

Operational-search Counteraction to Crimes Committed in the Institutions of the Penal System using Information and Communication Systems

Andrey Nikolaevich Fedorov¹ and Eldar Faritovich Naruslanov¹ ^a

¹The Scientific Research Institute of the Federal Penitentiary Service of Russia, Ph.D. in Law, Moscow, Russian Federation

Keywords: Operational-search activity, information systems, communications, means of communication, fraud, counteraction, penal system, investigation of crimes.

Abstract: The need for widespread use of criminological knowledge in the development of theory and practice to increase the efficiency of detecting fraud committed using mobile telephone communications is impossible without deep comprehensive scientific research, legal, organizational and tactical measures of a covert operational-search nature. The specifics of the disclosure of fraud committed using mobile telephone communications, which includes such components as the detection, prevention, suppression of these crimes, has not been and is still relevant, including its penitentiary component. These circumstances indicate the need for develop and implement adequate measures to disclose fraud committed using communications, and determine the relevance of the topic of the article. In this work, the authors made an attempt to analyze the current set of measures to improve operational-search activities to disclose fraud committed using communications, as well as to determine the most effective ways of its development. Purpose of the study: generalization of knowledge that allows to develop complex scientifically grounded measures to improve operational-search activities to disclose fraud committed using communications. Objectives of the research: to investigate the current state of the operational-search activity to disclose fraud committed using communication means; to develop scientifically grounded recommendations and proposals for improving the organization of operational-search activities to disclose fraud committed using mobile telephone communications. Methodology: analysis of the current legislation, as well as scientific materials touching upon the issues on the topic of this study, conducting questionnaires and interviews with existing employees of institutions of the penal system, as well as communications workers. Results achieved: recommendations were formulated to improve the operational and investigative counteraction to crimes committed in prisons with the help of information and communication systems that can reduce the number of telephone fraud cases carried out on the territory of places of deprivation of liberty, as well as ensure an effective fight against telephone fraud without attracting additional forces and funds.


1 INTRODUCTION JUSTIFICATION OF NOVELTY, HYPOTHESIS

In modern realities, informatization is one of the most actively progressing directions in the development of society. Information systems, including those that ensure the communication needs of mankind, have now been widely implemented in various spheres of life, thereby forming a high-tech and at the same time public space, taking one of the dominant places in people's lives (Melnikov., 2015).

Such a rapid development of information networks seems to be a completely understandable phenomenon, primarily due to a number of factors (Miroshnikov, 2015):

- simplicity and availability;
- the possibility of interaction between subscribers to exchange information regardless of the distance of their location relative to each other;
- the absence of interstate restrictions and this applies to both users and service providers.

The considered aspect of the development of society is undoubtedly a positive global achievement that brings into people's lives an unhindered

 <https://orcid.org/0000-0002-6024-845X>

opportunity for communication and exchange of information, however, thanks to the functions described above, informatization becomes the object of attention of the criminals, and when it seems in the hands of criminals, it turns into an "instrument" of committing crime encroachments (Meshkova, 2003).

The emergence and development of mobile telephone communications led not only to the intensive development of modern society in the field of its informatization, but also to the introduction of the achievements of science and technology when committing fraudulent actions.

The negative consequences of fraud committed using mobile telephone communications means, in a broad sense, include the threat to the information security of the state, information and psychological security of the individual, wide opportunities for the use of disinformation and manipulation of consciousness, the widespread use of information systems and networks in illegal activities (Merzogitova, Mayorova, 1998). The information space is an ideal environment for the activities of criminals, since access to it is extremely easy, the potential environment for illegal activities is significant, and it is easy to ensure the anonymity of users, it is not controlled by anyone and is extremely poorly controlled (Zharova, 2019).

Technological schemes developed and applied by criminal groups using mobile telephony are distinguished by a high degree of thoughtfulness and organization, can be both fairly simple and multi-stage, spatially separated and lasting in time. At the same time, different areas of illegal activity in various areas are interconnected and synchronized with each other in the process of preparing and committing a crime (Sukhodolov, Ivantsov, Borisov, Spasennikov, 2017).

