself convey their secret character and therefore preferably contain the adjective "covert".

These provisions would also help cover particular online covert SITs, which is especially important to countries not party to the Budapest Convention on Cybercrime.

It is a subject of debate *per se* whether it is expedient to ponder the inclusion of a cross-border telecommunications interception into the scope of the mother Convention or its Protocols, as it is done in Title III of the 2000 EU Convention (it regulates both cross-border and domestic intercepts), or to embark on a review of the Contracting Parties' reservations to the cross-border SITS in the Second Additional Protocol to the 1959 Convention with a view to their withdrawal, bearing in mind their significant implications for

the State sovereignty[1] and the fact that some of these reservations were entered quite recently.[2]

2. One may also refer to other pieces of the Contracting Parties' subsequent agreement/practice as means of treaty interpretation.

The main subsequent CoE soft law instrument for all types of SITs is currently the 2017 Recommendation. As was shown above, the 2005 and 2017 Recommendations' definition of SITs does not fully reflect their surreptitious character.

The 2005 (para. 15) and 2017 (para. 21) Recommendations and their explanatory documents listing the relevant instruments that regulate the use of SITs do not mention the 1959 Convention among them, thus by implication negating its applicability to SITs.

The 2017 Recommendation does not concern the application and interpretation of the 1959 Convention, may not be taken to represent a subsequent agreement or subsequent practice of its Parties and consequently to create any obligations for them, nor its scope is sufficient for the 1959 Convention, which is generally applicable to all criminal offences rather than solely to serious crimes including acts of terrorism. In sum, in its current version it cannot help operationalize the 1959 Convention with regard to the use of SITs.

One may argue that there is no common understanding or uniform and consistent practice of the Parties in the application of the 1959 Convention to SITs, but for domestic intercepts, which would establish the agreement of the Parties regarding its interpretation.[3] This practice is heterogeneous and depends on the States' legal systems.

---

[1] See, e.g.: *White paper on transnational organised crime* (Strasbourg: Council of Europe, 2014), p. 26.

[2] E.g., by the Russian Federation in 2019.

There are also reservations and declarations that actually transform cross-border (joint) SITs under the Second Additional Protocol to the 1959 Convention into domestic ones by excluding foreign officials from the range of persons authorized to carry out these activities on their territory (e.g., Belgium).

For the relevant feasibility issues, see also the preceding section.

[3] Vienna Convention on the Law of Treaties of 1969 (art. 31.3.b); Draft conclusions on subsequent agreements and subsequent practice in relation to the interpretation of treaties, with commentaries (Adopted by the International Law Commission at its seventieth session, in 2018) (hereinafter referred to as the "Draft conclusions").

To change this, I suggest amending the 1959 Convention as formulated above.

3. Another solution could be for the Committee of Ministers to issue a dedicated Recommendation to the Member States to this effect by analogy with the 1985 Recommendation, in order to read all domestic covert SITs into the scope of the 1959 Convention upon its conclusion in addition to the original intent of its Parties as reflected in the Explanatory Report to this Convention, thus further conflating judicial and police forms of mutual assistance in evidence gathering. Such government-level recommendations may be held to represent a subsequent agreement between the Parties regarding the authentic interpretation of the treaty or the application of its provisions, or subsequent practice in the application of the treaty which establishes the agreement of the Parties regarding its interpretation.[1]

In addition, subsequent agreements and subsequent practice may assist in determining whether or not the presumed intention of the Parties upon the conclusion of the treaty was to give a term used a meaning which is capable of evolving over time (evolutive or dynamic vs. contemporaneous or static treaty interpretation, in our case of the generic term "procuring evidence" under art. 3.1 of the 1959 Convention).[2]

However, despite the assumption of correctness of the dynamic interpretation, there still remains the problem of the lacking common understanding or uniform and consistent practice of the Parties in the application of the 1959 Convention to SITs that could confirm this dynamic interpretation, which, again, calls for a document of the Parties certifying their subsequent agreement as to the existence of such common understanding and interpretation, that is, of the applicability of the mother Convention to SITs.

4. There is also a question of whether an issuance of the relevant PC-OC practical guidelines or non-binding opinions may be held to constitute a subsequent agreement or subsequent practice of the

[1] That said, it is presumed that the parties to a treaty, by an agreement or a practice in the application of the treaty, intend to interpret the treaty, not to amend or to modify it. The possibility of amending or modifying a treaty by subsequent practice of the parties has not been generally recognized. See on this: Draft conclusions (draft conclusion 7).

[2] Draft conclusions (draft conclusion 8 and the commentary thereto).

Parties to the 1959 Convention and its Protocols and thus a means of authentic evolutive treaty interpretation that would incorporate [all types of] domestic SITs into their scopes.

The terms of reference of the PC-OC, which is a subordinate body,[1] or of its parent committee, the CDPC, which is a steering committee,[2] both having a status of an intergovernmental committee,[3] or Resolution CM/Res(2021)3 do not directly address this question. That may *per se* be a matter to consider for filling the gaps, which is of course outside the scope of this paper.

There are also documents on particular aspects of SITs elaborated by other CoE expert communities whose interpretative role is similar to that of the PC-OC guidelines or opinions.[4]

It follows from the International Law Commission' Draft conclusions that nothing precludes the PC-OC and other intergovern-

[1] Extract from CM(2021)131-addrev: Committee of Experts on the Operation of European Conventions on Co-operation in Criminal Matters (PC-OC), Terms of reference valid from 1 Jan. 2022 until 31 Dec. 2025.

[2] Extract from CM(2021)131-addrev: European Committee on Crime Problems (CDPC), Terms of Reference valid from 1 Jan. 2022 until 31 Dec. 2025.

[3] Resolution CM/Res(2021)3 on intergovernmental committees and subordinate bodies, their terms of reference and working methods (Adopted by the Committee of Ministers on 12 May 2021 at the 1404th meeting of the Ministers' Deputies).

As such, they do not fall within the notions of an expert treaty body or a conference of States Parties as they are defined in the Draft conclusions and their commentaries.

[4] Opinion No. 10 (2015) of the Consultative Council of European Prosecutors to the Committee of Ministers of the Council of Europe on the role of prosecutors in criminal investigations, Strasbourg, 20 Nov. 2015, CCPE(2015)3 (paras. 40–43) ("Special techniques of investigations, e.g. the use of informants, under-cover-agents, the recording of meetings, the surveillance and interception of telephone calls, emails, internet communication, the use of intrusive computer programmes, G.P.S. or scanners, etc."); Opinion No. 11 (2016) of the Consultative Council of European Prosecutors on the quality and efficiency of the work of prosecutors, including when fighting terrorism and serious and organised crime adopted by the CCPE at its 11th plenary meeting (Strasbourg, 17-18 Nov. 2016), CCPE(2016)3 (paras. 41, 65–69 and item 13 of the Recommendations); Opinion No. 14 (2019) of the Consultative Council of European Prosecutors (CCPE) of 22 Nov. 2019 CCPE(2019)2 "The role of prosecutors in fighting corruption and related economic and financial crime" (paras. 35–36, 59 and item 10 of the Recommendations); Opinion No. 8 (2006) of the Consultative Council of European Judges (CCJE) to the attention of the Committee of Ministers of the Council of Europe on "the role of judges in the protection of the rule of law and human rights in the context of terrorism" adopted by the CCJE at its 7th meeting (Strasbourg, 8-10 Nov. 2006), CCJE (2006) 3 (paras. 54–56).

mental expert bodies' practical guidelines, non-binding opinions and other pronouncements from being considered such subsequent agreements or subsequent practice of the Parties. That said, the CoE Committee of Ministers' recommendations, as evidenced by the example of its 1985 and 2017 Recommendations on SITs, are arguably more appropriate, in terms of the required level, to embody the said agreement and practice of the Parties, i.e., States.[1]

5. I am not supportive of the idea to supplement or otherwise update, or follow the example of, the 1985 Recommendation because the legal technique it employs ("a treaty in its own right") is not commonly accepted nowadays and it cannot represent a final solution. Explanatory report on the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union (comment on Title III) states that "[a]rticle 1(1) of the European Convention on Mutual Assistance in Criminal Matters has of course made it possible for the Member States to develop practices in this area, particularly on the basis of Council of Europe Recommendation No R(85)10. However, the Council believed it was time to adopt specific provisions, particularly because it seems that not all Member States recognise Article 1(1) of the European Convention on Mutual Assistance in Criminal Matters as the relevant basis for responding favourably to a request for an interception of telecommunications".

Viable alternatives could be amending the 2017 Recommendation to explicitly cover the applicability of the 1959 Convention to all types of domestic SITs, or elaborating and adopting a new dedicated recommendation to that effect which would replace the rather outdated 1985 Recommendation.

Despite those other available options, the preferable one is undoubtedly supplementing the mother Convention.

For instance, the preceding section underscored the need to subject requested SITs to the restrictive regime of art. 5 of the 1959 Convention that currently contains only two coercive measures (search and seizure of property), which cannot be done in any way other than by means of amending the 1959 Convention or else mak-

[1] See also: Art. 15 of the Statute of the Council of Europe of 1949; Vienna Convention on the Law of Treaties of 1969 (art. 31.3.a and b); Draft conclusions (in particular, draft conclusions 6.2, 8 and 10.1 and their commentaries).

ing a reservation to the suggested new provision of this Convention that allows reservations to any of its provisions.[1]

A dedicated questionnaire could be circulated among the member states to further glean their ideas and needs on the subject.[2]

[1] Art. 23 of the 1959 Convention; Explanatory Report to the European Convention on Mutual Assistance in Criminal Matters, p. 5, commentary on art. 2.

[2] **Questionnaire on covert special investigative techniques in legal assistance**

Objectives

Establishing the current practices, positions and needs of Member States in the area regarding the treaty application and interpretation and deciding on the possible development of new international standards, including by way of non-binding guidelines.

References

The 1959 European Convention on Mutual Assistance in Criminal Matters (Articles 1(1) and 3(1)): "The Contracting Parties undertake to afford each other, in accordance with the provisions of this Convention, the widest measure of mutual assistance in proceedings in respect of offences the punishment of which, at the time of the request for assistance, falls within the jurisdiction of the judicial authorities of the requesting Party. […] The requested Party shall execute in the manner provided for by its law any letters rogatory relating to a criminal matter and addressed to it by the judicial authorities of the requesting Party for the purpose of procuring evidence or transmitting articles to be produced in evidence, records or documents.";

The Explanatory Report to the 1959 Convention (Commentary on Article 3): "The expression "procuring evidence" refers, inter alia, to the hearing of witnesses, experts or accused persons, the transport involved as well as search and seizure.";

The 2001 Second Additional Protocol to the 1959 Convention (Articles 17–19): Cross-border observations; Controlled delivery; Covert investigations.

Questions

1. Do your State authorities apply the 1959 European Convention on Mutual Assistance in Criminal Matters to covert special investigative techniques performed within the requested State's territory solely by its domestic authorities in behalf of the requesting State, i.e., those that do not involve both States' cross-border or joint actions and are not provided for in the Second Additional Protocol to this Convention, as in the example:

The authorities of a foreign State request your State authorities to install a hardware keylogger on a suspect's computer in his apartment, a covert listening device there and a GPS tracker in his vehicle as well as to deploy a confidential informant, in order to carry out covert surveillance and gather evidence for the requesting State's criminal case solely in the territory of your State without any participation of the requesting State authorities.

2. In case your State authorities deem the 1959 European Convention on Mutual Assistance in Criminal Matters inapplicable to such investigative measures, do they need a treaty basis to conduct them?

3. To what concrete types of covert special investigative techniques do your State authorities apply the 1959 European Convention on Mutual Assistance in

§ 4. Electronic International Law Immunities in Criminal Proceedings. Obtaining Evidence by Videoconference at State Foreign Missions

Due to the development and implementation of the provisions of some bilateral (executive agreements pursuant to the US CLOUD Act), regional (Budapest Convention of the Council of Europe on Cybercrime (arts. 18, 32(b)) and the Second Additional Protocol to it) and supranational (EU Regulation on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings and the relevant Directive) instruments, to which the Russian Federation is not a party, there is currently an ongoing process of gradual partial dismantling of the architecture of inter-State interaction, which is expressed in granting to foreign counterparts the rights and powers for unilateral cross-border access to information systems and data that are not publicly available, on the territory of another contracting state, which is not accepted by the Russian Federation.

Such approaches cannot be freely applied in the extra sensitive sphere of interstate relations in general and to the activities of state foreign missions in particular.

One of the reasons for the unacceptability of foreign law enforcement directly approaching or accessing ICT service providers, devices and other equipment, networks and data is that private-sector providers can be holders of data of interest, which actually enjoys inviolability and other immunities and whose protection constitutes a duty of host and transit states imposed on them under public international law.

State sovereignty and international norms and principles derived from sovereignty (such as non-intervention or non-interference in the internal affairs of other States) apply to State conduct of ICT-

Criminal Matters and its Protocols, apart from those enumerated in Articles 17–19 of the Second Additional Protocol to this Convention?

4. Do your State authorities consider it expedient to include the transborder interception of communications into the scope of the 1959 European Convention on Mutual Assistance in Criminal Matters?

5. What other specific types of covert special investigative techniques aimed at collecting evidence in criminal matters pursuant to international legal assistance requests need to be additionally addressed in the international legal framework?

related activities and to their jurisdiction over ICT infrastructure within their territory.[1]

The legal definition of the information infrastructure of the Russian Federation is given by the strategic planning document, Decree of the President of the Russian Federation of 5 December 2016 No. 646 "On Approval of the Doctrine of Information Security of the Russian Federation" (para. 2), as "a combination of informatization objects, information systems, Internet websites and communication networks located in the territory of the Russian Federation, as well as in the territories under the jurisdiction of the Russian Federation or used under international treaties to which the Russian Federation is a party".

As the territory of the receiving State includes the land and buildings occupied by foreign States' representations, the said informatization objects, information systems and communication networks encompass those of foreign States' representations. Conversely, "the territories under the jurisdiction of the Russian Federation or used under international treaties to which the Russian Federation is a party" include the RF diplomatic missions, consular posts, other representations and military bases abroad and other relevant overseas installations and facilities, their information systems and communications networks.

For the purposes of art. 5 (state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation) of the Federal Law of 26 July 2017 No. 187-FZ "On the Security of the Critical Information Infrastructure of the Russian Federation", "information resources of the Russian Federation" are comprised of "information systems, information and telecommunication networks and automated control systems located on the territory of the Russian Federation, in diplomatic missions and (or) consular offices of the Russian Federation".[2]

---

[1] UN General Assembly Resolution 73/27 of 5 Dec. 2018 "Developments in the field of information and telecommunications in the context of international security" reaffirming the set of international rules, norms and principles of responsible behaviour of States, enshrined in the reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, concerning the applicability of international law to State use of ICTs.

[2] The Law contains the incomplete list of state foreign missions (only diplomatic missions and consular posts). See, e.g.: the Federal Law "On the Public

Prosecutor's Office of the Russian Federation" (art. 39[1]), which contains a complete list of state foreign missions of the Russian Federation ("diplomatic missions and consular posts of the Russian Federation, missions of the Russian Federation to international organizations, other official representations of the Russian Federation and representations of federal executive bodies located outside the territory of the Russian Federation").

By Decree of the President of the Russian Federation of 22 Dec. 2017 No. 620 "On improving the state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation", the RF Federal Security Service is entrusted with the functions of a federal executive body authorized to ensure the functioning of the state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation — i.e. information systems, information and telecommunication networks and automated control systems located on the territory of the Russian Federation, in diplomatic missions and consular posts of the Russian Federation.

In accordance with Decree of the President of the Russian Federation of 7 Aug. 2004 No. 1013 "Issues of the Federal Guard Service of the Russian Federation" (para. 12(40) of the Regulations approved by the Decree), the RF Federal Guard Service organizes and ensures operation, improvement and information security of special-purpose communication networks in the interests of representatives (representations) of state authorities located abroad, as well as diplomatic missions and consular posts of the Russian Federation. According to Decree of the President of the Russian Federation of 30 Apr. 2015 No. 215 "On approval of the Regulations on communication for the needs of state authorities" (para. 7(r) of the Regulations approved by the Decree) special communication includes communication with official representations of the Russian Federation, representative offices of state authorities and representative offices of organizations located abroad, to ensure the performance by them of their powers.

The subject of activity of the Federal State Unitary Enterprise "Center for Technical Systems of Information Transmission under the Ministry of Foreign Affairs of the Russian Federation" is the provision of services in the field of communication and information transmission, technical support for events using audiovisual equipment, including with the participation of foreign states' delegations, protection of means and systems of communication and information transmission operated in subdivisions of the RF Ministry of Foreign Affairs and in its foreign missions, maintenance and operation of office, computer and communication equipment of the RF Ministry of Foreign Affairs, including with the use of information constituting a state secret, as well as performance of works and provision of services to other legal entities and individuals.

See also: Order of the RF Federal Security Service of 6 May 2019 No. 196 "On approval of the Requirements for the means designed to detect, prevent and eliminate the consequences of computer attacks and respond to computer incidents" (These requirements are set for technical, software, software and hardware and other means installed and used on the entire territory of the Russian Federation, in diplomatic missions and (or) consular posts of the Russian Federation for detecting

This approach is developed in more detail in legal frameworks of some foreign states. In accordance with the Doctrine of Cyber Security of the Republic of Poland, adopted by the National Security Bureau of the Republic of Poland in 2015, and the Policy on Protection of the Cyberspace of the Republic of Poland, adopted by the Council of Ministers of the Republic of Poland in 2013, "the cyberspace of the Republic of Poland is the cyberspace within the territory of the Polish state and outside its territory in places where representations (representatives) of the Republic of Poland are functioning (diplomatic missions, military contingents, ships and aircraft outside the territory of the Republic of Poland, that are subject to Polish jurisdiction)".[1]

According to art. 13 of Federal Law of 27July 2006 No. 149-FZ "On information, information technologies and information protection", technical means of information systems used by state bodies must be located on the territory of the Russian Federation. Operators of state information systems should not allow, when operating information systems, to use databases and technical means situated outside the territory of the Russian Federation that are not part of such information systems; when operating information systems, they are obligated to use computing capacities of a hosting provider

(including searching for signs of computer attacks in telecommunication networks used for organizing the interaction of objects of critical information infrastructure of the Russian Federation), preventing and eliminating the consequences of computer attacks and (or) exchanging the information that is necessary for subjects of critical information infrastructure in detecting, preventing and (or) eliminating the consequences of computer attacks, as well as for cryptographic means of protection of such information (GosSOPKA means). The operation of GosSOPKA means may not lead to disruptions in the functioning of information systems, information and telecommunication networks and automated control systems located on the territory of the Russian Federation, in diplomatic missions and (or) consular posts of the Russian Federation (information resources) (paras. 1, 3.5)).

