TO THE COMMITTEE OF MINISTERS OF THE COUNCIL OF EUROPE

On the execution of the European Court of Human Rights judgment on the case "Roman ZAKHAROV against the Russian Federation"

(application no. 47143/06)

Non-governmental report of

Agora International Human Rights Group

and

Public Association of Alternative Telecom Operators

under Rule 9(2) of the Rules of the Committee of Ministers for the supervision of the execution of judgments and of the terms of friendly settlements

17 December 2018

I. INTRODUCTION

1. The present Report has been prepared by Agora International Human Rights Group and Public Association of Alternative Telecom Operators according to the Rule 9(2) of the Rules of the Committee of Ministers for the supervision of the execution of judgments and of the terms of friendly settlements.

2. *Agora International Human Rights Group* is an association of more than 50 lawyers working on landmark human rights cases mainly in the territory of the Russian Federation. One of the priorities of Agora is the protection of freedom of expression and the right to privacy and anonymity both online and offline.

3. *Public Association of Alternative Telecom Operators (PAATO)* – is a non-registered public association, which unites managers of small telecom operator companies (mainly from St. Petersburg). PAATO exists since 2014 and actively participates in legislative activities (i.e. work with expert groups under the Ministry of Communications, the Government of the Russian Federation, Federal Anti-monopoly Service). PAATO also represents telecom operators in anti-monopoly cases.

4. This Report is devoted to the execution by the Russian Federation of the Judgement of the European Court of Human Rights (hereinafter – 'the Court') on the case of *Roman Zakharov v. Russia*, application No. 47143/06 (hereinafter referred to as 'the Judgement').

5. In its Judgement after analysing the existing legal provisions and the practice of their implementation, the Court concluded that **the Russian legal provisions governing interceptions of communications do not provide for adequate and effective guarantees against arbitrariness and the risk of abuse** which is inherent in any system of secret surveillance, and which is particularly high in a system where the secret services and the police have direct access, by technical means, to all mobile telephone communications[1].

1 *Roman Zakharov v. Russia*, application No. 47143/06, 4 December 2015, §302

6. On 3 August 2018 the Government of the Russian Federation (hereinafter – 'the Government') submitted to the Committee of the Ministers an Updated Action Plan on the execution of the Judgment, in which the Government proposed a number of measures designed to eliminate and prevent the violations of the Convention found by the Court.

7. In the present report we would like to provide an assessment of part of the proposals made by the Government as well as to inform the Committee of the Ministers about a significant deterioration of the situation with the right to privacy in Russia following the adoption of new legislative provisions which let law enforcement agencies and special services to obtain access to all electronic communications.

II. THE COURT'S ASSESSMENT

8. In its assessment of the circumstances of the case the Court noted that where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on interception of telephone conversations, **especially as the technology available for use is continually becoming more sophisticated**. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures[2].

9. In formulating the relevant criteria, the Court indicated in particular that the requirement to show an interception authorisation to the communications service provider before obtaining access to a person's communications is one of the important safeguards against abuse by the law-enforcement authorities, ensuring that proper authorisation is obtained in all cases of interception[3].

2 Ibid. §229
3 Ibid. §269

10. In particular the Court highlighted the following deficiencies of the Russian legal norms which regulate the interception of telephone communications.

In regard of scope of application of secret surveillance measures

11. Russian law allows secret interception of communications in respect of a very wide range of criminal offences, including for example, pickpocketing (§ 244).

12. Interceptions may be ordered not only in respect of a suspect or an accused, but also in respect of a person who may have information about an offence or may have other information relevant to the criminal case. Relevant terms are not defined in the legislation or law enforcement practice (§ 245).

13. The Operational-Search Activities Act (hereinafter – 'the OSAA') also provides that telephone or other communications may be intercepted following the receipt of information about events or activities endangering Russia's national, military, economic or ecological security. What events or activities can be considered as posing a threat to such types of security is not defined anywhere in the Russian legislation, which gives the Russian authorities almost unlimited freedom of discretion (§§ 246-247).

14. Interceptions in the framework of criminal proceedings are attended by more safeguards than interceptions conducted outside such a framework, in particular in connection with "events or activities endangering national, military, economic or ecological security" (§ 251).

