Issues of Cross-Border Collection of Electronic Evidence in Criminal Matters

Pyotr Litvishko

PhD, Deputy Head of the Chief Department for International Legal Cooperation – Head of the Department for Legal and Law Enforcement Assistance, Prosecutor General's Office of the Russian Federation

Workshop on "Current State and Prospects of Developing Cooperation in Criminal Law Field Between Law Enforcement and Judicial Authorities of the Russian Federation and Competent Authorities of Foreign States, Including New Challenges and Threats Context"

RF PGO Headquarters, Moscow, 19 February 2021

Prosecutor General's Office of the Russian Federation is Russian **CA for MLA** in criminal matters, incl. outgoing and incoming requests for obtaining e-evidence.

Enduring endeavors of the RF Prosecutor General's Office on the subject of cybercrime are instrumental as it is vested with **oversight and coordination powers** with regard to the entire law enforcement system in Russia.

Multi-Agency Working Group on Counteracting Cybercrime under the aegis of the RF PGO established by the RF Prosecutor General's Order No. 352 of 6 July 2020.

MLA Requests in Cybercrime Criminal Cases (2019 – Jan. 2021)

- Incoming: 5206.

- Among them from Belarus: 4978. The figure mostly attributable to the location of major SPs and social network hosting services in Russia popular with Belarusian users.

- Outgoing: 174.

Major *corpora delicti:*

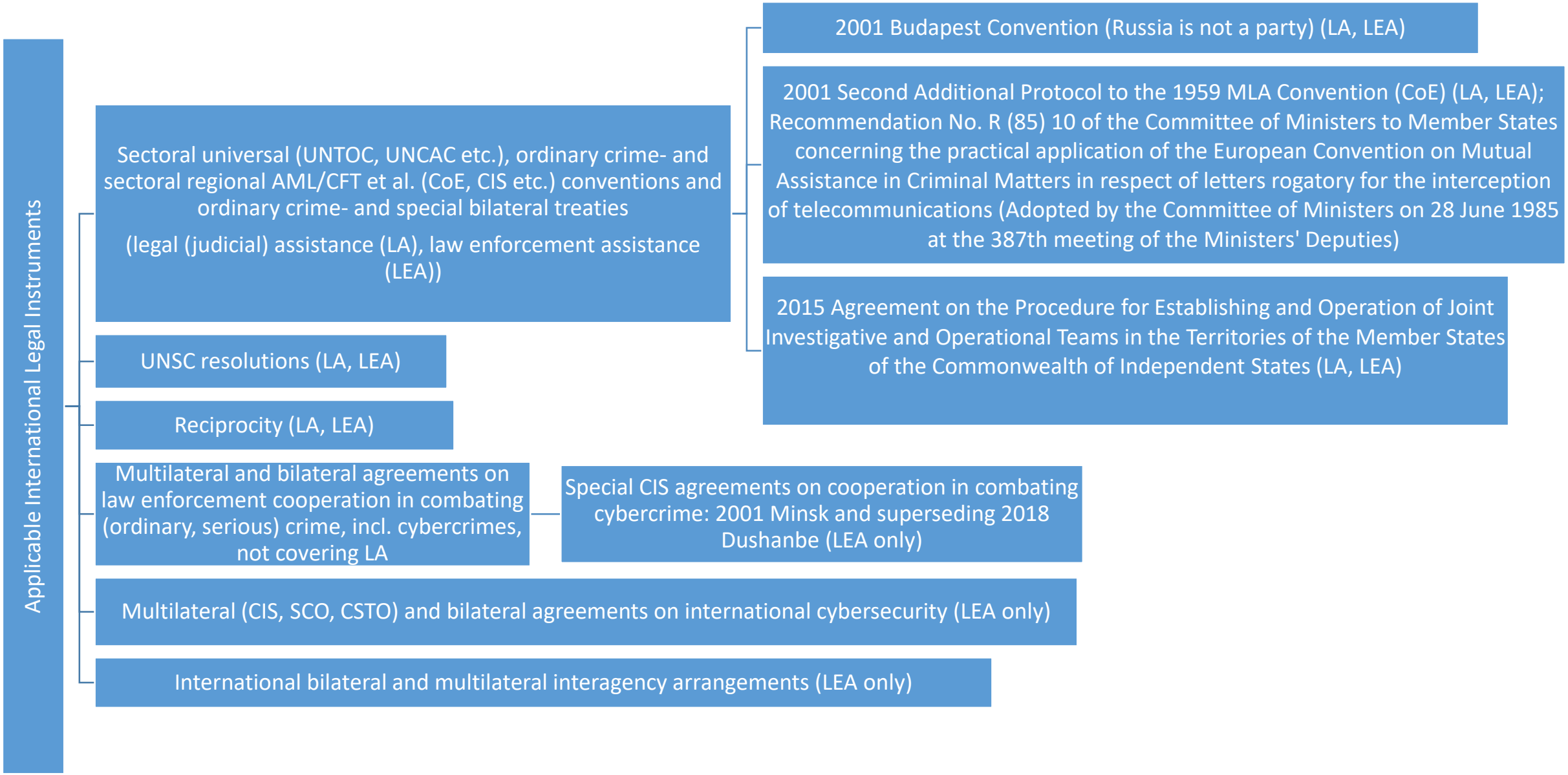
Incoming and Outgoing MLARs:

- ❖ *Cyberfraud;*
- ❖ *Cyber extortion, incl. Sextortion;*
- ❖ *Online sexual exploitation and sexual abuse of children (esp. self-generated content).*

Incoming MLARs:

- ➢ *Money/Parcel (Reshipping) Mule Scam (Droppers);*
- ➢ *Romance Scam*

✓Tech-savvy city of Yoshkar-Ola


Applicable International Legal Instruments
Sectoral universal (UNTOC, UNCAC etc.), ordinary crime- and sectoral regional AML/CFT et al. (CoE, CIS etc.) conventions and ordinary crime- and special bilateral treaties
(legal (judicial) assistance (LA), law enforcement assistance (LEA))
2001 Budapest Convention (Russia is not a party) (LA, LEA)
2001 Second Additional Protocol to the 1959 MLA Convention (CoE) (LA, LEA); 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)
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 (LA, LEA)
UNSC resolutions (LA, LEA)
Reciprocity (LA, LEA)
Multilateral and bilateral agreements on law enforcement cooperation in combating (ordinary, serious) crime, incl. cybercrimes, not covering LA
Special CIS agreements on cooperation in combating cybercrime: 2001 Minsk and superseding 2018 Dushanbe (LEA only)
Multilateral (CIS, SCO, CSTO) and bilateral agreements on international cybersecurity (LEA only)
International bilateral and multilateral interagency arrangements (LEA only)

A Race Against Time:

Ephemeral and transient nature of e-evidence

Clipart

Flip Side of the new instruments (the Budapest Convention, Draft Second Additional Protocol thereto, U.S. CLOUD Act-based int'l agreements, Draft European Production and Preservation Orders for electronic evidence in criminal matters) and mechanisms is

Dismantling the Architecture of Interstate Interaction.

Followed By: A Decentralized World Without Intermediaries.

P2P, Blockchain, 5G…

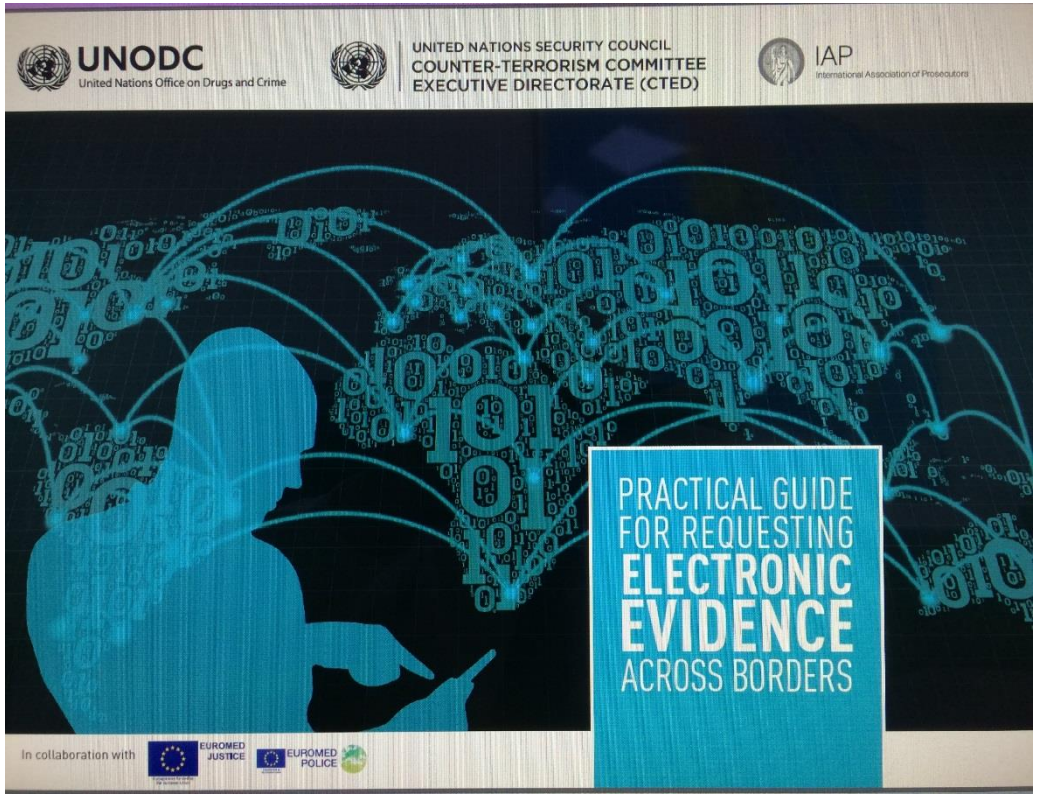
State sovereignty and int'l norms and principles that flow from sovereignty apply to State conduct of ICT-related activities and to their **jurisdiction over ICT infrastructure within their territory** (e.g., UNGA resolution 73/27 of 5 Dec. 2018 "Developments in the field of information and telecommunications in the context of international security").