[1] *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej* [Doctrine of cyber security of the Republic of Poland], wydana przez Biuro Bezpieczeństwa Narodowego 22 stycznia 2015 r. (pkt 4); Uchwała Nr 111/2013 Rady Ministrów z dnia 25 czerwca 2013 r. w sprawie *Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej* Polskiej [Policy on protection of the cyberspace of the Republic of Poland], załącznik (pkt 1.1, 1.4). See also: Stanowisko Rzeczypospolitej Polskiej dotyczące zastosowania prawa międzynarodowego w cyberprzestrzeni [Position of the Republic of Poland concerning the application of international law in cyberspace], *RP MFA*, 29 Dec. 2022, URL: https://www.gov.pl/web/dyplomacja/stanowisko-rzeczypospolitej-polskiej-dotyczace-zastosowania-prawa-miedzynarodowego-w-cyberprzestrzeni, accessed May 1, 2023.

who deploys technical means used for providing computing capacity to place information in the information system permanently connected to the Internet, on the territory of the Russian Federation. In addition, operators of state information systems, when creating or operating information systems, as well as interacting in an electronic form, inter alia, with citizens (natural persons) and organizations, are not entitled to use information systems and/or programs for electronic computing machines functioning through the use of the Internet, that belong to foreign legal persons and/or foreign nationals, except for cases established by the RF Government. Violation of the said obligation entails administrative liability (art. 13.27.1 (Violation of the requirement to place technical means of information systems on the territory of the Russian Federation) of the RF Code of Administrative Offences).

The issues under consideration should be explored from the standpoints of implementation at state foreign missions of the jurisdiction of the receiving state, the country of transit of their telecommunications and the sending state.

Jurisdiction of the Receiving State and the State of Transit

The inviolability and other immunities of foreign representations and their personnel, as well as their protection by the host state guaranteed by international law, extend, in their traditional interpretation, to the physical space of a mission premises or dwelling of a person enjoying immunity and physical objects located there, in the first place, material fixed and mobile media, — archives, official correspondence and other hard and soft copy documents,[1] servers, user devices and other data storage media, computer and telecommunications equipment, hardware and software.

In the modern, increasingly hi-tech environment, these international legal measures in their evolutive interpretation are to be employed to equally protect against unauthorized access, search and interception of documents and communications of the mission and personnel deployed not only in a static, including digital, form, but also in a dynamic transit state in cyberspace, including cloud infrastructures, transmitted over any telecommunication networks (electromagnetic systems), including instant messaging services:

[1] *Draft Articles on Diplomatic Intercourse and Immunities with commentaries*, Yearbook of the International Law Commission, 1958, vol. II, ch. III, pp. 96–98.

terrestrial (landline, cable, for example, fiber-optic communications, radio relay, tropospheric scatter and other mobile (wireless) radio communications), space (satellite) radio communications.

This is of particular importance not only for the performance of daily tasks of a foreign mission, but also for the exercise by it of extraordinary criminal procedural powers provided for by law (in relation to the Russian Federation, under art. 40(3)(3) RF CPC), including by way of consular legal assistance in criminal matters,[1] in particular, for consular officers conducting interrogations or other hearings and other proceedings commissioned by investigative authorities and courts of the sending state, by videoconferencing or telephone conferencing.[2] Some consular functions in criminal cases can be performed using ICT, online, such as sending and receiving documents, explanation notes with the use of an electronic signature.[3] It is difficult to overestimate the importance of the unhindered exercise of these powers in the context of pandemics and other emergencies that entail closure of state borders, termination or suspension of transport communication between countries.

Such applicability of international legal obligations follows from the precepts of the Vienna Conventions on Diplomatic and Consular Relations of 1961 and 1963 and bilateral consular treaties, as well as other international agreements establishing such immunities for international (interstate, intergovernmental) organizations, missions of foreign states to such organizations, representative offices of state bodies and military bases abroad.[4] As for the last two categories of

---

[1] П.А. Литвишко, *Осуществление уголовно-процессуальной юрисдикции в зарубежных представительствах государств: дис. ... канд. юрид. наук* [Exercise of criminal procedural jurisdiction at state foreign missions: PhD in Law dissertation] (M., 2014).

[2] П.А. Литвишко, *Производство процессуальных действий по уголовным делам в загранучреждениях и в отношении лиц, пользующихся международно-правовым иммунитетом: Методическое пособие* [Conduct of proceedings in criminal cases at state foreign missions and in relation to persons enjoying international law immunity: methodological manual] / науч. ред. А.Г. Волеводз (М.: Следственный комитет Российской Федерации, 2013), pp. 181–182, 195–197 and 271.

[3] Т. Зонова, "Цифровая дипломатия в дипломатической и консульской службе" [Digital diplomacy in the diplomatic and consular service], *Право и управление. XXI век* 3(36) (2015), pp. 176–183.

[4] See, e.g.: Agreement between the Russian Federation and the Republic of Abkhazia on the joint Russian military base on the territory of the Republic of Abkhazia of 17 Feb. 2010 (art. 12), Agreement between the Government of the Russian

objects mentioned, as a general rule, there are no obligations of third states (transit countries), which will be considered below, imposed on them by international law, since the appropriate arrangements are always bilateral in nature and do not contain universal generally recognized customary international law norms that would be binding upon states that are not party to the treaty.

In accordance with arts. 22, 24, 27, 30 and 37–40 of the 1961 Vienna Convention on Diplomatic Relations, a receiving State has both negative and positive obligations to ensure inviolability and other immunities of the premises of the mission and any property thereon as well as to protect these premises; the archives and documents of the mission shall be inviolable at any time and wherever they may be (this is a key point, including in relation to the obligations of the countries of transit of electronic communications); the receiving State shall permit and protect free communication on the part of the mission for all official purposes; in communicating with the Government and the other missions and consulates of the sending State, wherever situated, the mission may employ all appropriate means, including messages in code or cipher; the official correspondence of the mission shall be inviolable (official correspondence means all correspondence relating to the mission and its functions); the diplomatic bag shall not be opened or detained; the private residences of relevant persons enjoying immunity shall enjoy the same inviolability and protection as the premises of the mission; their papers, correspondence and property shall likewise enjoy inviolability. Third/transit countries are obligated to assure most of the said safeguards as well, but only in relation to data being transmitted (in transit) through their territory, and not in respect of data stored (at rest) outside their territory.[1] In particular, third States shall accord to official correspondence and other official com-

Federation and the Government of the Republic of the Sudan on the establishment of a representative office of the Ministry of Defence of the Russian Federation at the Ministry of Defence of the Republic of the Sudan (done at Moscow on 8 May 2019 and at Khartoum on 9 May 2019) (art. 6).

[1] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* / Ed. by M.N. Schmitt, L. Vihul (Cambridge: Cambridge University Press, 2017), pp. 15, 29, 33–34, 55–56, 215–216, 219–225 and 294; J. Kurbalija, *E-Diplomacy and Diplomatic Law in the Internet Era*, in Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy (ed. K. Ziolkowski) (Tallinn: NATO CCD COE, 2013), pp. 393–424.

munications in transit, including messages in code or cipher, the same freedom and protection as is accorded by the receiving State.

It stands to reason that such obligations for the protection of information and telecommunication systems, networks and data of foreign missions can be imposed upon host and transit states only when they have law enforcement jurisdiction over an ICT service provider, which has the possession or control of the stored or transmitted data, and/or over the location of the data themselves (the servers). The grounds for establishing and exercising this jurisdiction may be different: based on the place of incorporation or other establishment or of the physical presence of the service provider; the place where the services are offered; at the location of the servers, including data dispersed over the territories of different states and migrating through temporary cloud storages,[1]and other software and hardware; the place where the service provider exercises their possession or control over the data in question.[2]

The inviolability of property, archives and documents of a foreign mission notably means that state actors of both the receiving and third countries[3] must not conduct a remote search (having the technical capability to do it via the Internet), any other both close access and remote access (the latter is also held to amount to unconsented-to physical entry into the mission premises) cyber operations against the mission's ICT infrastructure, for instance, in order to secure, seize and exfiltrate data stored on the mission server, including those not relating to official duties, nor use as evidence in a criminal case the results of any actions aimed at monitoring and recording telephone and other conversations, obtaining information about connections between users and user devices, inspecting and

[1] 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 data location; situations when data that form a single whole unit (information resource) get actually scattered in a fragmented and/or dynamic state over different jurisdictions, or have their numerous mirror copies in those jurisdictions.

[2] П. Литвишко, "Юрисдикционные и международно-правовые аспекты обеспечительных и конфискационных мер в отношении виртуальных активов" [Jurisdictional and international law aspects of provisional and confiscation measures in relation to virtual assets], *Законность* 3(1037) (2021), pp. 8–14.

[3] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* / Ed. by M.N. Schmitt, L. Vihul (Cambridge: Cambridge University Press, 2017), pp. 213–214 and 221–222.

seizing electronic messages and other communications transmitted over telecommunication networks, obtaining computer information or otherwise capturing information from technical communication channels situated in the premises enjoying inviolability.[1]

In 1990, Germany's Federal Court of Justice in a case against two attachés of the Consulate General of Turkey in Hamburg, who were members of Turkish intelligence community, accused of intelligence activities, held that covert wiretapping and recording of telephone communications (conducted not under the criminal procedure rules but within extrajudicial administrative proceedings for preventive purposes) from a communications link installed in the official premises of the consulate general, violate the international law principles of inviolability of consular premises and consular immunity, and their results must not be used as evidence, at least where the underlying allegation concerns criminal acts that may be associated with the performance of consular functions. The same year, in the same case against an accomplice of the said attachés, a social worker of a penitentiary facility in Hamburg, a Turkish citizen, the Federal Court of Justice had found that the results of the wiretapping and recording of communications obtained with the said violations, as opposed to the proceedings against the attachés, can be used as evidence in the case against the accomplice since this person is not covered by the mentioned principles of international law.[2]

---

[1] See, e.g.: *Annex to the Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions: Investigation into the unlawful death of Mr. Jamal Khashoggi* (UN Doc. A/HRC/41/CRP.1 of 19 June 2019), footnote 191, paras 395–398; M. Milanovic, "The Murder of Jamal Khashoggi: Immunities, Inviolability and the Human Right to Life", *Human Rights Law Review*, vol. 20, issue 1 (2020), pp. 1–49.

See on views of diplomatic cables losing their inviolability as a result of leakages of their contents: Judgment R (on the application of Bancoult No 3) (Appellant) v Secretary of State for Foreign and Commonwealth Affairs (Respondent) given on 8 February 2018 (Hilary Term [2018] UKSC 3 On appeal from: [2014] EWCA Civ 708); *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* / Ed. by M.N. Schmitt, L. Vihul (Cambridge: Cambridge University Press, 2017), pp. 223–224.

[2] J. Polakiewicz, "Die völkerrechtliche Zulässigkeit der Überwachung des Telefonverkehrs von Konsulaten ausländischer Staaten. Zu den Beschlüssen des Bundesgerichtshofs vom 4. und 30. April 1990 — 3 StB 5 und 8/90" [Admissibility under international law of surveilling telephone communications of foreign states' consulates. Re decisions of the Federal Court of Justice of 4 and 30 April 1990 Nos. 3 StB 5 and 8/90], *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht*, Bd. 50 (1990), S. 761–794; H. Kreicker, "Konsularische Immunität und Spionage. Anmerkungen zu BGH, Beschl. v. 27.6.2013 — StB 7/13" [Consular immunity and espionage. Remarks to the decision of the Federal Court of Justice of 27 June 2013

In the context of the application of art. 3(2) RF CPC, one reasonably argues that it "sets out a requirement according to which all procedural actions provided for by the RF CPC in respect of persons enjoying immunity from such actions in accordance with the generally recognized principles and norms of international law and international treaties of the Russian Federation, shall be carried out with the consent of the foreign state, in the service of which the person enjoying immunity is or was, or of the international organization, of which the person enjoying immunity is or was a personnel member. In this regard, it is recommended that in each case where there is a need (the presence of factual grounds) for inspection and, moreover, seizure of messages transmitted over telecommunication networks and addressed to such a person, even before filing a motion for a court decision, the foreign state should be asked to grant the appropriate consent".[1]

Due to the countries' concern about the instances of (electronic) surveillance and interception of telecommunications, including those of an extraterritorial character, undertaken with regard to foreign missions and breaching the inviolability of their archives, documents, official correspondence and communications made

No. StB 7/13], *Zeitschrift für Internationale Strafrechtsdogmatik* 3 (2014), S. 129–133; *Postępowanie w sprawach karnych ze stosunków międzynarodowych. Komentarz do Działu XIII KPK* [Proceedings in criminal matters in international relations. Commentary on Chapter XIII of the CPC] / S. Buczma, M. Hara, R. Kierzynka, P. Kołodziejski, A. Milewski, T. Ostropolski (Warszawa: Wydaw. C.H. Beck, 2016), s. 8.

[1] А.П. Рыжаков, *Комментарий к статье 2 Федерального закона от 6 июля 2016 года № 375-ФЗ* [Commentary to article 2 of the Federal Law of 6 July 2016 No. 375-FZ], СПС КонсультантПлюс (2016).

See in more detail on the issues of obtaining data on all subscriber numbers linked to a base station (information on subscribers and subscriber devices located in the coverage area of the base station of the telecommunication operator) for a specific period of time, among which there may be numbers of persons enjoying immunity: С.В. Петраков, А.Ю. Ушаков, *Организация взаимодействия следственных органов с представителями компаний сотовой связи по вопросам своевременного предоставления информации о телефонных соединениях, переговорах и текстовых сообщениях абонентов по уголовным делам о тяжких и особо тяжких преступлениях против личности, общественной безопасности и коррупционных преступлениях: практическое пособие* [Organization of interaction of investigative authorities with representatives of cellular communication companies on issues of timely provision of information on telephone connections, conversations and text messages of subscribers in criminal cases of grave and especially grave crimes against the person, public security and corruption crimes: practical guide] (СПб: Санкт-Петербургская академия Следственного комитета, 2022), pp. 14–17 and 31–33.

public by E. Snowden,[1] in 2014 the UN General Assembly Sixth Committee supplemented for the first time the UN General Assembly standard Resolution (69/121 of 10 December 2014) "Consideration of effective measures to enhance the protection, security and safety of diplomatic and consular missions and representatives" with the indication that the said archives, documents and official correspondence may take a variety of forms (mainly in hard copy or on digital platforms) and that missions may use a variety of means of communication.[2]

At present, there is no universal international legal position on whether the 1973 Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, is applicable not only to kinetic actions, but also to cyber attacks on information systems of a foreign mission, if their nature and consequences fall within the provisions of art. 2 of the Convention. Here one can draw a parallel with the applicability of the norms of international humanitarian law to attacks on objects protected by it in cyberspace, recognized by some, but by no means all countries and international organizations.[3]

On the contrary, it is arguably obvious that the above-mentioned duties to secure immunities and protection cannot apply to the same extent with regard to the forms, means and methods of public digital diplomacy,[4]such as official websites, accounts, posted

[1] A. Deeks, "An International Legal Framework for Surveillance", *Virginia Journal of International Law*, vol. 55:2 (2015), pp. 312–313; C.G. Buys, "Reflections on the 50th Anniversary of the Vienna Convention on Consular Relations", *Southern Illinois University Law Journal* 38 (2013), pp. 57–72; S. Duquet and J. Wouters, *Diplomacy, Secrecy and the Law*, in Working Paper No. 151 — March 2015. The Leuven Centre for Global Governance Studies, the Institute for International Law (KU Leuven), 25 p.

[2] Summary record of the 15th meeting held on 21 Oct. 2014, UN General Assembly Sixth Committee, sixty-ninth session (UN Doc. A/C.6/69/SR.15 of 2 Dec. 2014), pp. 8–14, paras 48–84; Summary record of the 29th meeting held on 14 Nov. 2014, UN General Assembly Sixth Committee, sixty-ninth session (UN Doc. A/C.6/69/SR.29 of 15 Jan. 2015), pp. 6–7, paras 37–42.

[3] *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy* (ed. K. Ziolkowski) (Tallinn: NATO CCD COE, 2013), pp. 162–165, 186 and 189–238.

[4] The concept of digital diplomacy should be distinguished from the "cyber diplomacy toolbox", which in the European Union refers to measures of diplomatic response to malicious activities in cyberspace. See: Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") — Adoption of 7 June 2017, 9916/17.

content and transmitted messages of foreign missions in social media, in the blogosphere, including those that are of an official character.[1] The same applies to virtual embassies and other foreign missions,[2]including those deployed in metaverse.[3] Despite exercising certain functions, for example, providing some electronic consular services, conferred on them by the establishing state, they cannot *per se* have an international legal status of a regular foreign mission with the physical presence, first of all due to the absence of a receiving state as such, which gives its consent to another country's establishing a representation on its soil (geographic territory) in the manner prescribed by the Vienna conventions and other international legal instruments.

These resources have an unlimited target audience and are devoid of any elements of confidentiality, for the protection of which the immunities and privileges of archives, documents and correspondence of foreign missions are actually intended; and these resources themselves do not constitute archives, documents or correspondence, they cannot be considered as a form of a mission's communications for official purposes. The preparatory materials for the Vienna Convention on Diplomatic Relations indicate that official purposes encompass communications with the Government of the sending State, with the officials and authorities of that Government or the nationals of the sending State, with missions and consulates of other Governments or with international organizations,[4]which implies a limited circle of communications addressees.