In regard of authorization procedures

15. Judicial scrutiny is limited in scope. Materials containing information about undercover agents or police informers or about the organization and tactics of operational-search measures may not be submitted to the judge and are therefore excluded from the court's scope of review (§ 261).

16. The judges are not instructed, either by the Code of Criminal Procedure or by the OSAA, to verify the existence of a "reasonable

suspicion" against the person concerned or to apply the "necessity" and "proportionality" test" (§ 262).

In regard of the authorities' access to communications

17. In Russia the lawenforcement authorities are not required under domestic law to show the judicial authorization to the communications service provider before obtaining access to a person's communications, except in connection with the monitoring of communications-related data under the Code of Criminal Procedure (§ 269).

18. The manner in which the system of secret surveillance operates in Russia gives the security services and the police technical means to circumvent the authorization procedure and to intercept any communications without obtaining prior judicial authorization (§ 270).

In regard of supervision of the interception

19. A court which has granted authorization for interception has no competence to supervise its implementation. It is not informed of the results of the interceptions and has no power to review whether the requirements of the decision granting authorization were complied with. Nor do Russian courts in general have competence to carry out the overall supervision of interceptions. Judicial supervision is limited to the initial authorization stage (§ 274).

In regard of notification of interception of communications and available remedies

20. Persons whose communications have been intercepted are not notified of this fact at any point or under any circumstances. It follows that, unless criminal proceedings have been opened against the interception subject and the intercepted data have been used in evidence, or unless there has been a leak, the person concerned is unlikely ever to find out if his or her communications have been intercepted (§ 289).

21. A person who has somehow learned that his or her communications have been intercepted may request information about the corresponding data but the access to information is conditional on the person's ability to prove that his or her communications were intercepted. Furthermore, the interception subject is not entitled to obtain access to documents relating to interception of his or her communications; he or she is at best entitled to receive "information" about the collected data (§ 280).

III. MEASURES, PROPOSED BY THE GOVERNMENT

22. The Updated Action Plan submitted by the Government on 3 August 2018 states the following.

23. In accordance with the plan of the legislative drafting activities of the Government for 2018, the Ministry of Justice of the Russian Federation in cooperation with other competent authorities in October 2018 should develop the draft federal laws "On Introduction of Amendments to Article 9 of the OSAA" (regarding the improvement of guarantees of human rights and freedoms when authorizing the conduct of and appeal against of operational search activities)" and "On Introduction of Amendments to the Code of Administrative Procedure of the Russian Federation (regarding the procedure for judicial review of materials on the limitation of the constitutional rights of citizens when conducting the operational-search activities)". Relevant draft laws should be submitted to the State Duma in December 2018 (Para. 1 of the Updated Action Plan).

24. After the events examined by the Court In the said case there was the Judgement of the Constitutional Court of the Russian Federation no. 12-P of 9 June 2011 delivered which explicitly states that the bodies conducting operational search activities when requesting authorization to carry out secret operational search activities shall provide the court with appropriate justification and materials indicating specific factual circumstances confirming reasonableness of the allegation as well as a number of the Constitutional Court's decisions (in particular, No. 114-O of 22 January 2014, No. 86-O of 28 January 2016 and No. 568-O of 28 March 2017).

25. From 2014 to 2017, 79 persons were convicted under Article 138 § 2 of the Criminal Code of the Russian Federation (violation of privacy of correspondence, telephone conversations, postal, telegraphic or other communications of citizens committed by a person abusing his powers).

26. From 2016 to first half of 2018 as a result of 630 000 inspections carried out by prosecutors 295 operative and search activities were discontinued.

IV. ASSESSMENT OF THE MEASURES PROPOSED BY THE GOVERNMENT

27. The efforts of the Government for execution of the Judgment are essentially reduced to an intention to amend Article 9 of the OSAA, and to include in the Code of Administrative Procedure certain provisions on the judicial review of materials which concern restrictions of the constitutional rights of citizens in the context of operational-search activities.

