Federal law dated 01.05.2019 № 90-FZ "On amendments to the Federal law "On communications" and the Federal law "On information, information technologies and information protection"

Summary and comments on particular provisions:

Amendments to the Federal Law "On Communications" 2003:

- **Definition of the traffic exchange point. "**A set of hardware and software and/or communication facilities, with the use of which the owner or other owner provides the ability to connect and pass unchanged traffic between communication networks, if the proprietor/owner has a unique identifier set of communication and other technical means in the Internet."

- The **federal executive authority** in the field of communications **determines the order of operators' interaction**, as well as establishes requirements for the functioning of communication network management systems **in the event of threats to the stability**, security and integrity **of the Russian Internet and public communication network operation**.
  According to the text the law refers to two different networks. According to article 13 of the law, public communication network also connects to the public communication networks of foreign countries that implies the definition of Internet. However, in this article they are mentioned as two distinct networks.

- Operators, who are **also ISPs, are required to ensure the installation in their networks of technical means for countering threats (hereinafter, technical means) to the stability**, security and integrity of Internet operation on the territory of the Russian Federation. The Government of the Russian Federation defines the order of installation, operation and modernization of technical means in operators' networks.
  These technical means or "black boxes" are provided by RKN for free only for telecom operators. Their purpose implies DPI technology inside (for detail see the post).

- **ISPs are no longer obliged to limit access** to the information distributed on the Internet according to the Federal law 149-FZ *(RKN blacklist*) if they use the technical means provided by RKN. During normal operations these technical means will just filter prohibited Internet resources. But during an external threat, these black boxes are supposed to **provide the basis for centralized management of the public communication network by RKN**.

- **An ISP cannot be held liable** and cannot be subject to response measures **for violations of the license agreement to provide communication services if the violations are caused by failures in communication networks as a result of the functioning of technical means** of countering threats.
  Nobody is now responsible for any network crashes, operators can only send and inquiry to RKN and ask whether its equipment was the cause.

- A **new Chapter 7.1 "Ensuring stable, secure and integral functioning of the Internet in the territory of the Russian Federation**" is added to the law:

  1) telecom operators and owners and/or proprietors of: (1)technical communication networks (used for operations of transport/energy and other infrastructural objects, not connected to the public communication network) (2)traffic exchange points, (3)communication lines crossing the state border and (4) autonomous system numbers (ASN) are obliged to ensure a stable operation of Internet in Russia.

  The subjects of Runet operation are listed.

  Regarding the inclusion of owners of technical networks into the scope of the law: this provision was met with high criticism by Gasprom and RZD (two state-owned corporations responsible for oil and gas extraction and distribution and national railway transportation network, respectively). This provision threatens the operation of technical networks of enterprises and can lead to emergency situations in their work. Integration of external technical means of monitoring and control and SORM, as well as the empowerment of RKN to determine routing in technical networks, will violate the principle of their isolation and challenge their security.

  2) **RKN will coordinate all subjects** of public communication network **in a centralized way.**

  3) In order to acquire practical skills to ensure the stability of Runet, **all subjects are required to participate in the exercises**, the provision on which, including the goals and objectives of their implementation, as well as the list of participants, is established by the Government of the Russian Federation.

  4) RKN approves the order of handling the information according with the **new paragraph 56.2**:

  - **Records of communication lines crossing the border** of the Russian Federation
  - MoC in agreement with FSB establishes requirements for the operation of traffic exchange points.
  - Owners of traffic exchange points must notify RKN on their start of the work
  - the Government defines the order of how RKN will maintain **the registry of traffic exchange points**
  - the owners of traffic exchange points must not connect the networks, whose owners do not have installed SORM[1]. RKN should consider how it will be monitored.
  - Owners of ASN when connecting to other ASN owners and telecom operators should **use traffic exchange points only from the registry**
  - **ASN owners while resolving network addresses in their respective domain names must use the national domain name system** – *this provision will come in force on January 1, 2021*
  - ASN owners should provide to RKN information about:
    - their autonomous system number and network addresses belonging to the autonomous system;
    - interaction with operators, owners of technical communication networks, other persons who have autonomous system number/s.
    - about places of connection to the communication lines crossing the border of the Russian Federation;

[1] SORM is the technical specification for lawful interception interfaces of telecommunications and telephone networks operating in Russia. The current form of the specification enables the targeted surveillance of both telephone and Internet communications

• about places of installation of their means of communication connected to the communication lines located outside the territory of the Russian Federation;
• on telecommunication routes;
• on their technical and software means of communication
• on the infrastructure of their communication network.