Therefore, the exercise of enforcement jurisdiction in cyberspace comes with the need for observance of int'l law principles therein, such as respecting *territorial sovereignty of another State and non-intervention in its domestic affairs, otherwise the respective actions can be assessed as constituting a (criminal) offence or even an internationally wrongful act.*

Practical guide for requesting electronic evidence across borders. Vienna: United Nations, 2019:

Disseminated by the RF PGO among Russian central judicial and law enforcement authorities, as well as their research and educational institutions; getting **positive feedback.**

Russia's pp. of the Guide: 197, 200.



State

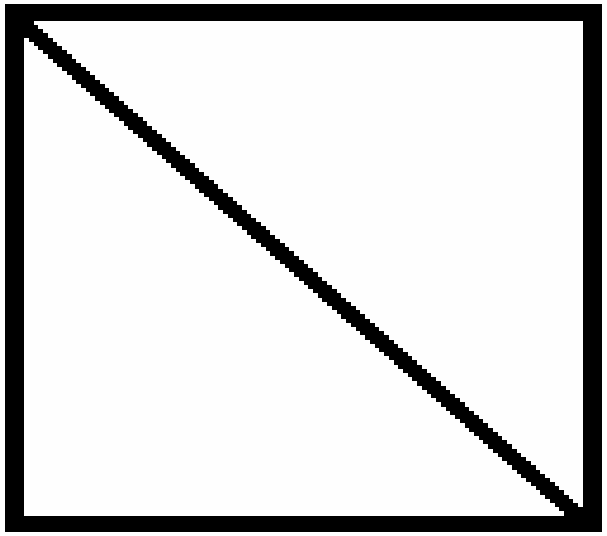
‘~~Man~~-in-the-middle’ approach

Getty Images/iStockphoto

No direct access to Russian SPs or their subsidiaries by foreign authorities;
Diagonal (asymmetric) cooperation for incoming requests excluded.

State A

State B



SP in State B

Offset by 24/7 interagency networks

Clipart

On the other hand, outgoing requests (as opposed to compulsory orders) by Russian judicial and LEAs to foreign SPs and their subsidiaries offering their services in Russia for voluntary data preservation or production of BSI relating to such services are possible, where the ***SP's Guidelines*** *(platforms, portals)* ***for LEAs***, officially published and therefore explicitly or implicitly approved or acquiesced to ***by the State of the SP,*** allow that (U.S., Canada).

Predicaments to address in prospective instruments:

- The State of the SP is deprived of exercising its right to **assess** the requested data and **refuse** or **impose conditions** on its production, inter alia, on the grounds of eventual prejudice to its sovereignty, security or other essential interests, political persecution or other human rights abuses by the requesting State.
- Unclarity as to safeguards and **legal remedies** available to the data subject and/or SP from the actions of a foreign agent, difficulties in enforcing them, e.g. for violating **privacy and personal data protection,** obtaining bulk BSI of uninvolved subscribers.
- Risk of violating **e-immunities** of diplomats and other persons enjoying them in the State of the SP and their premises.