28. Meanwhile, in accordance with Decree the Government No. 851 of 25 August 2012 "Concerning the disclosure by federal executive institutions of information about draft legislation and about the results of public consultations", the executive institution entrusted with drafting the new legislation is required to publish on the Official web portal for publication by federal executive institutions of information about draft legislation and about the results of public consultations (i) a notification that new legislation is being drafted and (ii) **the draft legislation for a pubic consultation process, the period of which cannot be less than 15 days.** The publication of information about the drafting of federal laws is mandatory.

29. Until the present time the drafts of the federal laws mentioned in the Government's Updated Action Plan (Para. 1) have not been published on the official web-portal, the detailed information about the drafting of these documents is not available publicly, the draft itself was not presented for the public discussion.

30. The Judgement of the Constitutional Court of the Russian Federation No.12-P of 9 June 2011, mentioned in the Updated Action Plan, which underscores the necessity to refer to certain factual circumstances which confirm the reasonableness of the allegation that a person committed a crime, while considering the authorisation of operational-search activities, applies only to such activities in respect of judges. This is set out clearly in Paragraph 1 of the said Judgement of the Constitutional Court: 'the matters examined by the Constitutional Court of the Russian Federation in this case are the interrelated provisions of Article 16 § 7 of the *Status of Judges in the Russian Federation Act* and Article 9 § 1 of the *Operational-Search Activities Act*'.

31. In regard of the decisions of the Constitutional Court of the Russian Federation, mentioned in the Updated Action Plan, notable is the absence of evidence that these decisions are followed by the national judges which authorise operational-search activities and investigative actions involving restrictions of the constitutional rights of citizens.

32. It should be noted in this respect that in the case of Roman Zakharov, the Court observed that the domestic law does not explicitly require the courts of general jurisdiction to follow the Constitutional Court's opinion as to how a legislative provision should be interpreted if such opinion has been expressed in a decision rather than a judgment (see § 263). This situation has not changed since the above-cited Judgement was delivered.

33. Furthermore, the Government observes that 79 individuals have been prosecuted under Article 138 § 2 of the Criminal Code of the Russian Federation in the period 2014 - 2017 (Para. 4 of the Updated Action Plan).

34. The Government however does not indicate how many state officials, in particular police and Federal Security Service officers, have been prosecuted.

35. Meanwhile when assessing these statistics, it should be borne in mind that Article 138 § 2 of the Criminal Code applies to for example

employees of telecom operators who – in breach of their official duties and typically seeking to obtain some personal benefit – unlawfully access telephone conversations of subscribers and details of the calls made.

36. Thus, and in view of the limited number of criminal cases and sentences for breach of the secrecy of telephone conversations (less than 20 per year), the information provided by the Government does not confirm that the above-cited provision of the criminal law is capable to effectively deter abuse in this area.

37. It should also be noted that the Updated Action Plan does not include measures designed to address the fundamental flaws identified by the Court, in particular the broad spectrum of criminal offenses in respect of which interception can be applied, the possibility to intercept an unidentified group of individuals, and the existence of technical capabilities to bypass the authorisation procedure and intercept any communications without ex-ante approval by the court, and the absence of effective *ex post factum* judicial control.

38. The law on the OSA still provides for the possibility of interception of messages and information in some cases without a court decision, notifying its post factum with notifying the court at 24 hours. That is, even within the law, the court, refusing to wiretap, can no longer change and prevent the violation of the rights of citizens by “law enforcement” bodies that occurred. Moreover, in a number of cases, for example, in the electoral process, the legislation of the Russian Federation provides for the adoption of emergency court decisions (Art. 78 p. 4 of the Federal Law of 12 June 2002 N 67-FZ "On basic guarantees of electoral rights and the right to participate in referendum of citizens Of the Russian Federation "), that is, in this case it is possible to prescribe an emergency court decision in the law, and not to allow wiretapping with subsequent notification.

V. THE CURRENT SITUATION

39. Since 2015 the Russian authorities have applied a whole range of steps aimed at restricting to a significant extent the right to privacy and secrecy of correspondence. Thereby the authorities have essentially extended the system for permanent control on telephone conversations to all online communications.

