1999-03

Kafka's World: FSB and 'Law'

Pustintsev, Boris

Boston University Center for the Study of Conflict, Ideology, and Policy

PERSPECTIVE

Volume 9, No 4 (March-April 1999)

Kafka's World: FSB and 'Law

By BORIS PUSTINTSEV

Citizens' Watch (1)

During decades in which the Soviet regime failed to impose legal limitations on the security organs, these services became accustomed to relying on "administrative measures," even when such measures were contradictory to the law. Today's Federal Security Service (FSB) spares no effort to perpetuate those practices. The infamous case of the ecologist Aleksandr Nikitin rests on FSB attempts to support the espionage charge by using defense ministry regulations that were never published for the general public and therefore cannot be used as a criterion for guilt or innocence. Although the General Prosecutor's Office required the FSB to remove all references to unpublished acts from the indictment in April 1998, the case against Nikitin remains open.

The security services are trying to extend a similar approach to the communication networks that provide electronic mail and Internet access to the public. Officially the FSB insists that its surveillance of electronic communication aims at curbing crime and corruption; however, we have reason to suppose that the main targets are in fact highly placed federal and regional officials, political and social activists, and journalists. At a time when kompromat (2) wars define Russian politics, the surveillance of private correspondence of public figures can serve as a very useful tool in the hands of some not so savory characters. Journalists constitute a target because e-mail can help to identify the source of information which certain political figures or the FSB would wish to suppress.

The Russian Federation law "On Operational-Investigative Activity" requires all Internet providers to supply the FSB with technical data from their mail servers and to install a

System of Operational-Investigative Activities (SORM) on their mail servers. These actions provide the FSB with the technical capability to inspect client correspondence on that server, but the mechanism is only to become operational when a court-ordered warrant is presented to authorize the surveillance of a particular client's e-mail. The FSB, however, chafes under such restrictions: Imagine having to obtain a warrant! Referring to unpublished decrees of the Ministry of Communication [No. 226 (June 24, 1992), No. 252 (November 11, 1994) and No. 25 (February 18, 1997)], and in the absence of a court document, the security service has demanded access to information about subscribers and the correspondence of certain persons. Thus, the FSB is using secret regulations to compel the service providers to break the law.

Law-abiding martyrs

The communication ministry decrees punish recalcitrant providers by denying them a new license or revoking their existing license. In theory, the provider can disobey FSB dictates and, if subjected to extralegal or administrative reprisals, he can go to court, possibly winning the case. In practice, everyone knows that martyr-providers are scarce: Those who seek justice in the courts would go broke long before their cases even reached the trial. The prevalent lack of faith in the judicial system, particularly in its ability to enforce the law against the powerful security agencies, virtually guarantees the FSB freedom from client-instigated litigation.

It is not known how many providers across Russia systematically break federal law and infringe on the constitutional rights of their subscribers by allowing the FSB to observe all electronic correspondence without court sanctions. Intimidated owners and network administrators do not publicize such activity. One extraordinary person who refused to break the law for the sake of the FSB finally emerged in November 1998: Oleg Syrov, the manager of the Bayard-Slavia Communications (BSK) joint-stock company in Volgograd, declared that he would install a SORM only if the FSB demands did not violate constitutional norms and federal laws. In response, the head of the regional FSB, General Viktor Kolesnikov, contacted the agency charged with monitoring the service

providers (Gossvyaz'nadzor) of the Volgograd oblast' and "strongly recommended" that it revoke BSK's license.

The monitoring agency conducted a review and found that there were no grounds to revoke the operating license in this case. The agency sent the FSB a letter repeating that BSK stands ready to cooperate if the use of SORM conforms to the law. Thereafter BSK was subjected to an avalanche of FSB-inspired inspections -- a tax audit, visits from the police division for the fight against corruption, etc. Suddenly, in February, Syrov resigned. The FSB continues to look for a reason to deprive the BSK of its license, thereby intimidating other potential "rebels." The BSK owner, Yuri Skorokhodov, told me in March that he will not give in to blackmail and stands ready to take this case to court. He asked Citizens' Watch to help him appeal to the European Court in the event that the Russian court finds for the FSB.