It should be emphasized that the problem of disclosing fraud committed using communication means is one of the most urgent in the field of combating ordinary and penitentiary crime. It is determined by the high latency of these crimes and the fact that 93.7% of people living in Russia use mobile telephone services, which makes them potential victims of "telephone scams".

Since mid-2008, "telephone fraud" has spread in prisons as well. This is due to the fact that the specifics of staying in institutions of the Penal System of the Russian Federation (hereinafter - PS) predetermines an extremely high degree of demand for communication services for suspects, accused and convicted persons.

The surge in mobile phone fraud has naturally attracted the attention of science. In recent years,

dissertation research has been carried out on issues affecting the designated problems (M.N. Bogdanov, S.V. Gorobchenko, S.N. Kazinskaya, B.A. Kurinov, V.V. Malygina, I.M. Mishina, A.N. Rozin, A.A. Nuzhdina). However, their analysis shows that they are dedicated to:

the study of general issues of fraud investigation methodology;

prepared taking into account the specifics of certain areas of activity (banking, housing, etc.).

As for the issues of operational and investigative counteraction to crimes committed in the institutions of the penal system using information and communication systems, they were not the subject of independent scientific research.

In this regard, the purpose of the study described in this article is to generalize knowledge that allows the development of comprehensive scientifically grounded measures to improve operational-search activities to disclose fraud committed using communications.

Achievement of the set research goal necessitated the formulation and solution of the following tasks:

1) to investigate the current state of operational and investigative activities to disclose fraud committed using communication means;

2) develop scientifically grounded recommendations and proposals for improving the organization of operational-search activities to disclose fraud committed using mobile telephone communications.

Thus, this article will consider the problematic issues of operational-investigative counteraction to crimes committed using information and communication systems, including by persons held in penal institutions.

2 MATERIALS AND METHODS

The methodology and methods of research represent a system of general scientific and special legal means and methods of cognition that ensure objectivity and comparativeness in the study of operational-search activities to disclose fraud committed using communications. Among them, in the process of work, the comparative legal method, general scientific methods of analogy and statistics, induction and deduction, sociological methods of questioning, interviewing, content analysis, and other research tools of modern socio-humanities were used, which make it possible to comprehensively study the stated topic of the article. Analyzed the current legislation,

as well as scientific materials raising issues on the topic of this study.

3 RESULTS AND DISCUSSION

It should be noted that the operational-investigative counteraction to crimes committed in the institutions of the penal system using information and communication systems is complicated by the fact that today there are a number of problematic issues in places of deprivation of liberty that do not allow to fully exclude the commission of remote frauds committed by suspects accused and convicted. These issues include:

- lack of funding for the purchase of technical means to suppress radio signals used by mobile operators within the boundaries of penal institutions. The approximate cost of the equipment of 1 institution of the penal system is 15-20 million rubles. The equipment of all institutions of the Russian penal system requires more than 14 billion rubles. However, even if there is the necessary amount of funding, this equipment, after a certain time, needs to be updated in view of the improvement of communication services. At the same time, according to the position of the Ministry of Telecom and Mass Communications of the Russian Federation, the setting of intentional radio interference for civilian purposes is not allowed, since it will lead to the creation of unacceptable interference with the operation of existing mobile radio communication networks, at the same time, guaranteed blocking of cellular communication signals throughout the institution is not ensured. In addition, these devices do not block 3G / 4G cellular networks;

- the absence in the Federal Penitentiary Service of Russia of normative documents establishing the norms for the position and the procedure for the use of blockers;

- lack of normative consolidation of the obligation of mobile network operators to exclude communication services on the territory of institutions of the Federal Penitentiary Service of Russia. Amendments to the Federal Law of 07.07.2003 No. 126 - FL "On Communications" are required;

- lack of interest of mobile operators in the exclusion of the territories of institutions of the PS of Russia from the coverage area of their base stations.