40. The most serious step was the Federal Law of 6 July 2016 No. 374-FZ "On amending the Counter-Terrorism Act and other legislative acts of the Russian Federation by introducing additional measures to combat terrorism and guarantee public security" (hereinafter - 'Law No. 374', 'Yarovaya Law').

41. Law No. 374 is in itself a package of amendments, in particular to the *Information, Information Technology and Data Protection Act*, and to the *Communications Act*, which under the pretext of combating terrorism concern various regulatory aspects of the telecommunication sector, including those related to privacy and anonymity.

Inclusion of computer information in the scope of the OSAA

42. Law No. 374 also includes the obtaining of computer information to the list of operational-search activities in Article 6 of the OSAA (144-FZ of 12 August 1995).

43. The new amendments do not provide additional guarantees for the respect of human right during the conduct of operational-search activities.

Imposition on telecom operators of obligations to collect and store subscribers' metadata and messages

44. On 16 April 2014 the Ministry of Communications of the Russian Federation approved Order No. 83 which establishes binding requirements to the equipment which is used for the switching and routing of data packages and forms part of public communication

networks or dedicated networks, including software programs which enable the performance of certain actions in the context of operational-search activities (hereinafter - 'OSA equipment'). The Order requires each telecom operator to maintain at least the following capabilities:

- Connection of at least 16 OSA equipment control terminals, prohibition to connect any other control interfaces;

- Storage in a ring buffer for at least 12 hours of all incoming data packages as well as processing of these packages by the following criteria: static and dynamic IP address, user account names, email addresses (including mail.ru, yandex.ru, rambler.ru, gmail.com, yahoo.com), identifiers of the telephone line and the telephone numbers of call recipient and of the caller, identifier of the messaging service, IMEI, IMSI, MAC addresses of the various devices, data about the location of subscribers' terminals etc.

45. On July 2014, the Rules for the provision of telematic services were supplemented by para. 22.1 (Government Decree of 31 July 2014 No. 758), according to which all telecom operators are required to supplement contracts with subscribers-legal entities, as well as individual entrepreneurs, to provide the operator with the lists of persons using the terminal equipment with an indication of their place of residence, and passport details. The Decree does not indicate the safety requirements of this data as well as the procedure of its processing.

46. According to the revised version of Article 64 § 1 of the Communications Act, introduced by Law No. 374, all telecom operators are required to store in the territory of the Russian Federation: (1) information concerning the reception, transmittal, delivery and/or processing of voice, text, images, audio, video or other messages of communication services users, for a period of three years as from the winding up of these activities; (2) text messages of communication services users, voice, images, audio, video or other

messages of communication services users for a period of up to six months from the end of each reception, transmittal, delivery and/or processing activity.

47. Communication operators have the statutory obligation to facilitate OSA in accordance with the established rules and procedures.

48. On 30 December 2017, amendments were introduced in Decree of the Government of the Russian Federation No. 538 of 27 August 2017 by which the Government approved *Rules for the collaboration of telecom operators with authorised State bodies which perform operational-search activities*. The amendments require the telecom operator to store for period of three years in the territory of the Russian Federation information contained in the operator's databases relating to its subscribers and the services provided to these subscribers, including information concerning the reception, transmittal, delivery and/or processing of voice, text, images, audio, video or other messages, and make this information available to the Federal Security Service and to the Ministry of Interior by providing remote access to their databases on a 24/7 basis.

49. By Decree No. 445 of 12 April 2018, the Government of the Russian Federation approved *Rules for the storage by telecom operators of text messages of communication services users, and voice, text, images, audio, video or other messages of communication services users*.

50. The Rules require each telecom operator to store in the territory of the Russian Federation text messages of communication services users, voice, text, images, audio, video or other messages of the users of the services provided by that operator ('e-messages') on data storage equipment which belongs to that operator.

51. In order to comply with these obligations, as from 1 July 2018 the operators must provide for storage of e-messages in zero volume and as from 1 October 2018 – full storage of e-messages on data storage equipment with a capacity equal to the amount of e-messages sent and received by the users of the services provided by that operator for

the 30 days preceding the date on which the data storage equipment is put into service. The capacity of the data storage equipment must be increased by 15 % per annum in the course of five years from the date on which the data storage equipment is put into service.