The service provider has ample grounds for a legal case. Article 23, Paragraph 2 of the Russian Constitution states, "Each person has the right to privacy of correspondence, telephone conversations, and postal, telegraph, and other communications. Limitation of this right is permitted only on the basis of a judicial decision." The relevant legislation, "On the FSB, " "On Communication, " and "On Operational-Investigative Activity" elucidate this principle: To monitor private correspondence, the FSB must obtain a warrant.

Our legal system retains certain atavistic traits dating from the Soviet period when legal norms were arbitrarily applied. Many Russian laws suffer from an identical defect, supporting a very broad range of interpretation. To press its case, the FSB has been able to exploit a seeming contradiction in the law. On the one hand, the court decision comes into effect only after certain procedural conditions have been met. In the given case, the procedural conditions are minimal; for instance, a service provider cannot appeal a warrant authorizing the surveillance of a client's e-mail. However, the minimal procedural requirement must be fulfilled -- the FSB must show the warrant. If the warrant is not presented to the service provider, he can hardly be expected to abide by

it. The FSB and the court can do with the document whatever they like, but they cannot keep it hidden and apply it to third parties.

On the other hand, Article 12 of the law "On Operational-Investigative Activity" states, "The judicial decision authorizing operational-investigative measures and the materials that constituted the basis for the court finding are stored only in the organs that carry out the operational-investigative activities. " From our point of view, the FSB's right to store the document does not obviate its obligation to present a warrant to the service provider. Otherwise, the service provider has to take the existence of the warrant on faith, and the absurdity of the situation approaches Kafka's novel The Trial.

Procurator's interpretation

Of course, the FSB and the procuracy see matters in an entirely different light. Aleksei Simonov, the president of Glasnost Defense Fund, the very well-regarded Moscow human rights group, recently lodged a complaint with the Volgograd Procuracy. On February 22, 1999 the Volgograd procurator, Viktor Glagolkin, responded that the presentation of a warrant "contradicts" Article 12 cited above. That response suggests that the provider should simply take FSB agents at their word. Moreover, the provider does not even need to know which client is being observed. If the procurator's interpretation becomes the norm, the FSB would be given limitless access to the providers' data -- an outcome that negates a series of constitutional guarantees.

Without getting bogged down in too many legal technicalities, it should be mentioned that a provider who allows the FSB to conduct surveillance without seeing a warrant violates Article 138, Paragraph 2, and Article 286 of the Criminal Code. The FSB agents who press the provider into breaking the law are liable under the same articles.

Not content with the current range of surveillance possibilities, the FSB has developed a new version of SORM, called SORM-2, which governs e-mail, cellular telephones, and pagers. Unlike the other documents mentioned in this article, Citizens' Watch has not

been able to obtain a copy of the SORM-2 regulations; apparently, development of the system has not been completed. However, it is known that in all cases the system would operate in the same manner. The service provider gives the FSB the equipment necessary to conduct surveillance from a remote location (up to 16 kilometers from the mail server) -- that is, from the FSB office. This access would extend to monitoring the frequency and duration of a client's use of his e-mail account, as well as providing the ability to identify the client's correspondents and to obtain the information in the correspondence. Moreover, the FSB could block certain communications or even alter their content and no one, including the service provider, would be able to detect such activities. If and when SORM-2 becomes operational, the only safeguard remaining will be the provision that the FSB must have a warrant to make such materials obtained through surveillance admissible in court. At least for now we have this measure of protection: Next year, who knows?

Notes:

(1) Citizens' Watch is a nongovernmental human rights organization based in St. Petersburg.

(2) Kompromat refers to efforts (usually by the "services") to collect (or fabricate) compromising material -- of a criminal, pornographic, or "treasonous" nature -- against persons or an organization deemed to be "targets."