- A **new article 65.1 "Management of communication networks in the event of threats to the stability and security of the Runet**" is added to the law:

1) In order to identify threats RKN monitors the operation of public networks

2) In the event of threats to the Runet and public networks, RKN provides centralized management of the public communications network and the Internet on the territory of the Russian Federation
Again, the law refers to two different kinds of networks.

3) RKN provides operators with technical means to counter threats free of charge. RKN also establishes specifications for technical means, as well as requirements for networks when using these means.
These technical means are DPI systems, see more details in this post. ASN owners won't be provided with them, as operators, though they must execute the law too.

4) During an emergency caused by threats to Runet stability, **centralized management is carried out by RKN through these means of countering threats OR through the transmission of mandatory instructions to operators, who do not have them.**
In what form the instructions will be transmitted? Will RKN send mails with new routing policies? Also, the law doesn't define what the case of emergency is. For the Head of RKN, Mr. Zharov, blocking is already a case of emergency: "According to the bill, the government will determine the list of threats when the centralized management of the communication network will be switched on: these are emergency situations <...> Blocking is an emergency. It is obvious that in cases of non-execution of the legislation by the organizers of information dissemination (OID) the state has a tool to force it to execute the law. If the OID helps terrorists to communicate, it is an emergency, so we must take all measures to ensure that they do not use these messengers."

5) **The Government of the Russian Federation approves the procedure for centralized management of the public communication network, which defines:**

- **types of threats to the Runet and public network**
  the law prescribes the Government to describe in what cases it should be applied
- regulations for identifying these threats and measures to address them, including how RKN will execute it
- requirements for interaction between RKN and operators in case the latter have claims to the functioning of the technical means for countering threats
- methods for determining the technical feasibility of the execution of instructions transmitted within the framework of centralized management of the public communication network;
- cases in which the operator has the right not to direct traffic through the technical means to counter threats

6) **Routing of telecommunication messages** (sender and receiver must be in the Russian Federation) **in the case of centralized management is carried out according to the rules established by RKN**
Why this provision specifies the location of sender and receiver and what to do with that other directions of traffic?

7) Communications equipment through which the centralized management of public communication network is performed, shall be located in the territory of the Russian Federation.
8) To implement paragraphs 1,2,3,4 and 7 the **Center for monitoring and control of public communication networks** under the Radio Frequency Service (sub agency of RKN) is established. RKN will determine its powers and scope of work.

Amendments to the Federal Law "On Information" 2006:

- The **organizers of information dissemination** (OID: social networks, messengers, forums are examples) **that own ASN also must comply** with the requirements for traffic routing.

- Regulation of **national cryptographic protection**: state bodies and agencies when interacting in electronic form (among themselves and with organizations and citizens) are obliged to ensure the possibility of such interaction in accordance with the rules and principles established by the national standards of the Russian Federation in the field of cryptographic protection of information defined by FZ-162, 2016.
  This provision come into force on 1 January 2021

- A **new article 14.2. "Ensuring stable and secure use of domain names in the Russian Federation**" added to the law:
  - **A national domain name system is established,** which is a set of interrelated software and hardware tools designed to store and obtain information about network addresses and domain names.
  - **The regulation on the national domain name system**, the procedure for its creation, including the formation of the information contained therein, as well as the rules for its use, including the conditions and procedure for providing access to information, **is determined by RKN**.
  - **RKN defines the list of domain name groups that make up the Russian national domain zone**
  - **Coordination of activity for formation of the Russian national domain zone is performed by the non-profit organization which will be founded by the Russian Federation (represented by RKN)** and which is an accredited owner of databases of that zone in the international organizations responsible for distribution of network addresses and domain names.
  - *The law neglects the existing Coordination center for TLD .RU (it is a non-profit administrator of national top-level domains and in 2015 MoC joined its founders). It's unclear whether RKN will create a brand-new organization or will reorganize the Coordination Center.*

- **Operators are not obliged to block resources from the RKN blacklist if they installed the technical means to counter threats**
  This provision is inserted to harmonize the legislation and avoid mutually excluding articles in both laws.

- Article 15.5. "Procedure for restricting access to information processed in violation of the legislation of the Russian Federation in the field of personal data" get a special emphasis that

operators are obliged to immediately restrict access to the information resource, including the website on the Internet, **where the information is processed in violation of the Russian legislation on personal data protection.**

It looks like this article was amended with future purpose to block Twitter and Facebook because they still do not comply with the law on personal data protection and do everything possible to delay the negotiations and avoid transferring their servers to Russia.