- Risk of breaching the **privileged status** of data enjoyed under law of the State of the SP.
- Misunderstanding and mistakes due to the **different languages** used by a foreign agent and SP.
- **Confidentiality** of requests to SPs.

Default **notification** by U.S. SPs of customers whose 'voluntary' data are requested by a foreign LEA.

- **Volatility** of SP's unilateral policy, **unpredictability** of disclosure due to SP's discretion powers.

While U.S. SPs may produce subscriber, traffic and even content data directly and voluntarily to foreign LEAs upon request under U.S. law (18 U.S. Code § 2702 – Voluntary disclosure of customer communications or records), this is not the case for European SPs that do not disclose directly to foreign LEAs, even in emergency situations.

- SPs face significant challenges in verifying **security, authentication, and certification** of foreign requests, and vice versa foreign authorities do in respect of foreign SPs' files.
- SPs are not in a position to properly **evaluate themselves potential prejudice** to their States' sovereignty, security or other essential interests, **risks** of political persecution or other human rights abuses by the requesting State, as well as whether the **sought data** is **relevant, necessary and proportionate**, or standard of proof is met**.**
- SP's reaction to a foreign preservation request would in most cases already reveal information as to the availability or absence of electronic evidence (confirmation or denial).

Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order […] a service provider offering its services in the territory of the Party *[i.e. the SP or data's (servers') location, incl. roaming, or 'loss of location' are irrelevant – P.L.]* to submit ***subscriber*** information ***relating to such services*** in that service provider's possession or control.

(Art. 18(1)(b) of the Budapest Convention.) – Targeting Test for asserting jurisdiction.

"Agreement to this Guidance Note does not entail consent to the extraterritorial service or enforcement of a domestic production order issued by another State".

(T-CY Guidance Note #10 Production orders for subscriber information (Art. 18 Budapest Convention), para. 3.3.)

Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Paris: FATF, 2019, pp. 22–23, 29, paras. 78–79, 81, 113; Guidance for a Risk-Based Approach to Virtual Currencies. Paris: FATF, 2015, p. 18, para. 71.

A Party may, without the authorisation of another Party […] access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the ***lawful and voluntary*** consent of the person who has the ***lawful*** authority to disclose the data to the Party through that computer system.

(Art. 32(b) of the Budapest Convention.) – Extended Search etc.

- Wide discretion in verifying and validating ‘lawfulness and voluntariness’.
- **‘Lawful’ – whose law and by whom** is assessed? Is law of the State where the data subject/controller, SP, terminal equipment or other essential touchpoint is located, taken into account?

“SPs are **unlikely** to be able to consent validly and voluntarily to disclosure of their users’ data under Art. 32. Normally, SPs 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.”

(T-CY Guidance Note # 3 Transborder access to data (Article 32), para. 3.6.)

<u>But:</u>

- SPs are normally considered to be Data Controllers.

- Guidance notes to the Budapest Convention are not binding on the State parties.

- Provisions of the **Draft Second Additional Protocol** to the Budapest Convention relating to Direct disclosure of subscriber information **in many aspects boil down to interstate cooperation**, given their multiple reservations, notification and consultation regimes.

Art. 32(b) of the Budapest Convention – Trans-border access to stored computer data not publicly available.

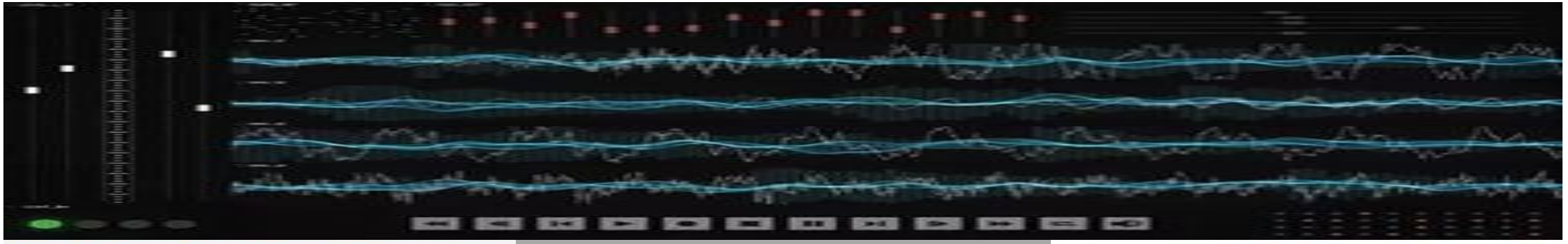
“It should be taken into account that many Parties would object – and some even consider it a criminal offence *[e.g. Switzerland – P.L.]* – if a person who is physically in their territory is directly approached by foreign law enforcement authorities who seek his or her cooperation”. (T-CY Guidance Note # 3 Transborder access to data (Article 32), para. 3.8.). See also: Practical guide for requesting electronic evidence across borders. Vienna: United Nations, 2019, pp. 6–7, 9, 54–55, 188, 197, 199.