---

[1] See on views of diplomatic cables losing their inviolability as a result of leakages of their contents: Judgment R (on the application of Bancoult No 3) (Appellant) v Secretary of State for Foreign and Commonwealth Affairs (Respondent) given on 8 February 2018 (Hilary Term [2018] UKSC 3 On appeal from: [2014] EWCA Civ 708); *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* / Ed. by M.N. Schmitt, L. Vihul (Cambridge: Cambridge University Press, 2017), pp. 223–224.

[2] See, e.g., *U.S. Virtual Embassy in Iran*, URL: https://ir.usembassy.gov/, accessed Apr. 4, 2021.

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / Ed. by M.N. Schmitt, L. Vihul (Cambridge: Cambridge University Press, 2017), pp. 216–217, 220, 224 and 227.

[3] A. Gupta, "Metaverse: Challenges and Opportunities for Diplomacy and International Relations", *Journal of International Law and Politics*, vol. 55, No. 1 (2023), pp. 1–15.

[4] Draft Articles on Diplomatic Intercourse and Immunities with commentaries, p. 97.

The principles prohibiting the use of a foreign mission premises in any manner (including criminal ones in the first place) incompatible with its functions, imposing the duties not to interfere in the internal affairs of the host country and to respect its laws and regulations laid down in said treaties, should be equally applicable to acts of the foreign mission itself in cyberspace, and their violations can lead to the host country employing the permissible exceptions to the inviolability and other immunities,[1] for instance, in the event of disseminating malware, perpetrating cyber attacks on critical information infrastructure of the host nation from servers installed in the mission premises, electronic surveillance, interception of telecommunications, cyber espionage or other intelligence activities conducted from the mission compound and inflicting serious damage to the security or other essential interests of the host nation.

However, modern sources point to international law prohibiting such reprisals (countermeasures) that breach the inviolability of diplomatic or consular agents, premises, archives, documents or official correspondence, including those undertaken in response to an internationally wrongful act associated with the abuse of diplomatic functions and privileges; at the same time, they underscore the lack of absolute inviolability of mission premises, and permissibility to exert certain external influence on the mission's ICT infrastructure as part of the host nation's right to self-defence.[2]

In the context of e-government and the virtualization of international law immunities, one cannot fail to mention the recent emergence of the concept of a data embassy, which is not related to a virtual embassy as a means of digital diplomacy and is aimed solely at ensuring the protection and immunity of government electronic data, information systems and telecommunication net-

[1] Diplomatic intercourse and immunities, summary record of the 394th meeting (UN Doc. A/CN.4/SR.394); 395th meeting (UN Doc. A/CN.4/SR.395), Yearbook of the International Law Commission, vol. I (1957), pp. 54–60; Diplomatic intercourse and immunities, summary record of the 456th meeting (UN Doc. A/CN.4/SR.456), Yearbook of the International Law Commission, vol. I (1958), pp. 129–130, paras 1–21.

[2] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* / Ed. by M.N. Schmitt, L. Vihul (Cambridge: Cambridge University Press, 2017), pp. 125 and 211–214.

works, especially those constituting objects of critical information infrastructure.[1]

A data embassy represents the following solutions: a data center for hosting servers and network equipment and/or backups of data of critical government information systems and mirrors of critical service applications situated in the premises of the operating state's embassy abroad (this data protection solution is regarded as useful but having numerous organizational, legal and technical challenges)[2], or located at a dedicated high-level data protection facility in a friendly foreign country (Physical Data Embassy); backups of non-sensitive government data in private companies' public cloud (Virtual Data Embassy).[3]

The first data embassy was established pursuant to the Agreement between the Grand Duchy of Luxembourg and the Republic of Estonia on the hosting of data and information systems of 20 June 2017, which literally reproduces the 1961 Vienna Convention's provisions on inviolability and other immunities of the premises and archives of diplomatic missions and their personnel's residences, their protection, freedom and protection of official communications, the prohibition to use the premises in any manner incompatible with the purpose laid down in the Agreement or by other rules of international law; some of its articles treat the data centre's premises, data and information systems and official communications as the premises, archives and official communications of diplomatic missions.

Jurisdiction of the Sending State

On the other hand, it is lawful for the sending state to exercise its prescriptive and, under certain conditions, enforcement criminal

---

[1] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* / Ed. by M.N. Schmitt, L. Vihul (Cambridge: Cambridge University Press, 2017), pp. 216–217.

[2] N. Robinson, L. Kask and R. Krimmer, *"The Estonian Data Embassy and the Applicability of the Vienna Convention: An Exploratory Analysis"*, in Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance (ICEGOV'19) (Melbourne, Australia, April 3–5, 2019), pp. 391–396.

[3] *Implementation of the Virtual Data Embassy Solution. Summary Report of the Research Project on Public Cloud Usage for Government, Conducted by Estonian Ministry of Economic Affairs and Communications and Microsoft Corporation*, URL: https://www.mkm.ee/sites/default/files/implementation_of_the_virtual_data_embassy_solution_summary_report.pdf, accessed Apr. 4, 2021.

jurisdiction in cybercrime cases on the territories of its foreign missions overseas.[1] In this regard, it is useful to consider the existing foreign case law.

In a US court's assessment Ph. Agee, a former CIA employee, charged with seditious conspiracy, while in 1979 from the territory of Germany counselling over the telephone the Iranian terrorists who seized the US Embassy in Tehran, to demand from the United States all CIA records on CIA intelligence operations in Iran for the past 30 years, in return for the release of hostages, acted so on that Embassy's territory, which is subject to the concurrent jurisdiction of the United States criminal laws.[2]

In 2016, the US District Court for the Northern District of Georgia (at the defendant's place of residence) sentenced M.C. Ford, a former employee of the US Embassy in London, to 57 months in prison for several counts of cyberstalking, computer hacking to extort (sextortion) and wire fraud conducted from his computer at the said US Embassy.[3]

In 2021, US District Court for the District of Oregon, Eugene Division sentenced G.L. Thompson, Jr., a former US Department of State employee, an Information Programs Officer at the US Embassy in Seoul, Republic of Korea, to 18 months in prison and three years of supervised release, and his spouse G. Zhang to three years of supervised release, the first eight months of which consist of home confinement. They were also ordered to forfeit a combined total of $229,302. Between 2017 and 2019, they sold hundreds of thousands of dollars in handbags and other goods bearing counterfeit Vera Bradley trademarks on a variety of e-commerce platforms. Thompson Jr. used his State Department computer at the embassy to create numerous e-commerce accounts, Zhang took primary responsibility for operating the accounts. Thompson's said work station was situated at the Embassy inside an Information Program Center which is considered a Sensitive Compartmented Information Facility, a secure facility designed to protect classified information.

---

[1] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* / Ed. by M.N. Schmitt, L. Vihul (Cambridge: Cambridge University Press, 2017), p. 33.

[2] *Agee v. Muskie*, 629 F.2d 80 (U.S. Court of Appeals, D.C. Cir. 1980).

[3] *United States v. Ford* (U.S. Distr. Court for the Northern Distr. of Georgia, Atlanta Div., 2016, Case 1:15-cr-00319-ELR-RGV), Public Access to Court Electronic Records (PACER), URL: http://www.pacer.gov/.

That Department of State computer used Internet Protocol ("IP") addresses in the United States.[1]

Chiefs of mission, consular and other authorized officials of foreign missions may not, in performing both urgent investigative actions in a case on a crime committed in the mission territory and actions of consular legal assistance in other criminal cases, conduct inspection and seizure of electronic messages or other messages transmitted through telecommunication networks; monitoring and recording of telephone or other conversations; obtaining communications data on connections between subscribers and subscriber devices, insofar as they concern the capturing of information from technical communication channels, obtaining computer or other information or documents from local ICT service providers in the host country.

The arrival, clearance, admission and activities in a foreign mission of computer emergency response teams both of the sending and receiving states for the purpose of participating in criminal investigations into cybercrime should be subject to the same procedure as foreseen for the activities of criminal investigators in the mission compounds.[2] Representatives of such teams may be engaged in criminal investigations in the capacity of forensic experts.

Presently, one witnesses the emergence of special customary rules of diplomatic and consular law regarding "e-immunities" and "e-protection" of foreign missions; the scholarly discourse uses the concept of a "diplomatic (consular) cyber bag".[3] Applicability of international law principles of sovereign equality of states, non-interference in the internal affairs and others to activities of states and other actors in cyberspace is underscored in documents of the UN, CoE, EU and other international organizations.

One of the problems faced by the need to ensure e-immunities and e-protection of foreign missions by host countries as well as

---

[1] *United States v. Thompson, Jr., and Zhang* (U.S. Distr. Court for the Distr. of Oregon, Eugene Div., 2021, Case 6:19-cr-00561-MC), PACER.

[2] П.А. Литвишко, *Производство процессуальных действий по уголовным делам в загранучреждениях и в отношении лиц, пользующихся международно-правовым иммунитетом: Методическое пособие* [Conduct of proceedings in criminal cases at state foreign missions and in relation to persons enjoying international law immunity: methodological manual] / науч. ред. А.Г. Волеводз (М.: Следственный комитет Российской Федерации, 2013), 312 p.

[3] Won-Mog Choi, "Diplomatic and Consular Law in the Internet Age", *Singapore Year Book of International Law* 10 (2006), pp. 117–132.

by countries of the transit of transmitted computer and telecommunications data which is to be solved in the near future, is the development of universal instruments and mechanisms ensuring that ICT service providers in those countries implement the bans on the access to systems and data of a foreign mission not authorized by the sending state. A decisive requirement for foreign missions themselves securing the inviolability of their e-documents and telecommunications would be that the missions provide them with visible external marks identifying their affiliation and pointing to their character, for instance, by using electronic signatures, special registration procedure, dedicated servers, which would help assure that a potential wrongdoer's act had been committed knowingly, with the possible simultaneous application of transcoding, encryption or steganography to such documents or communications.[1]

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 contain special provisions aimed at the observance of immunities and privileges in applying these instruments, including the procedure for their waiver.

The updated version of the Model Law on Mutual Assistance in Criminal Matters (UNODC) also contains articles reflecting certain aspects of the legal regime of electronic evidence that is subject to legal privilege or immunity, including that under international law.

[1] See also: П.А. Литвишко, "Электронные международно-правовые иммунитеты: вопросы теории и практики" [Electronic international law immunities: issues of theory and practice], *Вестник Университета прокуратуры Российской Федерации* 3(83) (2021), pp. 126–135; М.А. Перепелицын, "Дипломатическая неприкосновенность в условиях цифровой дипломатии" [Diplomatic inviolability in the conditions of digital diplomacy], Молодой учёный. Международный научный журнал, No. 20(310), p. IV (2020), pp. 307–309; *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* / Ed. by M.N. Schmitt, L. Vihul (Cambridge: Cambridge University Press, 2017), pp. 225, 515–517 and 536.

Obtaining Evidence via Videoconferencing at State Foreign Missions

The product of investigative and judicial proceedings performed through the use of video conference is regarded as a particular type of electronic evidence.

Based on a questionnaire developed by the Prosecutor General's Office of the Russian Federation jointly with other federal law enforcement and judicial authorities concerned, the Consular Department of the Ministry of Foreign Affairs of the Russian Federation has collected country-specific information from foreign host states on the possibility and procedures for Russian consular posts and diplomatic missions rendering consular legal assistance in serving subpoenas and other procedural documents and in questioning the participants in criminal proceedings, including by video conference (which is admissible on the basis of art. 1(3) RF CPC, para. 8 of the Regulations on the Consular Post of the Russian Federation approved by Decree of the President of the Russian Federation of 5 November 1998 No. 1330, relevant self-executing norms of international treaties of the Russian Federation on legal assistance and legal relations in criminal matters, consular conventions, legislation on their ratification and other legal acts to them).[1]

In 2023, the Prosecutor General's Office of the Russian Federation, in coordination with all the federal law enforcement and judicial authorities concerned, prepared a draft federal law with a view to implementing this kind of international legal assistance into the RF CPC, which is currently being considered by the Russian parliament. It provides for consular officers of Russian consular posts and diplomatic missions executing, in accordance with an international treaty of the Russian Federation, in exceptional cases and upon approval by the RF Ministry of Foreign Affairs, Russian investigatory and judicial authorities' requests for serving summonses and other

[1] *Компетентные органы России и иностранных государств в сфере уголовного судопроизводства: статус, полномочия и механизмы взаимодействия: монография* [Competent authorities of Russia and foreign states in the field of criminal proceedings: status, powers and mechanisms of interaction: monograph] / под ред. докт. юрид. наук, проф. С.П. Щербы (М.: Юрлитинформ, 2019), pp. 173–195; *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.

procedural documents and conducting hearings, including through the use of videoconferencing systems.[1]

The Russian Federation initiated consideration of the issues of consular legal assistance in criminal matters, including consular hearings by video conference, at the Council of Europe bodies.[2]

The 2021 Russian draft United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes in art. 54 ("Powers of Diplomatic Missions and Consular Posts") establishes the sending States' rights to serve documents on their own citizens, under instructions from their competent authorities to interrogate their own citizens through their diplomatic missions or consular posts, including through the use of video or telephone conferencing systems, while no means of coercion or the threat thereof may be used.[3]

The RF CPC provides for participation in certain investigative and judicial actions both directly, in person (physical presence) and through the use of videoconferencing systems.

By using videoconferencing systems, interrogation and confrontation can be conducted at the pre-trial stage (regardless of the procedural status of the interrogated persons), as well as presentation for identification (art. 189^1 RF CPC), and at the trial stage (also when examining evidence by a court of appeal) — interrogation and (any) other judicial actions (participation in a court session of

[1] 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).

[2] *Consular Legal Assistance in Criminal Matters: State of Play and Added Value of Developing the Council of Europe's Framework: Discussion Paper by Mr Pyotr Litvishko (Russian Federation), PC-OC Mod Substitute Member*, Strasbourg, 19 Aug. 2021 [PC-OC/PC-OC Mod/Docs PC-OC Mod 2021/ PC-OC Mod (2021)03E]; *Introductory Note to Discussion Paper* PC-OC (2021)09EN.

[3] United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (Draft as of 29 June 2021), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_E.pdf, accessed Aug. 3, 2021.

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. URL: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home, accessed Apr. 14, 2023.

the defendant and other persons summoned to the court session) (arts. 240, 241[1], 277, 278[1] and 389[13] RF CPC).

These remote actions can also be carried out in a cross-border format in conjunction with the referential provisions of arts. 453, 455 and 457 RF CPC on international legal assistance.[1]

An obstacle to the extrapolation of the "domestic" art. 189[1] RF CPC to the execution of Russian and foreign requests for international legal assistance can be seen in the requirement of this article on the mandatory use of "videoconferencing systems of state authorities conducting preliminary investigations", which obviously refers to the terminal user equipment of both parties — the requesting and requested, and in a transnational context, the equipment used by a foreign party may be regarded as not meeting this requirement.

In addition, the provision of art. 189[1](8) RF CPC, which does not allow conducting investigative actions in the videoconference mode if it is possible to divulge thereby state or other secrets protected by federal law, seems problematic as well. One may argue that public disclosure of information constituting a secret of investigation (art. 161 RF CPC), secrecy of communication, banking, commercial or other secrets, except for state secrets, carried out by an authorized person in accordance with the established procedure in the course of a remote investigative action (for example, by presenting the relevant documents to interrogated persons by the investigator), should not be interpreted as the aforementioned prohibited divulgence.

The provisions of art. 241[1](1) RF CPC on the defendant's remote participation in a court session may conflict with the provisions of art. 247(5) RF CPC on trial in absentia (in the absence of the defendant), since the defendant, who is outside the territory of the Russian Federation and (or) evades appearing in court (which obviously means physical arrival at the court considering the criminal case for participation in person), at the same time, may apply to this court

[1] Based on art. 9 (Hearing by video conference) of the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, or the provisions of other treaties or the principle of reciprocity. At the same time, an international treaty may not specifically mention interrogation via videoconference as a separate type of legal assistance provided under the treaty, but, instead, might contain a non-exhaustive list of requested actions and the standard rule on the provision of legal assistance in accordance with the legislation of the requested party, or under certain conditions, in accordance with the legislation of the requesting party.

for his or her participation in the court session by using videoconferencing systems, including from abroad by way of international or consular legal assistance. On the other hand, the law obliges the court to make a decision (obviously, positive or negative) on such remote participation of the defendant at the request of the party or on its own initiative if there are circumstances precluding the possibility of his or her participation in person (for example, again, being outside the Russian Federation and unwilling to appear and participate in person while being ready to participate remotely). In this regard, the second alternative condition for proceedings in absentia in art. 247(5) RF CPC, instead of "evades appearing in court", should be formulated as "evades participating in a court hearing" (in either of two forms — in-person or remotely by using videoconferencing systems). In practice, this conflict of norms, of course, can be alleviated due to the discretionary nature of the provisions of both art. 241^1 and art. 247(5) RF CPC, and the exceptional nature of the latter. Defendants, including those who are abroad, even if they are put in the international (interstate) wanted list and, at the same time, cannot be transferred to Russia, when their whereabouts have been established, should be advised of their right, under art. 241^1(1) RF CPC, to apply for participation in court sessions by using videoconferencing systems, as well as under art. 247(4) RF CPC, for consideration of the case in their absence.

It follows from those provisions that the subjects directly conducting an investigative/judicial action by using videoconferencing systems, including the making of its record/minutes, are, respectively, the investigator or inquirer in charge of the preliminary investigation, or the court considering the criminal case; while the investigator, inquirer, body of inquiry or court at the location of the person participating in the investigative action or court hearing through the use of videoconferencing systems, accordingly, solely execute commissions issued to them for organizing participation of the person in the investigative/judicial action, identifying him or her, and taking recognizances specified in the law.