Imposition on Internet Service Providers (ISPs) of obligations to store metadata, and store and decrypt users' messages

52. Law No. 374 introduced also amendments in Article 10.1 § 3 in the *Information, Information Technology and Data Protection Act* according to which the ISPs included in a special list of Information Dissemination Organizers are required to store in the territory of the Russian Federation: (1) information concerning the reception, transmittal, delivery and/or processing of voice, written text, images, audio, video or other messages of communication services users as well as information about these users, for a period of one year as from the winding up of these activities; (2) text messages of communication services users, and voice, images, audio, video or other messages of communication services users for a period of up to six months from the end of each reception, transmittal, delivery and/or processing activity.

53. Information Dissemination Organizers have the statutory obligation to make this information available to the authorities which perform operational-search activities or tasks related to the security of the Russian Federation in the cases set out in federal laws.

54. Moreover, ISPs that use encryption of traffic are required to disclose to the Federal Security Service all keys used for the encryption of the messages sent, received or processed with these keys (Article 10.1 § 4.1 of the *Information, Information Technology and Data Protection Act*). Withal, the national legislation currently in force does not make it mandatory for special services to obtain a court order before they can access such information.

55. Currently, the list of companies covered by the law consists of 152 services, including such popular platforms as Vkontakte,

Odnoklassniki, Mail.ru, Yandex, Threema, Badoo, as well as media, local community and professional forums, etc. According to the Russian telecommunication authorities, the issue of including Apple, Twitter, Facebook and WhatsApp, Google, Microsoft, Viber and other international companies representing billions of users around the world into the list is being considered.

56. During April and May 2017, a number of messaging services has been blocked in Russia for refusing to register as an organizer of information dissemination and provide the Russian authorities with access to data and messages, including Zello, Imo, Line, Blackberry Messenger and Vchat.

57. On 28 June 2017, Telegram instant messenger service owned by Telegram Messenger LLP was forcibly included in the Register of Information Dissemination Organizers by decision of Roskomnadzor (Federal Service for Supervision of Communications, Information Technology and Mass-Media). That, according to the position of the Russian authorities, means the duty of the service administrator to store a variety of metadata and all users' correspondence on the territory of Russia and provide them to intelligence services upon request.

58. On 14 July 2017, the FSB requested Telegram Messenger LLP to provide the keys needed to decrypt the correspondence on 6 phone numbers. There were no court orders provided to the Company. The decryption keys must be sent via regular e-mail to the public address of the Internet reception of the FSB (fsb@fsb.ru). The company refused to comply with this request.

59. On 16 October 2017, the magistrate in Moscow issued a decree recognizing the Telegram Messenger LLP guilty of committing an administrative offense provided for in para. 2.1 of Article 13.31 of the Code of Administrative Offenses of the Russian Federation (failure to provide information needed for decoding messages) and fined 800,000 rubles (approximately 11 000 euro).

60. On 13 April 2018, Tagansky District Court of Moscow ordered the Roskomnadzor, as well as third parties, to block users' access to the Telegram service in the territory of the Russian Federation[4].

61. In its Appellate Ruling of 9 August 2018 in Case No. APL18-298, the Supreme Court of the Russian Federation held, in respect of Article 9 of the *Information, Information Technology and Data Protection Act*, that **the information required for the decryption of messages is not does not form part of the message secrecy, which the Constitution and the federal laws protect.** Moreover, Information Dissemination Organizers (i.e. ISP owners) are not regarded as entities which control and supervise the lawfulness of operational-search activities.

62. Other amendments to the Personal Data Act and the Information, Information Technology and Data Protection Act apply since 1 September 2015 which is the date of entry into force of Federal Las No. 242-FZ of 21 July 2014 amending certain legislative acts of the Russian Federation by establishing more detailed rules for the processing of personal data in information and communication networks. Law No. 242-FZ requires personal data controllers (including ISPs) to use only databases located within the territory of the Russian Federation for processing the personal data of citizens of the Russian Federation.

63. In 2016, by order of Moscow City Court the social platform LinkedIn was blocked in the territory of the Russian Federation due to their refusal to localize the personal data of their users on Russian servers.