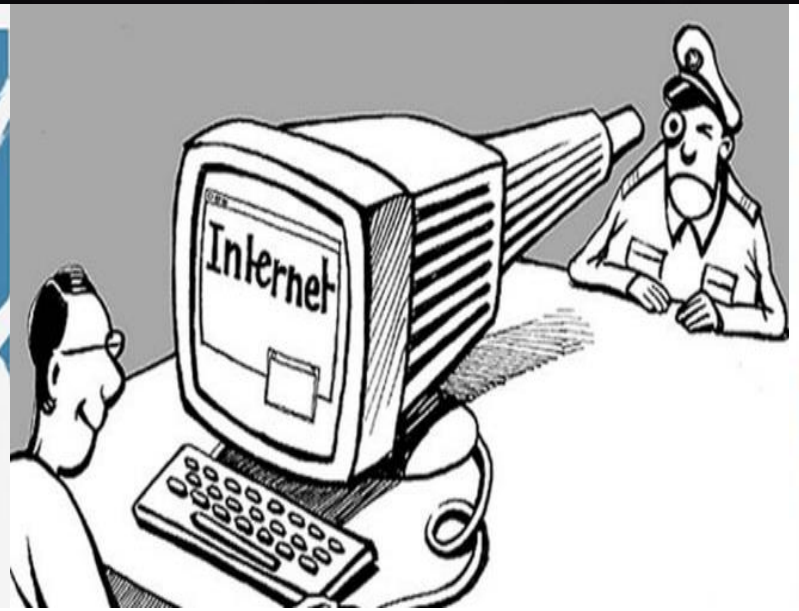
Foreign production orders to the U.S. SPs under int'l agreements concluded pursuant to the U.S. CLOUD Act may not target U.S. persons.

State parties to the Budapest Convention continue voicing their **concern about direct unilateral transborder access** to data that are not in the public domain**.**

(2019 Report of the Secretary-General 'Countering the use of information and communications technologies for criminal purposes' (A/74/130).)

Due to the above problems – **inadmissibility** of the gathered e-evidence.





Categories of data available to **domestic and foreign** judicial and law enforcement authorities under 'Big Brother' laws, **channels to access** them, domestic **legal requirements** and **retention periods** (possible under MLATs and other treaties, UNSC resolutions or based on reciprocity) for the purposes of criminal proceedings and criminal intelligence operations:

Type of Data/Access	Channel	Judicial Authorization and Other Legal Requirements	Retention Period
Data preservation	Law enforcement (police-to-police) request, Interpol's I-24/7, or MLAR		
BSI, incl. both static and **dynamic** IP addresses	Law enforcement request, Interpol's I-24/7, or MLAR	Court order not required. Cf re dynamic IP addresses: ECHR case of **Benedik v. Slovenia** (2018).	Telecom service providers: **three years;** Persons that organize circulation of information in Internet: **one year.**
Stored traffic data, including cell tower dumps	MLAR	Court order (domestic and, where appropriate, one of the requesting state attached to MLAR)	Telecom service providers: **three years;** Persons that organize circulation of information in Internet: **one year.**
Stored content data (text, voice, images, sound, video and other communications)	MLAR	Court order (domestic and, where applicable, of the requesting state attached to MLAR)	**Six months**
Real-time collection (interception) of traffic or content data in transit	MLAR	Court order (domestic and, where applicable, of the requesting state attached to MLAR); available for crimes of average gravity, grave and especially grave crimes.	

Type of Data/Access	Channel	Judicial Authorization and Other Legal Requirements	Retention Period
Any type of data	Info/Intel exchange from a parallel domestic investigation, incl. spontaneous transfer	Investigator‘s discretionary decision	Not applicable
Any type of data	JITs	Domestic investigator‘s discretionary decision	Not applicable
Any **direct approaches** to Russian SPs, incl. preservation, emergency and voluntary disclosure, disclosure by user’s consent requests, are not permitted; European Production and Preservation Orders for electronic evidence in criminal matters - ?	Law enforcement request, Interpol’s I-24/7, or MLAR, depending on the type of data requested	As indicated above, depending on the type of data	As above

Under Russian law, organizers of information circulation in Internet are also obligated to provide the state security agency with **decryption information** for electronic messages.