In this regard, the mentioned provisions are not applicable, both at the pre-trial and trial stages, to hearings by a consul, even *mutatis mutandis*.

In 2021, the Embassy of the Republic of the Philippines to the Russian Federation sent notes to the RF authorities informing that the Philippine Supreme Court had adopted rules that allowed testi-

mony via video conferencing from witnesses outside the Philippines in connection with criminal and civil proceedings in a Philippine court. It was specified that one meant hearings of Philippine witnesses residing in the Russian Federation. The notes also indicated that "[t]he testimony via video conferencing would take place at the Philippine Embassy with the passive participation of a Philippine consul". The Embassy requested an opinion from the RF authorities as to whether performing the said activity lay within the scope of consular functions as set out in art. 5 (j) and (m) of the 1963 Vienna Convention on Consular Relations, and whether it was not prohibited by the laws and regulations of the Russian Federation, or whether the Russian Federation took no objection to that activity.

Pursuant to the Supreme Court of the Republic of the Philippines's Guidelines on the Conduct of Videoconferencing A.M. No. 20-12-01-SC of December 9, 2020[1] that are applicable during the pandemic and thereafter, the presiding judge or justice shall, at all times, supervise and control the proceedings; perjury and contempt laws shall apply. (Any unauthorized sharing of the invitation or link to the videoconferencing, or unauthorized recording of any portion of the videoconferencing hearing may be considered a contempt of court.)

Court hearings and proceedings, including the taking of testimony, through videoconferencing technology may be conducted in civil, criminal and other cases, inter alia, when a litigant or witness, including an expert witness, is an Overseas Filipino Worker or Filipino residing abroad or temporarily outside the Philippines, or is a non-resident foreign national who, while in the Philippines, was involved in any action pending before any court, and would like to appear and/or testify remotely from overseas. These persons who would like to participate or testify through videoconferencing may do so upon proper motion with the court where the case is pending. Such videoconferencing may be conducted only from an embassy or consulate of the Philippines provided that it has allowed the use of its facilities for videoconferencing. When the assistance of an interpreter is needed for the live-link, the movant shall secure the services of the official interpreter of the Philippine embassy or consulate. Should the court grant the motion for videoconferencing, it

[1] Published on the official website of the Supreme Court of the Republic of the Philippines. URL: https://sc.judiciary.gov.ph/16099/, accessed Sept. 4, 2021.

shall also furnish the concerned Philippine embassy or consulate, by the fastest means available, a copy of the order granting the motion. The movant shall defray all the expenses and costs that may be necessary for the conduct of videoconferencing from an embassy or consulate of the Philippines.

The Guidelines thus make clear that such interrogations and other proceedings through the use of video conference are carried out by the Philippine court (parties at a trial) rather than the consular officer. This does not constitute the exercising of consular functions, is not consistent with the nature of consular legal assistance and therefore does not conform to art. 5 of the Vienna Convention on Consular Relations in the light of its object and purpose (art. 31 of the 1969 Vienna Convention on the Law of Treaties). It is equally evident that such proceedings do not constitute international mutual legal assistance in its ordinary sense either as they are not requested from a foreign State and are not executed by its competent authorities.

Diplomatic missions and consular posts' premises constitute part of the territory of the receiving State in terms of public international law. As opposed to foreign diplomatic agents and consular officers whose presence and lawful official activities in the territory of the host State are *a priori* approved by it by reason of an *agrément*, exequatur or notification, the exercise of enforcement jurisdiction in its territory, that is with respect to persons and objects located there, by the sending State's law enforcement and judicial authorities is contrary to the international legal principles stemming from the sovereign equality of States, such as the duty to respect the laws and regulations of the receiving State, prohibition to use the mission's premises in any manner incompatible with its functions, and duty of non-intervention in the domestic affairs of the host country.

As exceptions to this general rule, the host nation's consent to foreign authorities' performing those activities on its soil on their own may be set out in a treaty or other document of an international character containing obligations recognized by the relevant State, or provided by its laws and/or regulations. These grounds are absent in the case at hand.

Pursuant to arts. 1, 5, 9, 11 and 21 of the Treaty between the Russian Federation and the Republic of the Philippines on Mutual Legal Assistance in Criminal Matters of 13 November 2017, nothing in this Treaty entitles a Contracting State to undertake in the territory of the

other Contracting State the exercise of jurisdiction and performance of functions that are exclusively for the authorities of that Contracting State by its domestic laws *[sic]*. The request for legal assistance shall contain, *inter alia*, in case of an indication that the presence of representatives of the central or competent authorities of the Requesting State is desired, their full names and official designations as well as reasons for their presence. If the Requesting State seeks the presence of the persons identified by its Central or competent authority during the execution of the request, the Requested State shall promptly inform the Requesting State about its decision; if granted, the Requesting State will be informed about the time and the place of the execution of the request. If the Requested State has permitted the presence of representatives of the Requesting State during the execution of the request, then, subject to the domestic laws of that State, such representatives shall be permitted to formulate such questions that may be asked of the person giving testimony or producing evidence [only] through the Central or competent authority of the Requested State. The Requested State shall meet the regular costs of executing the requests for legal assistance, except that the Requesting State shall bear, *inter alia*, the expenses associated with the taking of evidence from the Requested State to the Requesting State via video, satellite or other technological means.

As a general rule, the grounds and procedures for hearings by video- or telephone conference are fraught with certain restrictions since they affect the territorial sovereignty of the requested State. For example, pursuant to arts. 9 and 10 of the 2001 Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, if the judicial authority of the requested Party is of the view that during the hearing the fundamental principles of the law of the requested Party are being infringed, it shall immediately take the necessary measures to ensure that the hearing continues in accordance with the said principles.

State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory.[1]

[1] See, e.g., the UN General Assembly resolution 73/27 of 5 Dec. 2018 "Developments in the field of information and telecommunications in the context of international security" which again welcomes the set of international rules, norms

In Russia's domestic legal framework, a definition of the "information infrastructure of the Russian Federation" is given by Decree of the President of the Russian Federation No. 646 of 5 December 2016 "On Approval of the Doctrine of Information Security of the Russian Federation" (para. 2) pursuant to which it is "a combination of informatization objects, information systems, Internet websites and communication networks located in the territory of the Russian Federation, as well as in the territories under the jurisdiction of the Russian Federation or used under international treaties to which the Russian Federation is a party".

As the territory of the receiving State includes the land and buildings occupied by foreign States' representations, the said informatization objects, information systems and communication networks encompass those, and in particular the video conferencing systems, of foreign States' representations.[1] The inviolability and other immunities of their premises, objects, systems and networks are not equivalent to their complete exemption from the receiving State's jurisdiction, and where the use of video conference or any other of those technologies violates its laws and regulations and is regarded by it as the use of the mission's premises in a manner incompatible with its functions, the receiving State may employ the exceptions to the said inviolability and other immunities which are allowed by international law.

In view of the above, in instances like this and taking account of mutual interest in the same activities, the foreign counterparts

and principles of responsible behaviour of States, enshrined in the reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security on the application of international law to State use of ICTs.

[1] Conversely, "the territories under the jurisdiction of the Russian Federation or used under international treaties to which the Russian Federation is a party" include the RF diplomatic missions, consular posts, other representations and military bases abroad and other relevant overseas installations and facilities, their information systems and communications networks.

For the purposes of art. 5 (state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation) of the Federal Law of 26 July 2017 No. 187-FZ "On the Security of the Critical Information Infrastructure of the Russian Federation", "information resources of the Russian Federation" are comprised of "information systems, information and telecommunication networks and automated control systems located on the territory of the Russian Federation, in diplomatic missions and (or) consular posts of the Russian Federation".

concerned could be advised that in the light of the object and purpose of art. 5 (j) and (m) of the Vienna Convention on Consular Relations, the receiving State does not object, subject to reciprocity, to the consular officers and diplomatic agents of the embassy and consular posts of the sending State conducting, on the basis of requests from judicial and law enforcement authorities of the sending State, hearings of nationals of the sending State who do not have citizenship of the receiving State and serving documents on them in accordance with the laws and regulations of the sending State, in criminal, civil, commercial and administrative matters, provided that no coercive measures are used. These actions may also be performed through the use of video conference in the territory of the receiving State within the respective consular district or outside it in accordance with art. 6 of the Vienna Convention on Consular Relations. At the same time, the receiving State objects to the representatives of the sending State's judicial or law enforcement authorities taking part in such actions of consular legal assistance. In particular, interrogations and other procedural actions by video conference in criminal matters, in the (virtual) presence of officials from judicial or law enforcement authorities of the sending State, should be performed in accordance with the applicable treaty on mutual legal assistance in criminal matters. In the same manner, it is admissible to ensure participation or presence of consular officers or diplomatic agents of the sending State in the requested actions performed by the competent authorities of the receiving State.

A similar approach is taken in cases where the legal assistance treaty with the relevant state contains a rule on the use of videoconferencing in the provision of "classic" international legal assistance, but at the same time does not stipulate it for consular legal assistance,[1] or when neither the legal assistance treaty nor the consular convention contain provisions for the use of videoconferencing.

The issues raised by the Philippines are brought about by the processes of improvement and digitization of traditional forms of international cooperation, including consular legal assistance in criminal matters, which accelerated against the background of

[1] Treaty between the Russian Federation and the Syrian Arab Republic on Mutual Legal Assistance in Criminal Matters of 29 June 2022 (arts. 21–23).

the pandemic, and therefore one may predict a wider expansion of relevant practices.

As part of anti-COVID measures[1] in 2020, the Criminal Procedure Code of the Republic of Poland (RP CPC)[2] (art. 177) and the Polish Consular Law[3] (art. 26) were supplemented with the following provisions on interrogation by video conference: the interrogation of a witness can take place with the use of technical devices that allow remote conduct of this action with simultaneous direct transmission of image and sound. During proceedings in court, a court counsel, assistant to a judge or officer of the court, in whose district the witness is staying, takes part in the action at the place where the witness is present. A consular officer may be present[4] instead of the said persons at the place of stay of the witness being interrogated in this manner, if the witness, who is a Polish citizen, is staying abroad. By virtue of art. 197 of the RP CPC, this provision also applies to an expert.[5]However, the interrogation of an accused through the use of videoconferencing systems can be carried out in a domestic format, but not abroad, which follows from art. 377(4) of the RP CPC and, in the context of the correlation of consular legal assistance with ordinary international legal assistance, is consistent with Poland's declaration to the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters

[1] Ustawa z dnia 19 czerwca 2020 r. o dopłatach do oprocentowania kredytów bankowych udzielanych przedsiębiorcom dotkniętym skutkami COVID-19 oraz o uproszczonym postępowaniu o zatwierdzenie układu w związku z wystąpieniem COVID-19 [Law of 19 June 2020 on interest rate subsidies for bank credits granted to entrepreneurs affected by the consequences of COVID-19 and on the simplified procedure for approval of an arrangement in connection with the occurence of COVID-19] (art. 39, 57).

[2] Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego.

[3] Ustawa z dnia 25 czerwca 2015 r. Prawo konsularne.

[4] By using this term, Polish law expresses the most limited, passive nature of the consul's procedural role in the action at issue, which is reduced only to the presence during its conduct, although in reality the participation of the consul must inherently include at least actions related to the identification of the interrogatee.

[5] Some countries object to consular hearings via videoconferencing, recognizing this as a violation of their sovereignty, the administration of justice by foreign judicial authorities on their territory, and also pointing out the need to ensure that the rights of examined persons be protected by competent judicial authorities. See: P.M. Nowak, "Pomoc prawna konsula w praktyce" [Consul's legal assistance in practice], *temidium.pl Portal Okręgowej Izby Radców Prawnych w Warszawie*, 1 Apr. 2022, URL: https://www.temidium.pl/artykul/pomoc_prawna_konsula_w_praktyce-6954.html, accessed Sept. 3, 2022.

of 2001, and some other treaties, on the nonuse of the possibility of interrogation by video conference of the accused or suspect. It is debatable whether Polish law provides for interrogation by telephone conference in general, and within the framework of international (for example, on the basis of the aforementioned 2001 Protocol) and consular legal assistance, in particular. Some Polish authors mention the possibility of consular interrogations through the use of a telephone conference.[1]

As opposed to the RP CPC and Consular Law, in 2021 Polish special "anti-COVID" law of 2020 was supplemented with a provision specifically on consular interrogation in pursuance of a court commission, according to which, in cases considered in civil proceedings, interrogation by a consul is carried out using technical devices that allow its remote conduct with simultaneous direct transmission of image and sound, if the court *ex officio* (upon its own initiative) or at the request of the consul considers this necessary due to the crisis situation caused by COVID-19 at the place of interrogation. The course of the interrogation is recorded using a device that captures images or sounds. An image or sound recording constitutes an attachment to the interrogation protocol. Putting the signatures of persons other than the consul in the protocol is not required.[2] The materials drawn up for the draft of this law explain that the introduction of this provision is due to the unfavorable epidemiological situation in many foreign countries, which actually prevents Polish consuls from performing the actions assigned to them by the courts; given the right to a fair trial, such a decision applies only to civil cases, since the application of such provisions to criminal cases could limit too far a defendant's right of defence.[3]

---

[1] Ł.D. Dąbrowski, *Dowód z przesłuchania stron i innych uczestników procesu przez konsula — wybrane zagadnienia procesowe* [Evidence of interrogation of parties and other participants in proceedings by a consul: selected procedural issues], in Polskie prawo konsularne w okresie zmian. Pod redakcją W. Burka i P. Czubika (Warszawa: Ministerstwo Spraw Zagranicznych RP, 2015), s. 33–42.

[2] Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych [Law of 2 Mar. 2020 on particular solutions related to preventing, counteracting and combating COVID-19, other contagious diseases and crisis situations caused by them] (art. 15zzs[8]).

[3] Projekt ustawy o zmianie ustawy — Kodeks postępowania cywilnego oraz niektórych innych ustaw. Druk sejmowy nr 899, 15 stycznia 2021 r.

In accordance with art. 209.2 of the Criminal Procedure Code of the Republic of Armenia of 1 September 1998 No. ZR-248[1] (Particularities of interrogation by video-link of a witness or victim who is outside the territory of the Republic of Armenia) (introduced in 2020; the Code does not contain its analogue for the stage of court proceedings), the interrogation of a witness or victim who is present outside the territory of the Republic of Armenia, by decision of the body of preliminary investigation, can be organized via video-link through the body of diplomatic service of the Republic of Armenia, which provides consular services in a foreign state, in the event that the witness or victim appears before this body. Before the interrogation, the body of diplomatic service checks and certifies the identity of the witness or victim and provides video communication for the purpose of the body of preliminary investigation performing the procedural actions provided for by this article. Interrogation of a witness or victim by video-link is carried out in compliance with the rules established by arts. 206 (Interrogation of a witness[2]) and 208 (Interrogation of a deaf or other severely ill witness[3]) of the Code, taking into account the specificities set out in art. 209.2, and in case of interrogation of a minor witness or victim, also taking account of the requirements established by art. 207 of the Code.[4]

Before interrogation, the investigator certifies the identity of the witness, communicates factual grounds on which the criminal case was initiated, in which he is being interrogated, and warns of his obligation to tell everything that he knows about the case, as well as of criminal liability for refusing to testify, giving false testimony, advises of his right not to testify against himself, his spouse and close relative if the witness reasonably assumes that his testimony can later be used against him or them, and that his testimony can be

[1] It ceased to be in force on 1 July 2022. The Criminal Procedure Code of the Republic of Armenia of 27 July 2021 No. ZR-306 has not retained this provision.

[2] If the witness appeared for interrogation with a lawyer who was invited by the witness in order to provide the latter with legal aid, then the lawyer has the right to be present during the interrogation.

[3] Interrogation of a deaf witness is carried out with the participation of a sign language interpreter. If the witness suffers from a mental or other serious illness, the interrogation of the witness is carried out with the permission and in the presence of a doctor.

[4] Interrogation of a witness or victim under the age of sixteen is carried out with the participation of a teacher or qualified psychologist. During the interrogation of a minor witness or minor victim, his legal representative has the right to be present.

used as evidence. After that, the investigator establishes the nature of the relationship of the interrogated person with the suspect, accused, victim or witness and begins the interrogation.

The aforementioned actions, the course and results of the interrogation are recorded by audiovisual technical means in accordance with the rules of the Code. On the interrogation carried out in the manner prescribed by art. 209.2, a protocol is drawn up and sent to the body of diplomatic service of the Republic of Armenia, which provides consular services in a foreign state, in order to have the interrogated person familiarized with it. The interrogated person signs the protocol, and if there exist additions and corrections, makes an appropriate note in the protocol. In case of refusal to sign the protocol of interrogation, a corresponding note is entered into the protocol. The protocol of interrogation is sent to the investigator.

This type of interrogation does not constitute the taking of testimony by way of consular legal assistance provided for by international treaties of Armenia and art. 29 of the Law of the Republic of Armenia on the Consular Service of 7 June 1996 No. ZR-61, according to which the head of the consular post executes commissions of courts, public prosecutor's office and investigative bodies of the Republic of Armenia in respect of citizens of the Republic of Armenia who are present within his consular district, transmitted to him through the Ministry of Foreign Affairs of the Republic of Armenia. These commissions are executed in accordance with the legislation of the Republic of Armenia and norms of international law.