Data Protection

64. Government Decree No. 445 makes it incumbent on operators to protect their data storage equipment and the data stored in it from unauthorised access in accordance with requirements established by the Russian Ministry of Connectivity and Mass Communications.

---

4 Telegram Messenger LLP has appealed to the European Court (application No.13232/18).

65. These requirements are set out in Order No. 83 of the Ministry of Communications (see paragraph 43 above) and essentially mean that (i) the OSA equipment must be installed in separate premises with locking devices which exclude unauthorised access to the equipment and (ii) alternative control interfaces cannot be used.

66. In accordance with paragraph 4 of the aforementioned rules, technical means of data storage are part of and are identified as communications equipment, including software, which ensures the implementation of specified actions during operational search activities.

67. Technically and organizationally, all data storage facilities created under Law No. 374 ('Yarovaya Law') should provide for permanent, unrestricted access by intelligence services through technical means to all user data.

68. Thus, these repositories are a further evolution of the SORM system, which was the subject of consideration by the European Court in the case of *Roman Zakharov v. Russia.*

69. Currently, there is a monopolization of the SORM market for telecom operators. This strongly jeopardizes personal data: a company monopolizing the market, using the undocumented capabilities of its systems, will get access to almost any information stored in the databases of telecom operators and transmitted by users over the communication networks. The current certification system in Russia itself is often a very formal approach to certification, and also considering that the issuance of certification requirements for SORM systems is delayed, perhaps deliberately, do not guarantee the security of transmitted data. When carrying out certification, it is likely that attention will be paid to ensuring access of law enforcement officers to data through the SORM system, but the search and control of undocumented capabilities of the equipment will most likely not even be carried out.

The lack of efficient judicial control

70. According to the statistics of the Judicial Department of the Supreme Court of the Russian Federation, in 2015-2017 the domestic courts granted more than 1.8 million authorisations for the restriction of the constitutional rights of citizens as regards secrecy of correspondence, telephone conversations, postal, telegraphic and other messages transmitted in electronic and postal systems, in the framework of operational-search activities. Thus, on an averaged basis the courts granted 99.32 % of the requests for such authorisations.

71. In the same period, in the framework of investigative activities more than 0.8 million authorisations were granted for control and for recording of telephone and other conversations as well as for obtaining of information on the connections between subscribers, meaning that on average 97.32 % of the requests were granted.

72. Thus, the ex-ante judicial control on the activities of operational-search agencies is illusory and unable to guarantee that citizens' rights are respected when messages and conversations are being intercepted.

73. The OSAA still provides for the possibility of interception of messages and conversations in some cases without a court decision, with *post factum* notification within next 24 hours. That is, even within the law, the court, refusing to wiretap, can no longer change and prevent the violation of the citizens' rights that occurred. Moreover, in a number of cases, for example, in the electoral process, the legislation of the Russian Federation provides for the adoption of emergency court decisions (i.e. Article 78 of the Federal Law 'On basic guarantees of electoral rights and the right to participate in referendum of citizens Of the Russian Federation'), that is, in this case it is possible to prescribe an emergency court decision in the law, and not to allow wiretapping with subsequent notification.

The economic consequences

74. According to various estimates, the telecom operators' costs for implementing the measures set out in the Law No. 374 would range from several billion[5] to 10 trillion[6] Roubles per year.

75. The inevitable consequences include higher prices of communication services, bankruptcies of smaller communication services providers, and further monopolization of the communication market. Following the Law No.374 is extremely difficult for most telecom companies, its requirements to purchase and install storage equipment is fatal for smaller ones. It encourages local companies either to sell business or to violate the legislation.

76. Starting in the Spring of 2018, telecom operators began to raise tariffs, explaining that by the need to compensate for the cost of implementation of the 'Yarovaya Law'. The price increase by an average of 5-10%.

VI. CONCLUSION AND RECOMMENDATIONS

77. The foregoing discussion leads to a conclusion that in the period following the delivery of Court's Judgment in the case *Roman Zakharov v. Russia* the situation with respect to human with regarding the interception of communications in the context of law enforcement activities in Russia has indeed deteriorated significantly.