‘De-anonymization’ of users of instant messaging apps.

Photo Illustration by Lyne Lucien/The Daily Beast

Coercive Blocking Measures

(also available on the basis of eligible foreign requests and communications):

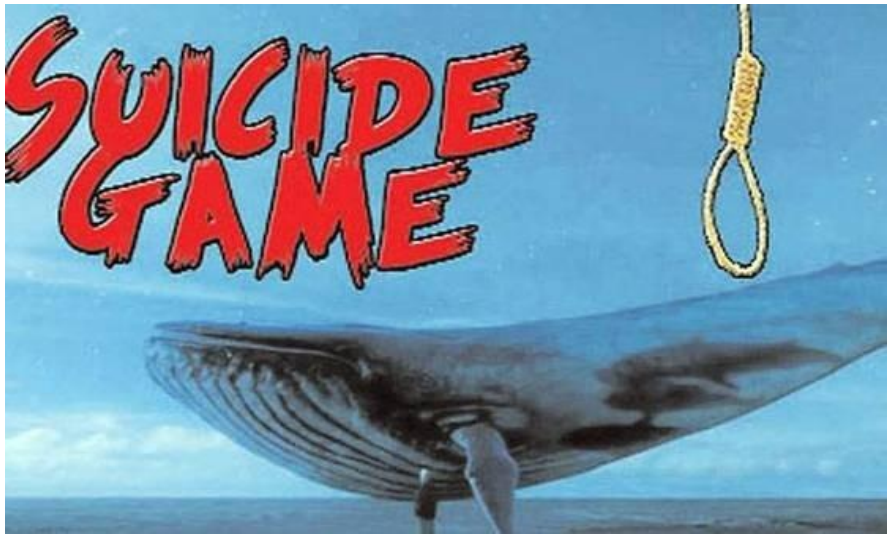
Extrajudicial: Blocking access to websites with terrorist, extremist, dangerously fake and some other illegal content pursuant to an extrajudicial request of a public prosecutor by the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor).

These decisions on access restrictions can be challenged in a court of law.

Judicial: Lodging of civil claims in court by public prosecutors to have illicit content removed from websites.

Case Study on

BSI Emergency Disclosure Requests



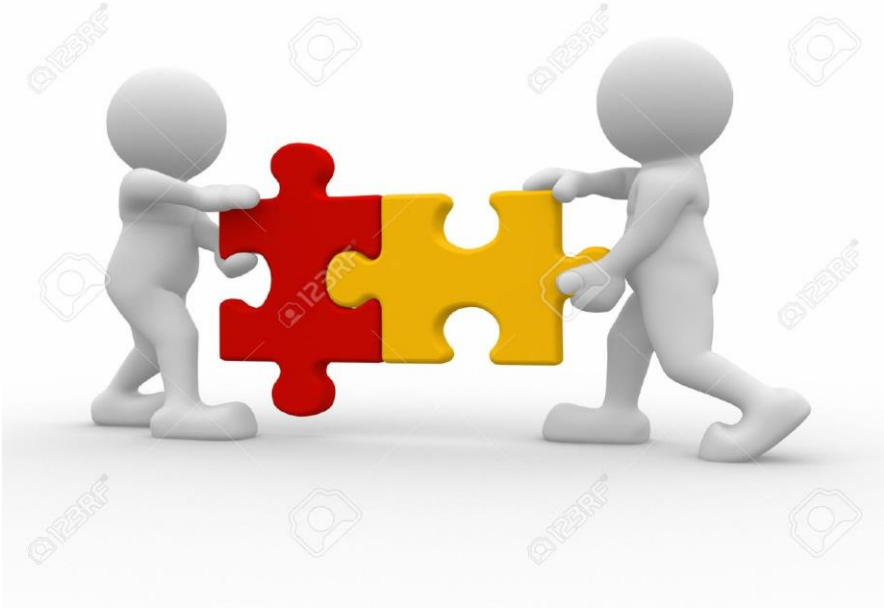
Russian social media (Odnoklassniki, Vkontakte etc.), also popular outside Russia, in Russian-speaking countries and among expat communities.