As one can see from the described foreign norms, a consular officer or diplomatic agent is, in fact, assigned only the functions of an organizational and technical nature to ensure the conduct of a remote investigative/judicial action, primarily with regard to identifying the person of the interrogatee.[1] Thus, they do not act

[1] Such organizational and supportive functions are entrusted by the RF CPC (arts. 189[1], 241[1] and 278[1]) and the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters of 2001 (art. 9) to the investigation bodies and courts at the location (outside the venue of proceedings in the case) of a person interrogated or participating in another investigative or court proceeding, which is carried out by the investigating body in charge of the case or the court examining the criminal case on the merits, namely the following: summoning, organizing the participation of the person in an investigative or court proceeding, identifying his or her personality; ensuring the participation of an interpreter or/and a lawyer; obtaining signatures and recognizances of the participants in proceedings, receipt of documents submitted by them. The Second

as interrogators directly performing these proceedings, which are actually carried out by somebody else, that is criminal investigators or courts of the sending state, so the former rather play the limited, auxiliary role of mere facilitators or assistants while the latter have the full-blown capacity of actual actors and decision-makers.[1] In addition, such proceedings do not involve the participation of investigative authorities or courts of the host state, whose assistance is not requested for their conduct. Hence, there is no consular or international legal assistance taking place — instead, the investigatory bodies or courts of the sending state thus exercise their extraterritorial jurisdiction to enforce directly in relation to the participants in criminal proceedings who are present in the territory of the state hosting the relevant foreign mission.

Therefore, the Prosecutor General's Office of the Russian Federation refuses to give consent to such proceedings (in cases when such consent is requested from it by foreign counterparts), since they are not consistent with the legislation and international treaties of the Russian Federation, and suggests instead to arrange for relevant investigative actions to be carried out in compliance with art. 9 (Hearing by video conference) of the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, or the provisions of other international treaties of the Russian Federation, as well as art. 189[1] RF CPC, with the possible participation or presence of consular officers of the requesting state.

Domestic legislation of individual countries may allow law enforcement and judicial authorities performing such extraterritorial actions on their own by videoconferencing outside the international or consular legal assistance procedures, which can also be performed with the mentioned participation of consuls, acting solely in their auxiliary capacity of facilitators.

According to art. 113(11-13) of the Criminal Procedure Code of Georgia (Interview procedure), "a public prosecutor, or an investigator with the consent of a public prosecutor, shall be authorised to

Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, as opposed to the RF CPC, imposes the drawing up of an interrogation protocol (minutes) on the authority of the requested party.

[1] See also on this: P. Rylski, "Przesłuchanie przed konsulem w postępowaniu cywilnym" [Interrogation before a consul in civil proceedings], *Przegląd Sądowy* 6 (2019), s. 7–35.

interview, remotely with the use of electronic means, a person staying within the territory of a foreign state without sending a request for legal assistance if interviewing a person using such procedure is permitted by a relevant international treaty of Georgia, the law of the state where this person is present, or/and by the clearly formed practice of this state. A person may not be interviewed in this manner if the person to be interviewed has not expressed a direct and explicit consent to be interviewed. A person may be questioned in this manner at the investigation stage as well".

Under arts. 2–3 RF CPC, Russian investigative authorities or courts, in cases of any extraterritorial criminal offence falling within Russia's prescriptive jurisdiction (art. 12 of the RF Criminal Code), are entitled to conduct particular investigative and other procedural actions outside the territory of the Russian Federation (not necessarily in the country of the *locus delicti*) on their own, including with respect to foreign nationals and stateless persons (also when they are suspects or accused), in accordance with the procedures of the RF CPC, which provides for legal effect of evidence so gathered. This provision applies not in isolation but only in conjunction with international law norms, the generally recognized principle of the sovereign equality of states and its derivative principle of non-intervention in the domestic affairs of another country, which have priority and require the receiving state's consent to such activities either in each individual case or expressed in a treaty or other document of an international character containing obligations recognized by the relevant state (notably, binding UN Security Council resolutions), or without consent in exceptional cases not contrary to universally recognized principles and norms of international law and international treaties to which the Russian Federation is a party, for instance, to preserve evidence during extraterritorial operations in exercise of a nation's right to self-defence. However, these provisions are not applicable to cases of criminal offences committed within the territory of the Russian Federation.

In German literature, it is rightly argued that the interrogation of a person conducted by a German presiding judge from the German territory by means of video conference through a German consul in the premises of a German foreign representation in a foreign state (on whose territory the said judge thus exerts foreign sovereign

power[1]), questioning of such an interrogee by other participants in the criminal proceeding, are not covered by the powers of the consul, including his right to conduct hearings himself, which he is initially allowed to perform by the receiving state (by exequatur, etc.), and therefore require a separate prior consent of the receiving state (in the form of a response to a German official request for international legal assistance, or even received by the consul from the competent authority of the host state in an informal manner). Otherwise, the sovereign interests of the host state are not observed, because, by virtue of the provisions of the Vienna Conventions and other norms of international law, the host state has at its disposal the control mechanisms in relation to a foreign consul, but not in relation to a foreign judge, and in case of unauthorized performance of such an audiovisual interrogation or hearing with the participation of the consul, the latter may be declared not acceptable for further stay in the host country or *persona non grata*.[2] In such cases, the German concept of the exclusively domestic nature of consular administrative assistance in criminal matters, as distinct from interstate legal assistance, fails to be fully applicable.

In the past, in isolated cases, embassies of some foreign states in Moscow used to provide their premises and equipment for the Russian investigative authorities to conduct, in accordance with Russian criminal procedure, interrogations by videoconferencing with the competent authorities of those states in pursuance of the latter's requests for international legal assistance.[3] The current level of technical equipment of the Russian investigative and judicial bodies makes this type of interaction redundant, moreover, due to

[1] At the same time, it is emphasized that audiovisual hearings and other administrative assistance of German diplomatic and consular missions cannot substitute the sovereign powers of the presiding judge in judicial proceedings in the territory of Germany, in particular, to take action for violation of order in the court session. See: K. Malek, *Verteidigung in der Hauptverhandlung*. 5. Auflage (Heidelberg: C.F. Müller, 2017), S. 249.

[2] A.B. Norouzi, *Die audiovisuelle Vernehmung von Auslandszeugen. Ein Beitrag zum transnationalen Beweisrecht im deutschen Strafprozess* (Tübingen: Mohr Siebeck, 2010), S. 96–98.

[3] И.М. Нурбеков, *Тактико-организационные особенности взаимодействия при расследовании преступлений международного характера: дис. ... канд. юрид. наук* [Tactical and organizational particularities of interaction in the investigation of crimes of an international character: PhD in Law dissertation] (M., 2010), pp. 178–179.

the requirements of art. 189[1] RF CPC on the mandatory use of videoconferencing systems of state preliminary investigation authorities, it is altogether inadmissible.

The issues of consular legal assistance in obtaining evidence by means of videoconferencing systems are most developed in relation to civil cases by the Hague Conference on Private International Law in relation to the Convention on the Taking of Evidence Abroad in Civil or Commercial Matters of 18 March 1970 (arts. 15–16 and 18–22).[1] The relevant documents can serve as a guidance or reference points and, in some practical scenarios, by agreement of the states concerned, be used by analogy with respect to criminal cases.

Based on the results of the interpretation and application of this Convention, it is recognized that consular officers and diplomatic agents, being endowed by the Convention with the right, under certain conditions, to obtain testimony and other evidence at the request of a court (competent authority) of the sending state for legal assistance, are also entitled to carry out "direct taking of evidence" by video-link from the state of execution, which is a party to the Convention and allows such proceedings. In addition, other alternative scenarios could be envisaged, like: in the case of geographically large areas a consul could use video-link to examine a witness located at a location which is a (significant) distance from the consular post but nonetheless still within the state of execution; in some rare cases, a consul may be located neither in the state of origin nor the state of execution, but in a third state, and be charged with taking evidence of the witness/expert physically located in the state of execution allowing these actions under the 1970 Evidence Convention (e.g., where the diplomatic mission (or consular post)

[1] Е.А. Куделич, "Видеоконференцсвязь как инструмент международной правовой помощи по гражданским и торговым делам" [Video conferencing as an instrument of international legal assistance in civil and commercial matters], *Закон* 8 (2012), pp. 39–50.

Explanations of the states parties to the 1970 Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (arts. 15–16 and 18–22) regarding their interpretation and application of the provisions of this Convention on the obtaining of evidence at consular posts and diplomatic missions through the use of videoconferencing systems are published in the "State Responses" subsection of the "Country Profiles" section of the official portal of the Hague Conference on Private International Law (URL: https://www.hcch.net).

of the state of origin accredited to the state of execution is located in a third state party to the Convention).[1]

In turn, the remote virtual presence or participation of the parties and their representatives and/or judicial personnel who are located in the sending state, may be permitted in such consular examinations by video-link to the same extent and subject to the same conditions of the state of execution as these persons could be physically present in its territory. This three-way video-link (court, consul, witness) should be established in the presence of another person competent to identify the witness and to ensure that the witness remains free from coaching and/or coercion at all times.[2]

However, it is arguably evident that such mechanisms are difficult to implement. Firstly, it is not clear who can be the person that identifies the witness in another place, on behalf of, instead of and for, the consul interrogating him (for example, this could be a notary of the relevant state).

Secondly, as can be seen from the above, the virtual presence or participation in consular actions of a judge, prosecutor, defence counsel, criminal investigator, or/and other participants in the proceedings is actually equated to a physical one and requires the consent of the state of execution, as a rule, within the framework of the international legal assistance procedure. At the same time, it is difficult to imagine a situation in which these persons would be solely observers, static figures, keeping complete silence and passivity during the interrogation performed by a consul of their own state (as opposed to cases of being allowed just to be present at the

[1] These scenarios can take place due to the provisions of art. 6 (Exercise of consular functions outside the consular district) and 7 (Exercise of consular functions in a third State) of the Vienna Convention on Consular Relations, bilateral consular conventions, art. 16(5) of the RF Consular Statute in conjunction with arts. 15–16 of the Evidence Convention ("a diplomatic officer or consular agent of a Contracting State may, in the territory of another Contracting State and within the area where he exercises his functions, take the evidence […] in aid of proceedings commenced in the courts of a State which he represents.")

According to art. 5 of the Vienna Convention on Diplomatic Relations, the sending State may, after it has given due notification to the receiving States concerned, accredit a head of mission or assign any member of the diplomatic staff, as the case may be, to more than one State, unless there is express objection by any of the receiving States.

[2] *Guide to Good Practice on the Use of Video-Link under the Evidence Convention* (The Hague: The Hague Conference on Private International Law — HCCH Permanent Bureau, 2020), pp. 67–68, 129–130, 151 and 176.

execution of an international legal assistance request by a foreign official). This would rather contradict their procedural status, role, functions, rights and obligations established by law, in particular in the context of the use of videoconferencing systems during the conduct of investigative or judicial actions (arts. 189[1] and 241[1] RF CPC), where they are the principal dynamic actors, but by no means those background static "present" figures.

At least, the record of such interrogation should in all cases be made by the consul and may not contain questions put to the interrogatee by the participants in the proceedings directly by themselves, but it would be acceptable for them to ask questions of the interrogatee through the consul and receive answers to them in the same way, by analogy with the presence and asking questions through a foreign public prosecutor, criminal investigator or judge conducting an investigative or court action as part of international legal assistance. If these conditions are met, the mentioned consent of the state of execution may not be required, unless it has stipulated otherwise. At the same time, given that, unlike the said foreign official, the consul does not have the right to disallow or change the questions (the list of which is provided to him in advance with the request for consular legal assistance), this artificial construction to a large extent loses its meaning.

In all cases, it is recommended to make an audiovisual recording of consular proceedings, whose records should be transmitted to the requesting authority of the sending state, along with the protocol (minutes) of the investigative/judicial action, recognizances and other documents.

Certain legal challenges in consular examinations via videoconferencing lie in the realm of criminalization, penalization and conflicts, both positive and negative, of territorial and extraterritorial jurisdictions of the sending state, receiving state, state of execution and third states, in relation to perjury under oath or affirmation or after the warning of liability for it, as well as to contempt of court. It appears that the predominant approach is to classify these acts under the law of the state of the court considering the case (*lex fori*), given the "virtual presence" of the witness/expert in the courtroom.[1]

When preparing audiovisual interrogations, the consul must resolve many internal legal, organizational and technical issues

[1] *Ibid*., pp. 76–77.

related to keeping a record/drawing up minutes or transcript of a proceeding, stenographing, using video and/or audio recording or filming, equipping the premises of the non-official area, admission to these premises and participation of third-party individuals other than the interrogatee, and organizations, both from the sending state and the host country, such as an IT specialist, interpreter, defence counsel (lawyer), legal representative (guardian), psychologist, teacher (when interrogating a minor), as well as handle the selection, verification, clearance and admission to the provision of services of commercial organizations that supply, install and/or maintain the relevant equipment and software for audiovisual broadcasting, interpretation and translation.

Consular interrogations by means of videoconferencing are widely used in common law countries, where representatives of the parties (legal counsel) gather evidence abroad themselves. Often it is the legal representative who takes the deposition in the presence of the consul, and in some instances the legal representative may even ask the consul to absent him or herself. In such instances, the primary role of the consul is to verify the identity of and administer the oath to the witness and/or assist with the testimony by arranging for an interpreter or translator, stenographer, videographer/video operator and other specialists if necessary. For example, a US consular officer presides over the deposition, but after administering the oaths he can withdraw, subject to recall, and then the interrogation is actually conducted by legal counsel.

In addition, in these countries, the requesting or requested state (their courts) often appoint a judge, public prosecutor or criminal investigator of the requesting state as a commissioner in accordance with art. 17 of the Evidence Convention, so that he could conduct the interrogation directly by himself, including in a cross-border format via videoconferencing, with the possible participation of a consul of the requesting state in the state of execution.[1]

The Swiss practice of international cooperation in civil matters proceeds from the premise that the interrogation by foreign competent authorities or legal counsel via videoconference from abroad of witnesses or parties located in Switzerland constitutes an interactive sovereign procedural action on Swiss state territory; therefore, its

[1] *Ibid.*, p. 72; *US Department of State Foreign Affairs Manual*, 7 FAM 920 — 7 FAM Exhibit 926.3.

performance requires the consent of the competent Swiss authorities, which is obtained under the same conditions as in the case of consent to the physical presence of the said authorities or counsel in Switzerland. This equally applies to consular interrogations by videoconference. Since, however, the parties are not in the same premises, there should be envisaged an identification procedure. Similar rules are applied by Switzerland to consular interrogations by telephone conference.[1]

§ 5. Electronic Evidence, Provisional Measures and Confiscation relating to Virtual Assets

Jurisdiction

The provisions of art. 14 (Circulation of digital currency) of Federal Law of 31 July 2020 No. 259-FZ "On Digital Financial Assets, Digital Currency and on Amendments to Certain Legislative Acts of the Russian Federation" (hereinafter referred to as Law No. 259-FZ) are key for determining the grounds for criminal jurisdiction, both substantive (to prescribe) and adjective (to enforce) with respect to actions related to the organization of issuance, issuance and organization of circulation of digital currency in the Russian Federation. The provisions of this article establish: (1) the spatial limits of the territorial jurisdiction of the Russian Federation in relation to the said actions — at the objects of the Russian information infrastructure, which is comprised of domain names and network addresses located in the Russian national domain zone, information systems, the technical means of which are located on the territory of the Russian Federation, and complexes of software and hardware means located on the territory of the Russian Federation, and in respect of user equipment located on the territory of the Russian Federation; (2) the effect of the Russian jurisdiction in relation to the range of persons — in respect of legal entities whose personal law is Russian law, branches, representative offices and other separate divisions of international organizations and foreign legal entities, companies and other corporate entities with civil legal capacity,

[1] Eidgenössisches Justiz- und Polizeidepartement EJPD, Bundesamt für Justiz BJ, *Die internationale Rechtshilfe in Zivilsachen: Wegleitung* [International legal assistance in civil matters: Guidance]. 3. Auflage 2003 (Stand Januar 2013), S. 35–36.

created on the territory of the Russian Federation, and individuals actually staying in the Russian Federation for at least 183 days over the course of 12 consecutive months.

A broader legal definition of the information infrastructure of the Russian Federation is given by Decree of the President of the Russian Federation of 5 December 2016 No. 646 "On Approval of the Doctrine of Information Security of the Russian Federation" (para. 2), as "a combination of informatization objects, information systems, Internet websites and communication networks located in the territory of the Russian Federation, as well as in the territories under the jurisdiction of the Russian Federation or used under international treaties to which the Russian Federation is a party".

As the territory of the receiving State includes the land and buildings occupied by foreign States' representations, the said informatization objects, information systems and communication networks encompass those of foreign States' representations. In turn, "the territories under the jurisdiction of the Russian Federation or used under international treaties to which the Russian Federation is a party" include the RF diplomatic missions, consular posts, other representations and military bases abroad and other relevant overseas installations and facilities, their information systems and communications networks.

For the purposes of art. 5 (state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation) of the Federal Law of 26 July 2017 No. 187-FZ "On the Security of the Critical Information Infrastructure of the Russian Federation", "information resources of the Russian Federation" are comprised of "information systems, information and telecommunication networks and automated control systems located on the territory of the Russian Federation, in diplomatic missions and (or) consular posts of the Russian Federation".[1]

[1] The Law contains the incomplete list of state foreign missions (only diplomatic missions and consular posts). See, e.g.: the Federal Law "On the Public Prosecutor's Office of the Russian Federation" (art. 39[1]), which contains a complete list of state foreign missions of the Russian Federation ("diplomatic missions and consular posts of the Russian Federation, missions of the Russian Federation to international organizations, other official representations of the Russian Federation and representations of federal executive bodies located outside the territory of the Russian Federation").

Federal Law of 1 July 2021 No. 236-FZ "On the Activities of Foreign Persons on the Information and Telecommunications Network "Internet" in the Territory of the Russian Federation" (informally, the law on "landing" of foreign IT companies in Russia) (art. 4), regulating the problem of localization of data, gives a definition of a foreign person operating on the Internet in the territory of the Russian Federation, against whom compulsory measures may be applied to have it comply with the requirements of the legislation of the Russian Federation.

The Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor), other Russian competent authorities and courts exercise their powers with respect to foreign service providers offering their services in, from and/or for the Russian Federation.