78. The steps undertaken by the Russian authorities, including the adoption of laws which require telecom operators to keep enormous amounts of user data and messages, withal in the absence of efficient mechanisms for control, for complaining against unlawful actions and for reparation of damages inflicted through disclosure of personal information, will inevitably lead to wide-scale violations of the citizens' rights to privacy and anonymity, to economic hardships for smaller private companies, to restriction of competition, and to a further monopolization of the market for telecommunication services.

5 https://www.rbc.ru/business/05/03/2018/5a9ce5939a794745f656c133

6 https://meduza.io/news/2017/04/10/rspp-otsenil-zatraty-na-zakon-yarovoy-v-10-trillionov-rubley-on-razgonit-inflyatsiyu

79. The measures which the legislation provides for ensuring the security of the data stored and for preventing *mala fide* access to these data by state and non-state entities are clearly insufficient.

80. Legal acts establishing all new mechanisms for mass surveillance of citizens are in fact adopted in an extraordinary manner - without a wide public discussion and consideration of the position of stakeholders, including representatives of civil society and the Internet industry.

81. We consider it important to note that in recent years the United Nations and its specialized institutions have formulated detailed standards for the respect of digital rights, including the right to freedom of expression, as well as privacy and anonymity, far ahead of the Council of Europe.

82. Thus the Resolution adopted by the UN General Assembly on 18 December 2013 "The Right to Privacy in the Digital Age" directly calls upon all States to To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law (A/Res/68/167).

83. According to the recent Report of the UN High Commissioner for Human Rights, secret mass surveillance and communications interception, collecting, storing and analyzing the data of all users relating to a broad range of means of communication (for example, emails, telephone and video calls, text messages and websites visited) is not permissible under international human rights law, as an individualized necessity and proportionality analysis would not be possible in the context of such measures (para. 17, A/HRC/39/29).

84. In the Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression David Kaye it is noted that

85. **Legislative proposals for the revision or adoption of restrictions on individual security online should be subject to public debate and adopted according to regular, public, informed and transparent legislative process. States must promote effective participation of a wide variety of civil society actors and minority groups in such debate and processes and avoid adopting such legislation under accelerated legislative procedures** (para. 58, A/HRC/29/32).

86. Establishing new mechanisms for storing, processing and intercepting all types of Internet traffic in the framework of SORM, 'Yarovaya Law' and the accompanying regulatory legal acts undertaken by the Russian authorities in recent years represents a further development of the system of arbitrary and uncontrolled mass surveillance and as such contradicts both international human rights law as a whole and the European Court Judgement on the case of *Roman Zakharov v. Russia*.

87. **We hereby request the Committee of Ministers to:**

a) Draw the Government's attention to the need for repealing *Federal Law No. 374-FZ amending the Counter-Terrorism Act and other legislative acts of the Russian Federation by introducing additional measures to combat terrorism and guarantee public security*, especially as regards the amendments to the *Communications Act* and to the *Information, Information Technology and Data Protection Act*;

b) Draw the Government's attention to the need for strengthening the responsibility of telecom operators and ISPs as regards the respect of human rights and in particular to the need for introducing a statutory obligation for publishing detailed reports showing the number of applications received from state bodies and private individuals concerning the restriction of access to content, and on the number of requests by state agencies for the disclosure of user data (transparency reports);

c) Draw the Government's attention to the need for modification of the interception technologies which enable the agencies which carry

out operational-search activities obtain permanent and direct access to all telephone conversations and web-based communications of all users.

d) Recommend that the Government strengthens the proposed amendments to the operational-search legislation by making it obligatory to present in advance to telecom services providers and to ISPs an authorisation from a competent court for access to user messages and metadata.

e) Formulate a requirement for mandatory prior public and transparent discussion of all adopted legal norms restricting digital rights of citizens, based on a multi-stakeholder approach involving representatives of civil society and the Internet industry.

f) Continue the supervision of the execution by the Russian Federation of the Judgement on the case of *Roman Zakharov v. Russia*.

On behalf of Agora *Pavel Chikov*

On behalf of PAATO *Ramil Akhmetgaliyev*