Identifying foreign users of the Blue Whale Challenge and other child suicide games hosted on those platforms 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 accounts. RF law enforcement regularly tipped off their foreign counterparts regarding such communications.

In 2017, the dedicated articles were introduced into the RF Criminal Code criminalizing incitement to suicide in cyberspace.

Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters of 2001 entered into force for the Russian Federation on **Jan. 1, 2020.**

Envisages **direct** communications between judicial and law enforcement authorities, incl. their local units in Russia, also with regard to procuring e-evidence that does not require a court warrant (see the chart above) or coercive measures, otherwise via the RF PGO.



- Jurisdictional and int'l cooperation rules concerning ICT service providers are mostly applicable to state authorities' communications with providers engaged in exchange services between decentralized virtual currencies and fiat currencies and custodian wallet providers.
- Telecommunications Secrecy + "Quasi-Bank Secrecy" – Judicial Warrant.
- Seizure or other restraint or confiscation of **virtual assets** in Russia are only possible after their prior conversion into fiat currency or other property. (Cf.: Belarus, art. 132 CPC (Seizure of Property – incl. cryptocurrency), introduced Jan. 2021.)
- **Federal Law** No. 259-FZ of 31 July 2020 **"On Digital Financial Assets, Digital Currency** and Amending Particular Legislative Acts of the Russian Federation", effective from Jan., 2021, does not yet regulate criminal procedure nor transnational issues.

Challenges:

Ephemeral and transient nature of e-evidence;

- E2EE;
- P2Ps (file-sharing websites, voice-over-IP services etc.);
- The Cloud;
- VPNs with zero-log policy;
- Proxies, anonymizers (Tor etc.);
- NAT (Network Address Translation);
- Darknet;
- WHOIS restrictions;
- 5G broadband cellular networks (decentralized configuration etc.);
- *Coronavirus pandemic:* paperless procedures only and use of protected telecom networks; need for urgent development of e-extradition, e-MLA and e-transfer tools; Treaty on the Electronic Transmission of International Legal Cooperation Requests between Central Authorities (Adopted in January 2018 by the Conference of Ministers of Justice of Ibero-American States (COMJIB)).

Where the offence is computer fraud, often the efforts boil down just to identifying so-called mules.

In cases of dynamic IP addresses, when there are no available data on the precise time of Internet access, up to a second, the time zone and visited resources' IP addresses, or application of NAT-technology, the efforts result in dragnets scooping up personal data (BSI) of dozens of uninvolved subscribers (data-mining), which is similar to prohibited fishing expedition in legal assistance.

Such across-the-board, indiscriminate and excessive personal data cannot be shared with foreign counterparts for filtering, matching and other purposes pursuant to their police-to-police requests or MLARs in most cases.

If the user of the information system identified in the process of executing a foreign MLA request happens to be unwitting and uninvolved (e.g. where his or her PC or device had been infected with malware, or in cases of identity theft), their personal data are deleted or blacked out in their interview and other records prior to the transfer to the requesting authority abroad. This approach is consistent with the principles of proportionality and necessity and DP requirements. Recommendations for subsequent transfer of criminal proceedings to the country where the culprit is present.

Covert use of geolocation (GPS/GLONASS tracking devices, direction finders etc.) on vehicles of suspects and other objects crossing the border of another state should qualify as a special investigative technique under art. 20 of the Palermo Convention, namely an electronic surveillance (and an operational search measure ‘surveillance’ under RF Federal Law “On Operational Search Activity”), represents a particular type of international cooperation and requires an advance approval by the state into whose territory a 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 where this was not initially anticipated and was established during the monitoring.

In addition to that, some countries’ laws regard this type of actions as procedural (judicial) ones, hence requiring the int’l mutual legal assistance process rather than law enforcement cooperation for their conduct.

- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 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) –

Unilateral transfers of personal data directly to recipients established in third countries.

Draft UN Convention on Cooperation in Combating Cybercrime (Annex to the letter dated 11 Oct. 2017 from the Permanent Representative of the Russian Federation to the UN addressed to the Secretary-General).