The provisions of the 2021 FATF Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers on the licensing and registration of such providers can also serve as a guide when defining the rules for establishing and exercising broader both territorial and extraterritorial criminal jurisdiction. The Guidance specifies that VASPs should be required to be licensed or registered in the jurisdiction(s) where they are created (incorporated, registered, etc.). In cases where the VASP is a natural person, it should be required to be licensed or registered in the jurisdiction where its place of business is located — the determination of which may include several factors for consideration by countries. The place of business of a natural person can be characterised by the primary location where the business is performed or where the business' books and records are kept as well as where the natural person resides (i.e., where the natural person is physically present, located, or resident). When a natural person conducts business from his/her residence, or a place of business cannot be identified, his/her primary residence may be regarded as his/her place of business, for example.

The place of business may also include, as one potential factor for consideration, the location of the server of the business.

.Jurisdictions may also require VASPs that offer products and/or services to customers in, or that conduct operations from, their jurisdiction to be licensed or registered in the jurisdiction. Host jurisdictions may therefore require registration or licencing of VASPs whose services can be accessed by or are made available to people residing or living within their jurisdiction, or may require

VASPs that have employees or management located in their jurisdiction. While coverage of these entities is not required by the FATF Standards, jurisdictions may find it to be useful in mitigating risks, particularly in view of the inherent cross-border availability of VAs. When in doubt, jurisdictions may consider that broader coverage is the safer course, as VAs will introduce whatever risks they carry with them in any jurisdiction in which they are accessible, regardless of the location in which they are incorporated.

In order to identify those VASPs offering products and/or services to customers in a jurisdiction without being incorporated in this jurisdiction, supervisors may use a set of relevant criteria. This could include the location of offices and servers (including customer-facing operations such as call centres), promotional communications targeting specific countries/markets, the language on the VASP website and/or mobile application, whether the VASP has a distribution network in a country (e.g., if it has appointed an intermediary to seek clients or physically visit clients resident in the country), and specific information asked to customers revealing the targeted country.[1]

Thus, one of the principal grounds for asserting and extending legitimate jurisdiction is determined by applying the targeting test, that is whether VA services (offered by cryptocurrency exchanges, custodians of crypto wallets,[2] etc.) are aimed at the consumer market of the country claiming jurisdiction. Such focus, in turn, can be determined by a combination of direct and indirect indications, which include a disclaimer, domain and top-level domain, the language of the portal interface or other country-specific references and the legal framework.[3]

Individual countries have adopted extraterritorial blocking statutes in relation to foreign operators of crypto platforms and cryptocurrency exchange targeting their territory from the outside.

---

[1] *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (Paris: FATF, 2021), pp. 43–44 and 107, paras. 125–128; *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (Paris: FATF, 2019), pp. 22–23 and 29, paras. 78–79, 81 and 113.

[2] There exist various types of cryptocurrency wallets: hardware, mobile, paper, desktop, USB, web (online) wallets, multi-signature, browser and hybrid wallets, wallets with a QR code, and also using technology such as Bluetooth; all of them, depending on whether or not they have an Internet connection, are divided into "hot" and "cold" (offline, "off the grid") wallets, respectively.

[3] *Guidance for a Risk-Based Approach to Virtual Currencies* (Paris: FATF, 2015), p. 18, para. 71.

For example, "provision of services by overseas virtual currency exchanges to residents in China via the internet is also considered to be an illegal financial activity. The domestic staff members of overseas virtual currency exchanges and those legal persons, unincorporated organizations, and natural persons that know or should have known that such exchanges are engaging in virtual currency-related business but still provide marketing, advertising, payment, settlement, technical support, or other services will be held accountable in accordance with the law".[1]

The Russian Federation's substantive criminal jurisdiction over relevant acts containing elements of criminal offences can only be asserted if they fall under the provisions of arts. 11–12 of the RF Criminal Code, including the protective extraterritorial jurisdictional principle, where, for example, the crime is directed against the interests of the Russian Federation in ensuring the financial security of the state, and procedural criminal jurisdiction can be exerted only if there are grounds enshrined in arts. 2–3 RF CPC.[2]

State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory.[3] Therefore, countries generally tend to regard remote "intangible" activities of representatives of a foreign state carried out from within its territory and physically reaching the persons or objects that are known to be located in those countries as activi-

[1] Notice on Further Preventing and Resolving the Risks of Virtual Currency Trading and Speculation of 15 Sept. 2021, issued by the People's Bank of China, Cyberspace Administration of China, the Supreme People's Court, the Supreme People's Procuratorate, Ministry of Industry and Information Technology, Ministry of Public Security, State Administration for Market Regulation, China Banking and Insurance Regulatory Commission, China Securities Regulatory Commission, State Administration of Foreign Exchange (para. 3). URL: http://www.pbc.gov.cn/en/3688253/3689012/4353814/index.html, accessed Jan. 4, 2024.

[2] See also: *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* / Ed. by M.N. Schmitt, L. Vihul (Cambridge: Cambridge University Press, 2017), pp. 51–78.

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

ties undertaken within their own territory. Such activities include cross-border contacts via any communication networks with persons knowingly staying and using relevant endpoint device on the territory of the country concerned (legal fiction of the "territorialization" of cyberspace). In cases of aforementioned actions and communications performed without informing the authorities of the state on whose territory the information system or other device used by their addressee is located, they can be regarded as violating international legal principles of the sovereign equality of states, non-interference in the internal affairs of another state, viewed as constituting a crime or other offence or internationally wrongful act.

This fully applies to transnational communications with ICT service providers, including VASPs. Therefore, states strive to agree on the international rules for mutually acceptable lawful behavior of this kind.

The "target" jurisdictional criterion mentioned in the context of the FATF standards was already laid down in art. 18 of the 2001 Convention on Cybercrime: its provisions empower 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, including their possible dispersion over the territories of different countries, the circumstance that the user's device is in roaming mode, or "loss of location" of data, as well as any other parameters.

2023 EU Regulation on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings and Directive 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 determine jurisdictions concerned, inter alia, based on the said target criterion.

The anti-crime regulation of virtual assets and states' jurisdiction to prescribe over acts related to them (in particular, the establishment of mandatory territorial jurisdiction based on the criteria of the

physical presence of the offender in the country's territory or the use of the information system in the country's territory when committing an offence) are dealt with in a number of sources of European law: the directives of the European Parliament and Council of the European Union of 2019 on Combating Fraud and Counterfeiting of Non-Cash Means of Payment,[1] and of 2015 (as amended in 2018) on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing;[2] besides, jurisdictional issues are covered in the directive of 2013 on Attacks against Information Systems,[3] as well as the Council Framework Decision of 2008 on Combating Certain Forms and Expressions of Racism and Xenophobia by means of Criminal Law.[4]

The procedures for requesting and rendering preservation and production of various types of electronic evidence (basic subscriber/user information, traffic and content data) from foreign VASPs are largely identical to those applied to general ICT service providers. Since in most cases gathering this evidence involves the use of coercive measures, disclosure of communication secrecy and of "quasi-banking" secrecy, a corresponding court order should be attached to the request for international legal assistance.

With regard to Russian law enforcement, investigative or judicial authorities' requests for voluntary preservation or production of electronic evidence, transmitted directly to foreign cryptocurrency

[1] Directive (EU) 2019/713 of the European Parliament and of the Council of 17 Apr. 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA (art. 12).

The preparatory materials for this directive (Procedure 2017/0226/COD) reflect the process of resolving the problem of a positive conflict of territorial jurisdictions of the EU countries based on the criteria of the physical presence of the offender in the country's territory or use of the information system in the country's territory when committing an offence.

[2] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Consolidated text with EEA relevance).

[3] Directive 2013/40/EU of the European Parliament and of the Council of 12 Aug. 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (art. 12).

[4] Council Framework Decision 2008/913/JHA of 28 Nov. 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law (art. 9).

exchanges and other VA custodians, one may argue that these are permissible insofar as they are envisaged by guidances or other instructions of these VASPs for foreign law enforcement and judiciary, officially published on their portals and thus denoting the express consent, implicit approval or acquiescence of the state of the VASP's "nationality" to such way of cross-border communications, and in all cases possible in relation to localized ("landed") VASPs.

As is known, in international legal assistance, one may confer on the requested foreign authority the performance of particular procedural actions, but not the taking of procedural decisions in a criminal case; the latter should precede the forwarding of the MLA request and be taken by an investigator, prosecutor or judge in charge of the case in the requesting state, since they are fraught with the need to secure rights, safeguards, immunities, duties and responsibilities of the participants in these proceedings, rightful owners of property concerned and *bona fide* third parties.

Therefore, a question arises as to whether it is appropriate to ask in requests for international judicial assistance in criminal matters to freeze or block virtual assets held by a foreign custodian/VASP (this kind of "administrative" request is typical for financial intelligence units' (FIU) international interaction rather than for that of judicial authorities), before a court's or other judicial decision is made on their seizure, attachment or any other provisional restraint measure,[1] and to execute such requests.

Firstly, such request not only means the foreign authority undertaking an action to freeze, but fully delegates to him the making of a decision on this coercive measure prior to its application as well. Secondly, such extrajudicial measure is normally not provided for by criminal procedure law nor requested in a domestic format, while conventions and other treaty provisions on freezing are evidently not self-executing. Legal assistance premises a partial transfer of jurisdiction and competence, for the purpose of and within the scope of the requested actions, from the requesting to the requested party, and the former cannot transfer to the latter something, which the former itself does not have. Therefore, law enforcement and judicial

[1] *Сбор и анализ цифровых следов преступления: практическое пособие* [Collection and analysis of digital traces of a crime: practical manual] / С.В. Петраков, М.А. Гудкова, Д.П. Бащук, А.А. Тимофеев, Д.Н. Пигильдин, И.С. Бедеров, Д.О. Сорокин, А.В. Пытайло (СПб: Изд-во Санкт-Петербургской академии Следственного комитета, 2023), 96 p.

authorities' (as opposed to FIU) right or power to make or execute such requests is disputable.

This particularly concerns such requests for suspension of transactions in cryptocurrency accounts addressed by investigative authorities to foreign VASPs, which is, however, without prejudice to the rights and duties of a service provider themselves to suspend or postpone, on their own, suspicious transactions, block accounts on their own initiative based on the information received from overseas investigatory authorities.

The following case study demonstrates the observance of those approaches.

Binance cryptocurrency exchange's Government Law Enforcement Guidelines published on its website, acknowledge their readiness to consider and answer direct official requests from foreign law enforcement authorities for preservation and production of evidence (records or information), at the same time requiring copies of official supporting documents (a valid court order from a competent jurisdiction or police orders/warrants) to be attached to the request, and warn of the default notice of requests to their users: unless specified in any court order or police warrant and on valid legal basis, they may notify the relevant user of the request before disclosure of any personal data.[1]

In 2022 and 2023, an investigative authority from the Russian Federation directly obtained, in the above described way, information on the Binance users, account balances and exchange rates in the course of investigation into criminal activities of a financial platform, the stolen assets from which were transferred to a number of static bitcoin addresses of foreign crypto exchanges, including to cryptocurrency wallet addresses of third persons allocated by Binance. In 2022, a district court in Moscow issued orders for seizure (i.e., provisional freeze) of cryptocurrency in the amount of current account balance and future funds to be credited to the account, in relation to the cryptocurrency wallet addresses allocated by Binance for the accounts verified in the name of citizens of two foreign countries (CIS and Baltic states). These orders were

[1] Binance Government Law Enforcement Request System, Government Law Enforcement Guidelines. URL: https://www.binance.com/en/support/law-enforcement, accessed Jan. 4, 2024.

forwarded for execution directly to the Binance e-mail account, to which Binance replied that transactions in the accounts indicated by the court had been suspended. About a year later, the Russian investigative authority received a mail from the Binance's technical support center informing of the need to submit official documents of those two states' competent authorities for blocking those accounts, as their users were citizens of those states.

Thus, the cryptocurrency exchange chose as a jurisdictional criterion the user's citizenship, rather than the exchange's own "nationality" (it holding registrations and licenses in several countries) as a basis for its further interactions with an overseas law enforcement authority and for determining a state authorized to interact with it for the purpose of blocking the cryptocurrency funds, which is not a standard approach. Binance was not licensed nor had its representative offices in the Russian Federation. Therefore, the Prosecutor General's Office of the Russian Federation, as a MLA central authority, forwarded the investigative body's requests for seizure of the said funds to the indicated foreign states of citizenship of the users, in which the Binance licensed dealers were registered as well.

Provisional Measures and Confiscation

Under the current legal regime for virtual assets[1] in the Russian Federation, taking immobilizing provisional measures with respect to them or confiscating them in criminal proceedings can still be challenging, since they are not recognized as property or its equivalent for all intents and purposes, but rather for a limited range of legal relations, for example, they can be subject to civil forfeiture of unexplained wealth (illicit enrichment) as property under anticorruption laws. Currently in most cases in criminal proceedings, virtual assets can be seized or confiscated after their prior conversion into fiat money or other property. Otherwise, they can only be seized or confiscated as an instrumentality of crime being a piece of physical evidence (object),[2] which is rather not a satisfactory solution.

[1] Cryptocurrencies, non-fungible tokens (NFTs) and other derivative products.

[2] See, e.g.: *Сбор и анализ цифровых следов преступления: практическое пособие* [Collection and analysis of digital traces of a crime: practical manual] / С.В. Петраков, М.А. Гудкова, Д.П. Бащук, А.А. Тимофеев, Д.Н. Пигильдин,

Seizure or other interim measures, confiscation or other conversion to state revenue in relation to digital financial assets (stablecoins) and digital currencies (cryptocurrencies), which are considered electronic data with property value, can be carried out only if law enforcement or judicial agencies have a private/signature key, a password for the owner's access to his/her electronic wallet or a mnemonic phrase (the so-called seed), and when virtual assets are stored on a crypto exchange/with another custodian, the latter, if they have both public/verification and private cryptographic keys,[1] should fulfill lawful orders presented to them by investigative/judicial authorities for enforcement of these measures.

The relevant procedural decision must contain the name and public address of the cryptocurrency wallet, certain types of which allow attaching to them an electronic "tag" (inscription) with the names of provisional or confiscation measures applied, the investigative body, public prosecutor's office or court implementing it, the case number, electronic signature etc., the name and amount of the cryptocurrency. One should draw up a record of the performed proceeding, to which it is advisable to attach screenshots of the crypto wallet.

High volatility of virtual asset value/exchange rates does not contribute to certainty in determining exactly which part of the crypto wallet's contents should be "seized", therefore it is necessary to calculate an average exchange rate of a cryptocurrency unit (market price of its purchase and sale) in relation to the official monetary unit — ruble, or other means of payment, according to the data of large cryptocurrency exchanges, and indicate it together with total amount, date and time of calculations in the protocol.

Where the owner of virtual assets provides to law enforcement or judiciary access to them, it does not, however, protect in any way from his own malicious actions or those of third parties consisting in their further disposal of these funds (transactions with virtual

И.С. Бедеров, Д.О. Сорокин, А.В. Пытайло (СПб: Изд-во Санкт-Петербургской академии Следственного комитета, 2023), 96 p.; М.М. Долгиева, *Теоретические основания уголовной политики в сфере оборота криптовалюты: дис. … д-ра юрид. наук* [Theoretical grounds of criminal policy in the sphere of circulation of cryptocurrency: Doctor of Laws dissertation] (M., 2023), pp. 356–373.

[1] That is addresses, which form the wallet, like, respectively, data about a bank account number and the holder's means of access to it.

assets, as a general rule, are irrevocable), counteraction of the criminal investigations or proceedings (using malware, cryptocurrency tumblers/mixers, anonymity-enhanced cryptocurrencies/privacy coins, chain-hopping, off-chain transactions, kill switches, etc.), when they are in possession of copied private keys/addresses, passwords or "seeds", and able to remotely access the wallet.

Therefore, in all cases, a prompt transfer of assets is required to be carried out to the addresses of cryptocurrency accounts of law enforcement or judicial authorities created for them in advance (crypto wallets, preferably multicurrency, multisignature, unhosted, hardware wallets on removable media protected by a PIN code or other software from unauthorized connection to the Internet, access to other external information and telecommunication networks), with the simultaneous removal of authorization identifiers on the medium belonging to the accused. It should also be borne in mind that it is necessary to pay the miners a transaction fee for the mentioned transfer, the amount of which will depend on the selected transfer processing speed, which in urgent cases can be a significant percentage of the transfer amount and therefore will further require a decision to whose account these costs will be charged.[1] From the moment of the transfer of control over these data records to the competent authority, such authority is responsible for the proper management thereof, including for ensuring the safety of assets, therefore, in the record of the proceeding, it is necessary to indicate the persons who are entrusted with the storage of data, the place and conditions of storage. All subsequent actions with the assets are also subject to logging (with the exception of the details of the private key, passwords and seed phrases that should be kept separately and strictly confidential). A relevant specialist should also be involved.[2]

The feasibility of measures of restraint and confiscation will also depend on whether the relevant state exercises its enforcement ju-

[1] *Guide on seizing cryptocurrencies. Version 1.0* (Strasbourg: Cybercrime Programme Office of the Council of Europe, 2021), 118 p.

[2] P. Opitek, "Kryptowaluty jako przedmiot zabezpieczenia i poręczenia majątkowego" [Cryptocurrencies as an object of restraint and bail], *Prokuratura i Prawo* 6 (2017), s. 36–60; P. Opitek, "Kryptowaluty w aspekcie czynności dochodzeniowo-śledczych policji" [Cryptocurrencies in the context of inquiry and investigation activities of the police], *Przegląd Policyjny* 2(126) (2017), s. 138–158.

risdiction over the virtual asset platform, its service provider and/or users. The grounds for establishing and exercising this jurisdiction may be different: based on the place of incorporation or other establishment or of the physical presence of the service provider; the place where the services are offered; at the location of the servers, including data scattered over the territories of different states and migrating through temporary cloud storages,[1] and other software and hardware; the place where the service provider exercises their possession or control over the virtual assets in question.[2]

Territorial jurisdiction will also depend on the nature of the virtual currencies — these could be either centralized (for example, in-game currencies, tokens) or decentralized (cryptocurrency, including automatically managed by smart contracts). In the first case, this would be the place of registration or actual location of the administrator/operator, and in the second case, it would be the same, if the cryptocurrency is at the disposal of a crypto exchange or other custodian that have a sufficient scope of rights granted to them by their customer for access and management of his assets, or otherwise it could be the physical location of the user's endpoint data processing equipment or other ICT device, which hosts a non-custodial/self-custodial crypto wallet, that is under the effective control of the user himself, carrying out peer-to-peer transactions.

Therefore, the warrant/order for a provisional measure or confiscation may be served for execution either on the operator or other custodian, or directly on the user/owner himself or his counsel or other legal representative.

In the absence of such procedural jurisdiction, it is necessary to turn to the foreign state that has it, with a request for international legal assistance, with the said order enclosed, or, in cases of freezing/

[1] 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 data location; situations when data that form a single whole unit (information resource) get actually scattered in a fragmented and/or dynamic state over different jurisdictions, or have their numerous mirror copies in those jurisdictions.

[2] *Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies* (Vienna: UNODC, 2014), pp. 140–141, 146–153 and 225.

blocking of assets in the framework of combating money laundering, terrorism financing and the financing of proliferation of weapons of mass destruction, through the interaction of FIUs.

The 2023 US Department of Justice Asset Forfeiture Policy Manual indicates that many cryptocurrency service providers are located outside the United States. Prosecutors should consult the Office of International Affairs (OIA) regarding seizure of cryptocurrency from foreign service providers, such as institutional exchanges, even in cases where a wallet company does not itself have access to or control of the private key. Generally, seizures from foreign-located service providers will require use of a mutual legal assistance (MLA) treaty request or other similar authority. Some exchanges located outside the United States might have U.S. offices or points of contact and will accept service of U.S. seizure warrants; however, prosecutors and agents should seek the voluntary restraint of foreign-located assets only through U.S. points of contact. Prosecutors should not agree to accept any cryptocurrency from a foreign-located company without an MLA request or permission from OIA, even if the company offers to transfer the assets voluntarily. Doing so without an MLA request or permission from OIA could violate the sovereignty of another country.[1]

Taking into account the mentioned sharp fluctuations in the exchange rates of cryptocurrencies (volatility), in many situations it will be appropriate to exchange the "seized" virtual assets on a crypto exchange that works with the widest possible range of cryptocurrencies and preferably operates in domestic jurisdiction, with the subsequent crediting of fiat funds, generated from the sale of crypto assets, to the deposit account of the body that made the decision on applying the provisional measure, or, in the event of making a final decision to turn these funds into state revenue, to the account of the Federal Bailiffs Service. The experiences of European countries, however, show that before the adoption of final procedural decisions in criminal cases, virtual currencies are not usually sold, because in the event of termination of prosecution on exonerating grounds or acquittal of the defendant, they will have to be returned to their legitimate owner and the authorities may be required to satisfy various damage claims, like to pay the amount of

[1] *Asset Forfeiture Policy Manual (2023).* U.S. Department of Justice, 2023, pp. 2-10–2-12.

the exchange rate difference, miners' transaction fees, compensation, interest or lost profits.[1]

Individual countries have introduced special legal regimes for virtual assets in investigation, court and enforcement proceedings to preempt such scenarios. In cases envisaged in art. 132(18) of the Criminal Procedure Code of the Republic of Belarus,[2] realization of cryptocurrency is carried out by a suspect, accused or persons who bear material responsibility for their actions under law, through an operator of a crypto platform and (or) an operator of cryptocurrency exchange under the control of the body conducting the criminal process, and in case the realization of cryptocurrency is not possible in this manner, then without the participation of an operator of a crypto platform and (or) an operator of cryptocurrency exchange. The expenses (commission fees, remunerations) related to transactions (operations) with cryptocurrency in the framework of criminal process and enforcement proceedings, are not reimbursed to owners of cryptocurrency.[3]

If the authorities fail to secure cooperation on the part of the owner of a crypto account or for other reasons fail to access the account, it is recommended to use the equivalent (value-based) confiscation in fiat money instead of virtual assets, the amount of which is calculated at the aforementioned rate.[4]

Digital financial assets (stablecoins) may also serve as bail in criminal proceedings.[5]

---

[1] *Handling of virtual currencies in criminal investigations and proceedings*, in Cybercrime Judicial Monitor. Issue 5 — December 2019 (The Hague: Eurojust, 2019), pp. 29–34; *Guidance on Financial Investigations Involving Virtual Assets*. Aug. 2019. FATF/RTMG(2019)2/REV3.

[2] It regulates the lifting of seizure from the property on the motion of a suspect, accused or persons who bear material responsibility for their actions under law, in order to have it realized for certain purposes under the control of the body conducting the criminal process.

[3] Decree of the President of the Republic of Belarus of 14 Feb. 2022 No. 48 "On the Registry of addresses (identifiers) of virtual wallets and specificities of cryptocurrency circulation".

[4] M. Simmler, S. Selman, D. Burgermeister, "Beschlagnahme von Kryptowährungen im Strafverfahren", *Aktuelle Juristische Praxis (AJP)/Pratique Juridique Actuelle (PJA)* 8 (2018), S. 963–978.

[5] For further reading on the Russian Federation legal frameworks, case law and other law enforcement practices concerning virtual assets in the criminal law context, see: *Возврат из-за рубежа преступных активов: теория и практика: Учебное пособие* [Return of criminal assets from abroad: theory and practice:

§ 6. Experiences and Problems of Recognition and Use of Electronic Evidence in the Context of International Cooperation in Criminal Proceedings

One of the key elements of ensuring the admissibility of evidence, especially electronic evidence, is the certification of its authenticity.

In art. 455 RF CPC, the admissibility of foreign evidence is conditioned on its obligatory certification: evidence obtained in the territory of a foreign state by its officials in the course of their executing requests for legal assistance in criminal matters or sent to the Russian Federation as attachment to a request for the transfer of prosecution in accordance with international treaties of the Russian Federation, international agreements or on the basis of the principle of reciprocity, certified and transmitted in the prescribed manner, enjoys the same legal effect as if it were obtained in the territory of the Russian Federation in full compliance with the requirements of the RF CPC.

The issue of the need for and forms of legalization, i.e., authentication or certification of foreign documents and the authenticity of copies of foreign documents, is quite often faced in the process of international cooperation in criminal matters. In practice, decisions on this issue by authorized entities may have serious consequences for establishing the legal effect and admissibility of evidence obtained by the investigative authorities from abroad[1] and

study aid] / Д.А. Кунев; под науч. ред. А.Г. Волеводза (М.: Прометей, 2021) (Серия: Библиотека магистратуры «Международное сотрудничество в сфере правоохранительной деятельности и уголовной юстиции». Вып. 1), pp. 76–79, 137, 143–147, 208–211 and 224–227; *Особенности расследования преступлений, совершаемых с использованием цифровой валюты: монография* [Specificities of investigation into crimes committed with the use of digital currency: monograph] / под ред. Е.В. Емельяновой и О.С. Бутенко (СПб.: Санкт-Петербургская академия СК России, 2022), 250 p.; *Противодействие преступлениям, совершаемым в сфере оборота криптовалюты: учебное пособие* [Counteraction of crimes committed in the field of circulation of cryptocurrency] / Е.А. Русскевич, А.В. Андреев, Д.В. Галиев [и др.] (М.: ИНФРА-М, 2022), 211 p. (Высшее образование: Магистратура); И.Б. Тутынин, О.В. Химичева, *Применение мер уголовно-процессуального принуждения при расследовании преступлений, совершенных с использованием криптовалюты* [Application of measures of criminal procedural coercion in the investigation of crimes committed with the use of cryptocurrency] (М.: Юрлитинформ, 2022), 144 p.

[1] Ю.А. Цветков, "Принцип равенства юридической силы доказательств в международно-правовом сотрудничестве по уголовным делам" [The principle of equality of the legal effect of evidence in international legal coopera-

sometimes even determine the fate of the criminal case involving that evidence.[1] Apart from that, legalization may be required not only for incoming foreign materials but also for outgoing requests from the investigative authorities.

The two main forms of legalization of foreign documents used in international communications are consular legalization (sometimes, diplomatic legalization is also distinguished) the procedure for which is rather complicated and burdensome,[2] and attaching an Apostille[3] (including an electronic one[4]) in countries that have agreed to waive consular legalization. The third form for introducing foreign materials into the national document flow is a waiver of any legalization, unconditional[5] or conditional, which is provided for in international treaties that generally govern legal assistance and legal relations in civil, criminal and other matters, administrative assistance in customs and tax matters, etc. The fourth form for recognizing authenticity is the non-treaty absence of any requirements for whatever legalization from a foreign state.

tion in criminal matters], *Международное уголовное право и международная юстиция* 2 (2013), pp. 7–10.

[1] P.A. Litvishko, *Legalization of Materials of Requests for Legal Assistance and Prosecution*, in Collection of Materials on International Cooperation of the Investigative Committee of the Russian Federation (Moscow: Prospekt, 2016), pp. 218–225.

[2] See also: European Convention on the Abolition of Legalisation of Documents Executed by Diplomatic Agents or Consular Officers of 7 June 1968; Convention on the Exemption from Legalisation of Certain Records and Documents of 15 Sept. 1977. (The Russian Federation is not a party to these Conventions.)

[3] Convention of 5 Oct. 1961 Abolishing the Requirement of Legalisation for Foreign Public Documents; *Apostille Handbook: Practical Handbook on the Operation of the Apostille Convention* (The Hague: The Hague Conference on Private International Law Permanent Bureau, 2023), pp. 59–60, paras. 149 and 154–161.

[4] e-Apostille is a certificate issued under art. 3(1) of the Apostille Convention, when issued in electronic form. It is signed with a digital signature. Subject to domestic law or policy, e-Apostilles may be issued on electronic public documents or on paper public documents that have been scanned into electronic form or otherwise digitised. The issuance of e-Apostilles is one of the two components of the e-APP (electronic Apostille Programme) (the other being the operation of e-Registers).

Electronic documents should be distinguished from scanned copies of documents which are created by scanning a paper public document. Electronic public documents can only be apostillised if the State of origin has implemented the e-Apostille component of the e-APP.

[5] See, e.g.: European Convention on Mutual Assistance in Criminal Matters of 20 Apr. 1959 (art. 17).

The Apostille Convention applies to any official (public) documents in their broad sense (the list included in art. 1 is not exhaustive), including those emanating from police and criminal justice authorities, or related to extradition because they are covered by art. 1(2)(a) or (b) of the Convention. This is directly referred to in the sources of official interpretation of the Convention published by the Hague Conference on Private International Law.

At the same time, the Apostille Convention does not affect the right of the state of destination to determine the admissibility and probative value of foreign public documents. It remains for the laws of evidence of the state of destination to determine the extent to which a foreign public document may be used to establish the existence of a fact.[1]

Bilateral treaties and multilateral conventions of the USSR and the Russian Federation on legal assistance and legal relations ordinarily include provisions on the validity of documents of the Contracting Parties and equal legal effect of their official documents, while at the same time establishing the minimum concomitant condition for mutual recognition regarding simple affixing of a signature and seal (as a rule, a coat-of-arms or official seal).[2]

In the Anglo-American legal system, to certify the authenticity of documents, one also issues various kinds of custodial certificates regarding the chain of custody, and uses oaths and affirmations to confirm the authenticity.

Rule 902 of the US Federal Rules of Evidence[3] establishes items of evidence that are self-authenticating, i.e. requiring no extrinsic evidence of authenticity, such as, primarily, the testimony of a foundation/authentication witness, in order to be admitted, among which, since 2017, is electronic evidence, namely:

---

[1] *Apostille Handbook: Practical Handbook on the Operation of the Apostille Convention* (The Hague: The Hague Conference on Private International Law Permanent Bureau, 2023), 149 p.

[2] Treaty between the Russian Federation and the Republic of Poland on Legal Assistance and Legal Relations in Civil and Criminal Matters of 16 Sept. 1996 (arts. 6(2), 10 and 15); Convention on Legal Assistance and Legal Relations in Civil, Family and Criminal Matters of 22 Jan. 1993 (arts. 7(3), 11, 13 and 73(2)); Convention of the same name of 7 Oct. 2002 (arts. 10(2) and 12).

[3] Federal Rules of Evidence. See also: 18 US Code § 3505 (Foreign records of regularly conducted activity); Federal Rules of Criminal Procedure (Rule 27. Proving an Official Record, which incorporates by reference Rule 44 of the Federal Rules of Civil Procedure), URL: https://www.law.cornell.edu/, accessed Jan. 8, 2024.

certified records generated by an electronic process or system, i.e. a record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements;

certified data copied from an electronic device, storage medium, or file, i.e. data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements. This amendment allows self-authentication by a certification of a qualified person that she checked the hash value of the proffered item and that it was identical to the original. The rule is flexible enough to allow certifications through processes other than comparison of hash value, including by other reliable means of identification provided by future technology.

In both cases, special certificates are issued. These rules also apply to documents and data obtained abroad.

In pursuance of these provisions, US requests for international legal assistance in obtaining electronic evidence are accompanied by sets of forms of certificates of authenticity that are to be completed (signed) by a foreign holder (custodian) of documents and data and that do not require special authentication (notarization or seal). These forms have the following attributes.

Certification of business records: advisement of a witness that a false attestation subjects him/her to a penalty of criminal punishment; his/her employment or association with the business from which documents are sought; business position or title by reason of which he/she is authorized and qualified to make this attestation; each of the records attached to this certificate is a record in the custody of the above-named business that: was made, at or near the time of the occurrence of the matters set forth therein, by, or from information transmitted by, a person with knowledge of those matters; was kept in the course of a regularly conducted business activity; was made by the business as a regular practice; and if not an original record, is a duplicate of the original; date and place of execution; signature.

Certificate of authenticity of domestic records pursuant to Federal Rules of Evidence 902(11) and 902(13): attestation, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct; employment by a provider

and title; he/she is qualified to authenticate the records attached to this certificate because he/she is familiar with how the records were created, managed, stored, and retrieved. He/she states that the records attached to this certificate are true duplicates of the original records in the custody of the provider; the attached records consist of (pages/CDs/megabytes); all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of the provider, and they were made by the provider as a regular practice; and such records were generated by the provider's electronic process or system that produces an accurate result, to wit: the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of the provider in a manner to ensure that they are true duplicates of the original records; and the process or system is regularly verified by the provider, and at all times pertinent to the records certified here the process and system functioned properly and normally; he/she states that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence; date and signature.

Certificate of authenticity related to data copied from an electronic device storage medium or file: attestation on penalty of criminal punishment for false statement or attestation; employment, official title; he/she certifies that the attached data is a true copy of the original data described below; he/she is qualified to copy data from an electronic device, storage medium, or file based upon his/her knowledge, training and experience; copying data from an electronic device, storage medium, or file, is done regularly, and copies of data made in this manner are kept in the ordinary course of business at the organization by which he/she is employed; the original data was an electronic device and/or storage medium, to wit: (e.g. two cell phones, a thumb drive, and a smart watch); the attached data was verified to be a true copy of the original data by a process of digital identification, to wit: the hash value(s) for the attached data was calculated and compared against the hash values calculated for the original data. This process confirmed that the hash values were identical; date and signature.

An analysis of international treaties of the Russian Federation, in particular those in force between the CIS countries, legislation

and agency regulatory legal acts[1], shows the following main forms of authentication of documents and certification of their copies, in addition to consular legalisation and apostillisation:

certification with a signature of an official of the competent authority and a seal or stamp of this authority (a coat-of-arms one or others);

notarial certification by a notary public (including of the equivalence of electronic documents and documents in paper form), and also e-notarization.

It is important to develop and improve not only the process of obtaining, evaluating and using electronic evidence itself, but also electronic channels of its transmittal and other communications with foreign counterparts, and to implement legally significant, i.e. having legal effect and validity, international electronic document management solutions. For example, during the 2020 coronavirus pandemic, for logistical and sanitary reasons, the central authorities for legal assistance and legal relations in criminal matters in many countries notified of their temporary transition to handling outgoing and incoming correspondence exclusively in paperless form, as well as of postponing the execution of many requests. With a number of countries, international correspondence turnover was suspended altogether: the Russian Post suspended the acceptance of international mail addressed to states who temporarily stopped processing incoming and outgoing international mail; courier service deliveries were impossible either.

In its Opinion No. 15 (2020) on "The role of prosecutors in emergency situations, in particular when facing a pandemic", the Consultative Council of European Prosecutors pointed out that: good

[1] See, e.g.: Agreement on interaction between the Prosecutor General's Office of the Russian Federation and the Central Bank of the Russian Federation in the exercise of the powers provided for by Federal Law of 7 May 2013 No. 79-FZ "On prohibiting particular categories of persons from opening and holding accounts (deposits), keeping cash funds and valuables in foreign banks located outside the territory of the Russian Federation, owning and (or) using foreign financial instruments" of 29 August 2019 (para. 8) ("The Central Bank of the Russian Federation takes measures to ensure the legalisation of documents received from the central bank and (or) other supervisory authority of a foreign state, whose functions include banking supervision, or a foreign financial market regulator, in one of the following forms: certification by the signature of an official of the bank (organization, competent authority) and a coat-of-arms or other official seal of the bank (organization, competent authority), apostille, notarization, consular legalisation").

practices should be identified and used to inform the development of new protocols and procedures related to the effective functioning of the prosecution offices during the COVID-19 pandemic. These should include a wider use of technology, such as online procedures to communicate cases, videoconferencing, legal recognition of electronic evidence or evidence presented by electronic means, establishment of electronic case files and evidence management systems, as well as the use of emergency regulations. Because of the difficulties with paper-based documents' transmission, affected by the pandemic, prosecution offices should consider the possibility of accepting and processing mutual legal assistance and extradition requests if communicated by electronic mail. States that have a mandatory requirement to provide legal assistance only when receiving paper-based requests, should temporarily reconsider such requirements and try to process the requests based on electronic copies until the receipt of the corresponding paper-based requests.[1]

Operating within INTERPOL are I-24/7, I-SECOM secure communications networks which are instrumental when taking urgent measures to preserve electronic evidence.