(A/C.3/72/12)

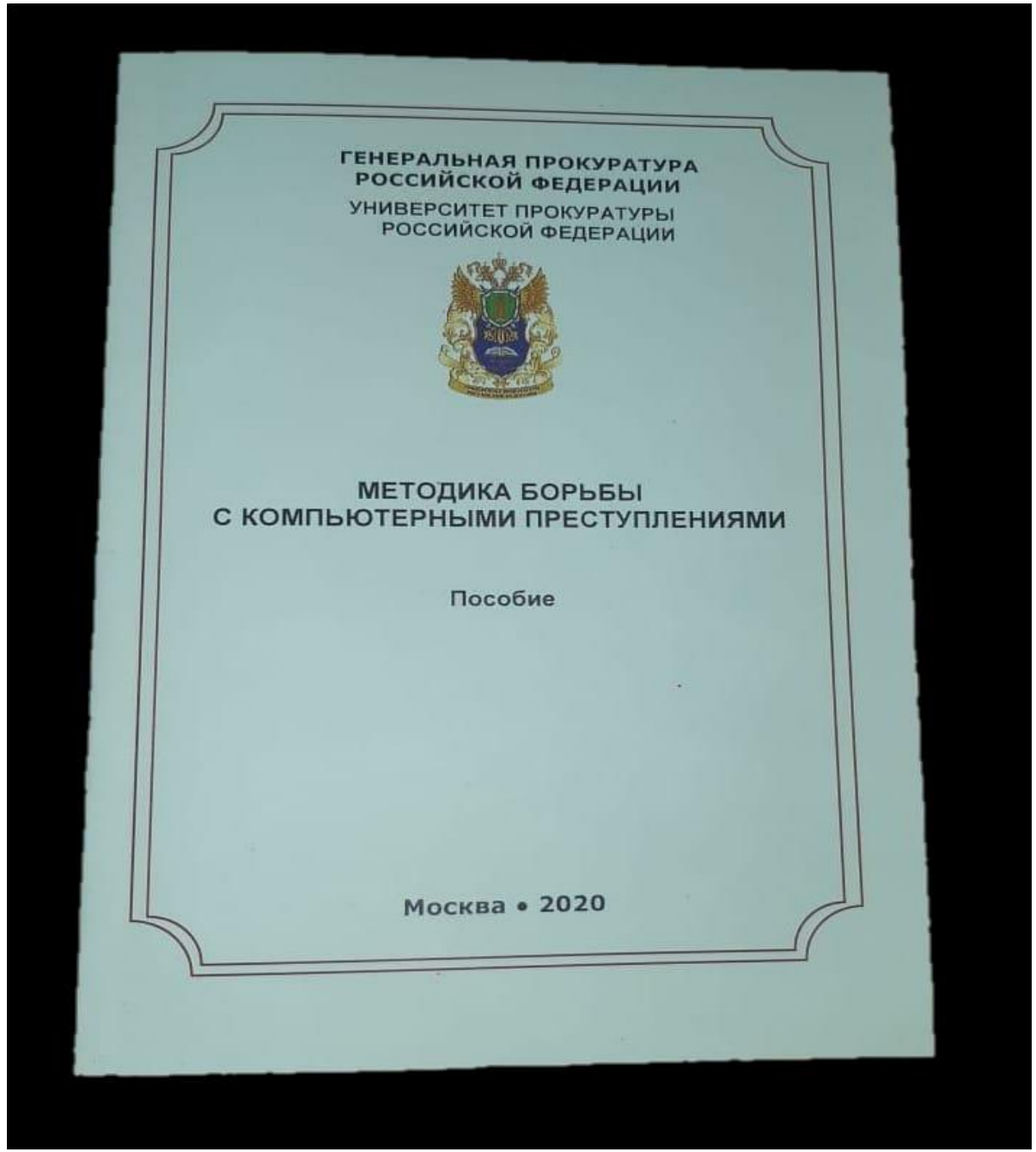
Up-to-date, Technology-neutral.

UNGA resolution 74/247 of 27 Dec. 2019 “Countering the use of information and communications technologies for criminal purposes”: established an open-ended ad hoc intergovernmental committee of experts to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes.

2021 Rollout.

- Methodology of Combating Cybercrimes (Moscow: RF Prosecutor General's Office, University of RF Public Prosecutor’s Office, 2020).

- Forthcoming in 2021: Collection of Electronic Evidence in Criminal Matters in the Territory of Russia and Foreign Countries: Experiences and Problems.


ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА
РОССИЙСКОЙ ФЕДЕРАЦИИ
УНИВЕРСИТЕТ ПРОКУРАТУРЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ
МЕТОДИКА БОРЬБЫ
С КОМПЬЮТЕРНЫМИ ПРЕСТУПЛЕНИЯМИ
Пособие
Москва • 2020

Thank you for your attention.