In addition, INTERPOL is developing tools for electronic extradition and mutual legal assistance procedures (e-extradition, e-MLA).

Ibero-American states have the Treaty on Electronic Transmission of International Legal Cooperation Requests between Central Authorities of 2019 in force among them, that is open for accession by third countries. It regulates recognition and execution of requests for international legal assistance transmitted in electronic form between central authorities through a secure dedicated electronic platform (Iber@), which guarantees authenticity and confidentiality of transmitted documents.

The European Union has adopted Regulation (EU) 2022/850 of the European Parliament and of the Council of 30 May 2022 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system), and amending Regulation (EU) 2018/1726.[2]

---

[1] *CCPE Opinion No. 15 (2020) of 19 Nov. 2020 CCPE (2020)2 on "The role of prosecutors in emergency situations, in particular when facing a pandemic"* (paras. 80–87; Recommendations, paras. 13–15).

[2] Individual countries point in their guidelines for foreign counterparts to the expediency of using publicly available secure file sharing platforms on the Internet designated for exchanging digital data in encrypted form, such as "Egress", for

During the elaboration of the draft UN Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, the Russian Federation proposed the inclusion of a dedicated non-self-executing article with flexible language that does not create any immediate obligations for the States Parties and would be of considerable added value, pursuant to which for the purpose of effectively ensuring the admissibility and legal validity of evidence collected in accordance with the Convention, States Parties are encouraged 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.[1]

The main principle of operation of e-MLA and other communications systems for these purposes, which in terms of technological solutions are either a secure e-mail or secure electronic platform (portal) for uploading and downloading documents, is the absence

transmittal and receipt of legal assistance documents (without additionally forwarding their paper originals in the absence of a special requirement to do this), on a par with their transmission in the PDF format by official e-mail. See, e.g.: *Request for Mutual Legal Assistance in Criminal Matters: Guidelines for Authorities outside of the United Kingdom* (London: Home Office, March 2022), p. 16.

Slovenia has made a declaration to art. 35(1) of the 2005 Warsaw Convention to the effect that it is ready to accept and execute requests received electronically or by other means of communication under the condition that the request was sent by a secure e-mail, in an encrypted form (e.g.: PGP key — Pretty Good Privacy or other equivalent commonly accepted mode of encoding) or by a protected network, as are ESW (Egmont Secure Web) and FIU-net (Reservations and Declarations for Treaty No.198 — Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No. 198). Status as of 08/01/2024).

SIRIUS EU Digital Evidence Situation Report 2022 (pp. 70 and 74) advises that if possible, law enforcement agencies should digitally sign e-mail messages sent to online service providers, for example, by adding a digital signature to an e-mail message and using means of encryption provided by Microsoft Outlook Trust Center as indicated at https://bit.ly/3Fb3mLV.

[1] 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. URL: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home, accessed Apr. 14, 2023;

of the need to additionally forward the original (hard copy) request or other document to the addressee after its scanned electronic image or original (paperless) electronic document (with an electronic signature, stamp or other means of authentication) had been transmitted to and accepted by the addressee, which is not fully compatible with the provisions of traditional international treaties on legal assistance, which require the subsequent mandatory transmittal of the original document as a precondition for the execution of the request and/or transfer of the evidence collected in pursuance of the request, to its initiator.[1]

The Russian Federation has concluded intergovernmental agreements with a number of countries on electronic information exchange for law enforcement and forensics purposes, which do not concern international legal assistance (except for providing information on the current status of execution of limited categories of MLA and police-to-police requests) and transfer of evidence. For instance, the Agreement between the Government of the Russian Federation and the Government of the Republic of Belarus on Informational Interaction and Exchange of Information in Electronic Form on Issues related to the Competence of the Internal Affairs Authorities of 13 December 2018 and its Technical Protocols provide for the exchange of information, criminal intelligence and documents, including personal data and excluding classified information, through a dedicated secure e-mail service functioning within a secure VPN network, with the use of cryptographic means of information protection and electronic signatures.

In 2021–2023, amendments to the RF CPC (arts. 222 and 474^1–474^2), as well as RF Civil Procedure Code and RF Arbitration Procedure Code were adopted, significantly expanding the use of electronic document management in proceedings as part of e-justice development.

One of the major difficulties in the way of establishing and using cross-border channels of legally valid and effective electronic document workflow is the requirement put forward by national laws, to have an interstate treaty for mutual recognition of electronic

[1] See, e.g.: European Convention on Mutual Assistance in Criminal Matters of 1959, as amended by the Second Additional Protocol of 2001 (art. 15(9)), declarations of the Russian Federation and other states parties to this clause; Treaty between the Russian Federation and the Republic of Panama on Mutual Legal Assistance in Criminal Matters of 30 Apr. 2009 (art. 4).

signatures of the states carrying out such document management in the relevant area of legal relations and the establishment of a trusted third party.[1]

As was shown, traditional international treaties on mutual legal assistance, states parties' declarations and reservations to them and their domestic legislation in most cases require the mandatory transmittal of the original request or response thereto as a prerequisite for the execution of the request and/or transfer of evidence gathered in its execution, to the requestor. Therefore, a question arises as to whether it is necessary for the states parties to conclude new treaties (additional protocols), or else to adopt declarations to the relevant articles of the existing treaties (if such are allowed by the treaty at issue) to accommodate the legally valid and admissible circulation of electronic legal assistance requests and evidence.

The answer is twofold.

A mutual legal assistance treaty and domestic legislation (e.g., arts. 454–455 RF CPC) may not put forward an express requirement to present the original paper document, but, at the same time, may mention a signature of an official and/or a seal of the competent authority as mandatory attributes of a particular document. Do these obligatory attributes imply an equivalent requirement, that is of the transmission of the original paper document, which a document in electronic form *a priori* does not comply with? The answer depends on which method of treaty interpretation should be applied — static (contemporaneous) or dynamic (evolutive).[2] In the first case, the intentions of the parties at the time of the conclusion of the legal assistance treaty, when there existed no agreement between them on the mutual recognition of electronic/digital signatures (and, possibly, stamps), would cover only a handwritten (wet, but not facsimile) signature and a seal/stamp imprint. In the second case, the intentions of the parties after the conclusion of the legal assistance treaty, as subsequent agreement between them regarding the interpretation of the treaty or the application of its provisions and

[1] *Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods* (Vienna: United Nations, 2009), 114 p.

[2] *Draft conclusions on subsequent agreements and subsequent practice in relation to the interpretation of treaties, with commentaries* (Adopted by the International Law Commission at its seventieth session, in 2018) (draft conclusion 8 and the commentary thereto).

subsequent practice in the application of the treaty which establishes their agreement regarding its interpretation, can be equally extended to electronic signatures and stamps, of course, after the signing of an (interstate) treaty on their mutual recognition in the relevant area of legal relations. The expression "in writing" (or "written record") would be interpreted in a similar way: denoting either exclusively an original document on paper (hard copy), or, on an equal footing with it, its electronic copy or image (soft copy) as well. Moreover, some treaties use this expression just as an antonym for an oral form ("orally") and thereby already actually include within its scope both originals reduced to writing, i.e. committed to paper, and their electronic versions.[1] In view of technological progress, it is justified to apply the evolutionary interpretation. In these cases, the specificities of the terminology of domestic laws and regulations will also play a significant role.[2]

Aside from the aforementioned electronic channels and platforms aimed at ensuring the authenticity and legal validity of electronic document management, there are also international communications networks of two other types or combining both of these types. The first type are secure communication channels for use by representatives of law enforcement and judicial authorities for the purpose of making inquiries and exchanging information on specific criminal cases (INTERPOL I-24/7 communications system, a specialized network of anti-corruption state bodies' focal points operating on its basis — Global Focal Point Network on Asset Recovery, INTERPOL's secure platform for intelligence exchange and coordination of law enforcement operations to combat cybercrime

---

[1] *Cf*: 2003 Merida Convention (art. 46(14)), 2005 Warsaw Convention (art. 35(1)), 1959 European Convention on Mutual Assistance in Criminal Matters as amended by the 2001 Second Additional Protocol (art. 15(9)), 2018 Dushanbe Agreement (art. 6(2 and 4)), states parties' declarations to them.

[2] E.g., the Criminal Procedure Code of Kyrgyzstan of 2021 (arts. 5, 89, 510, 522, etc.) draws a strict distinction between a written and an electronic form.

Conversely, Russian law does not put a written and an electronic form in contradistinction to each other, but, instead, distinguishes between documents on paper (signed with a handwritten signature, certified by a seal) and electronic documents (signed with a simple or advanced, (non)qualified electronic signature), including in the latter's scope also an electronic image of a paper document (art. 6 of Federal Law of 6 Apr. 2011 No. 63-FZ "On Electronic Signature"; arts. 474^1–474^2 RF CPC; Ch. XX.2 of the Fundamentals of the Legislation of the Russian Federation on Notariat of 11 Feb. 1993 No. 4462-1; art. 160 of the RF Civil Code), which is arguably the most appropriate approach.

Cybercrime Collaborative Platform — Operation, Camden Asset Recovery Inter-Agency Network (CARIN), as well as instant messaging service application Threema Work of the Global Operational Network of Anti-Corruption Law Enforcement Authorities (GlobE Network). The second type of networks are portals and other platforms with restricted access regimes, created for the exchange of experiences, educational and other information resources of a general nature that are not related to specific cases, as well as hosting professional forums and chats (Interpol's Cybercrime Knowledge Exchange workspace, European Judicial Cybercrime Network (EJCN), Global Prosecutors E-Crime Network (GPEN), SIRIUS Cross-Border Access To Electronic Evidence). These networks, as a rule, are of a thematic nature (preservation and production of electronic evidence, asset recovery, counteraction of corruption, terrorism, human trafficking, etc.).[1]

[1] See in more detail: П.А. Литвишко, Е.С. Михалева, "Состояние и перспективы электронного взаимодействия при оказании международной правовой помощи по уголовным делам и правоохранительного содействия" [The current state and prospects of electronic interaction in the provision of international legal assistance in criminal matters and law enforcement assistance], *Вестник Университета прокуратуры Российской Федерации* 2(88) (2022), pp. 130–144.

CONCLUSION

The undertaken study allows to arrive at certain conclusions and proposals relevant for science, practice and law-making activities. The main ones are as follows.

1. The novelty of the problem of collecting electronic evidence in criminal cases lies in the development of regulatory frameworks and creation of quick and effective mechanisms for obtaining it in Russia and foreign countries in the course of provision of legal assistance.

2. An analysis of the provisions of the RF CPC regarding the collection and use of electronic information carriers gives grounds for a general conclusion that the criminal procedure law recognizes the fact that digital technologies modify existing social relations, have a significant impact on the legal side of the activities of participants in criminal proceedings, and therefore their features and capabilities should be taken into account in the RF CPC and regulated in the relevant rules on evidence and proof in criminal proceedings.

3. The following concept of electronic evidence is proposed for the use in the science of criminal procedural law, in investigative, prosecutorial and court practice. Electronic evidence shall be considered an electronic medium that contains any information on the basis of which the circumstances to be proved in a particular criminal case are established, and features a significant amount of memory, ease of transfer and copying of such information from one medium to another, possibility of remote access to the content of the electronic medium and telecommunication systems, obtained in the manner prescribed by the RF CPC.

4. The collection of electronic evidence on the territory of a foreign state at the request of the Russian party depends largely on the domestic legislation of the Russian Federation. In the absence of a uniform legal regulation of this issue, this may lead to the inadmissibility of evidence due to differences in procedural rules, as well as in the regulation of data protection. Variation in domestic regulations can lead to problems with the admissibility of electronic evidence and hinder international cooperation, since the electronic data needed for an investigation would not be preserved.

5. The enshrining in the RF CPC of clear and unambiguous grounds and rules for collecting evidence through the use of modern electronic technologies will contribute to the observance of reasonable time limits for the performance of investigative and other procedural actions aimed at establishing the circumstances to be proved in a criminal case.

6. The establishment in the law of additional opportunities to ensure the rights of prosecution and defence to collect and present evidence, as well as to get familiarized with electronic evidence available in a criminal case, will secure the implementation of their procedural rights guaranteed by the RF CPC.

7. Since the collection of electronic evidence, as well as other types of evidence, is carried out by means of conducting investigative and other procedural actions, the experiences of the Republic of Kazakhstan, which regulates the procedure for handling an "electronic criminal case", can be used to improve the statutory regulation of preliminary investigation when working with electronic evidence.

To introduce the concept of an "electronic criminal case" in the Russian Federation, it is necessary to comprehensively reform the criminal process, starting, first of all, with determining the list of procedural documents that could be drawn up in electronic form in the course of criminal proceedings, and regulating the procedure for their execution. In addition, the interaction between participants in criminal proceedings should also be carried out within a single virtual environment, and the exchange of information should not take place between separate databases of law enforcement agencies, as it is currently the case. This will contribute to the development of information technologies criminal proceedings and will allow to conduct the criminal proceedings in electronic format.

Scientific publication

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.)

Production Editor
I. Krasnoslobodtseva

Proofreader
N. Pankratova

Layout
L. Tarasyuk

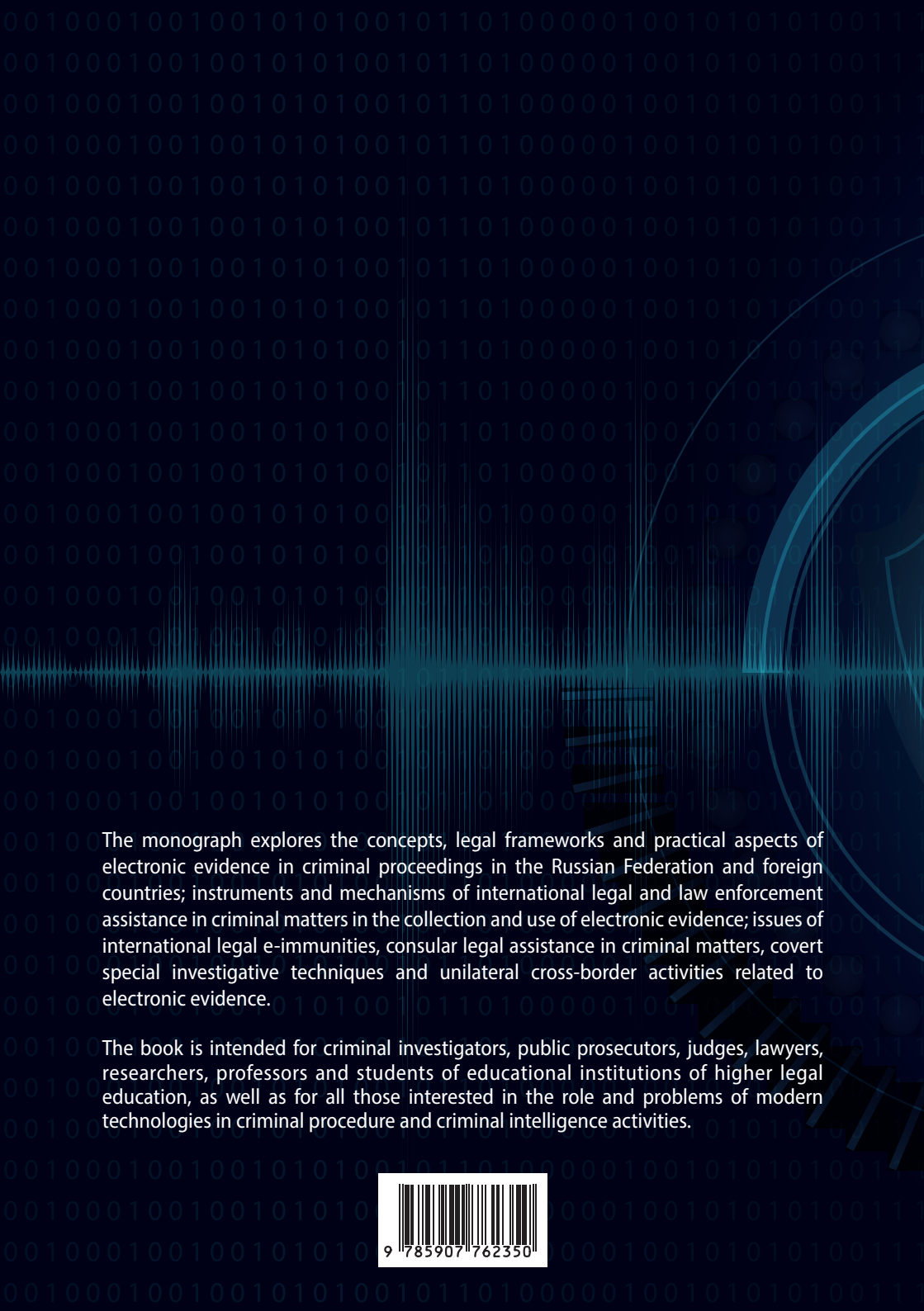
Signed to print 25.01.2024
60×90/16 format. Offset paper
Heuristica font

14 press sheets. Print run: 150 copies
Order No.

An imprint of Publishing House "Gorodets"
21 Perevedenovskiy Ln, bldg 7, ste 2
Moscow 105082
Russia

Tel.: +7 (985) 800-03-66
www.gorodets.ru
e-mail: info@gorodets.ru

Printed by JSC "T8 Publishing Technologies"
42 Volgogradskiy Ave, bldg 5, Moscow 109316, Russia



The monograph explores the concepts, legal frameworks and practical aspects of electronic evidence in criminal proceedings in the Russian Federation and foreign countries; instruments and mechanisms of international legal and law enforcement assistance in criminal matters in the collection and use of electronic evidence; issues of international legal e-immunities, consular legal assistance in criminal matters, covert special investigative techniques and unilateral cross-border activities related to electronic evidence.

The book is intended for criminal investigators, public prosecutors, judges, lawyers, researchers, professors and students of educational institutions of higher legal education, as well as for all those interested in the role and problems of modern technologies in criminal procedure and criminal intelligence activities.

9 785907 762350