In addition, in practice, there are cases when criminals who are outside the institutions of the penal system, acting in order to mislead the bodies of the preliminary investigation about their whereabouts,

commit remote fraud near the institutions of the Federal Penitentiary Service of Russia, for example, while in motor transport, thereby falling into a single coverage area base station of a mobile operator, as the institution of the PS. As a result of such activities of criminals, in 2019, cases of documenting the facts of remote fraud from the territory of former institutions of the penal system, liquidated or transferred to other departments, were identified. In such cases, the process of identifying suspects requires additional time required to carry out operational-search activities.

On the part of the Federal Penitentiary Service of Russia, at various government commissions and coordination meetings, topical issues of the need to exclude the possibility of using mobile communications by persons held in penal institutions are regularly raised.

It should be noted that telecom operators each year suffer losses associated with mobile fraud on a global scale of about \$ 25 billion. Unfortunately, domestic mobile operators prefer not to advertise their losses from this criminal activity. As for users, we note that as a result of a survey of Russian subscribers, it was found that 78 % of respondents are aware of telephone fraud, and 15 % noted that their relatives and friends have suffered from the actions of fraudsters who used mobile telephony.

In these conditions, it is important not only to organize and purposefully carry out security, but also operational-search measures to uncover fraud committed using mobile telephony facilities in penal institutions. The problem of increasing the efficiency of the operational-search support of their disclosure has acquired the character of a most important intersectoral, interdisciplinary scientific and practical problem. At the same time, its system is complex and requires deep scientific understanding, a clear definition of its subjects and objects, the delineation of competence and responsibility between the subjects of operational-search activity.

One of the most effective areas of activity of operational units for detecting qualified crimes related to telecommunications is the integrated processing of information about subscribers and the communication services provided to them, data from automated payment systems for communication services and technical, in-system information characterizing the operation of communication systems (billing information) (Kirilenko, Alekseev, 2020).

The primary data necessary for carrying out measures for analytical support of the activities of operational units of the FPS can be obtained:

- during the examination of telephones seized from persons held in penal institutions or transferred to them;

- by analyzing data on the connections of telephones operating on the territory of the penal system institutions or in the areas where crimes are committed by persons held in the penal system.

The proposed approach is based on the fact that when preparing and committing a fraud committed using mobile telephone communications, mobile telephones is used from the territory of the penal system at the stage of preparing and committing a crime. Therefore, solving the problem of identifying their subscribers who took part in the preparation and commission of a crime corresponds to solving the problem of identifying persons involved in the crimes being committed and establishing the facts of their illegal activities (Stepanenko, Bakhteev, Evstratova, 2020).

Moreover, in the conditions of an almost complete absence of data on users of communication networks, the rapid change of subscriber numbers and terminal numbers, as well as the use of one-time or session SIM-cards, identification and binding of control objects to communication means in most cases is possible only during the analysis of technical or intrasystem data, the acquisition and analysis of which is possible only with the use of both special hardware and software complexes, and specialized software tools or packages of application programs for general use (Ammar, 2019.).

Prevention, however, often comes down to only measures of criminal repression (Lavorgna, 2019), on which most of the interviewed employees of operational units still rely, believing that the only effective measure to prevent new crimes is the arrest and conviction of a fraudster. Therefore, the most serious attention should be paid to the prevention of cases of criminal fraud, suppression of the active activity of professional fraudsters, and neutralization of factors that facilitate their illegal actions (Galakhov, 2001). So, organizing the prevention of fraud committed using mobile telephony means, you need to:

- identify factors contributing to the commission of fraud and take measures to eliminate them;

- determine the circle of persons who may be capable of carrying out fraud, and take appropriate measures in order to prevent its commission;

- to identify ways of committing planned or planned crimes, conditions and other circumstances that fraudsters intend to use (Paramonov, 1998).

General preventive measures are aimed at identifying, eliminating and neutralizing the causes and conditions that contribute to fraudulent manifestations. Measures of this nature are based on the analysis of negative factors contributing to the manifestation of fraud, the available operational-search information.

Analysis of information, depending on the tasks at hand, allows you to have information about the effectiveness of preventive measures, to have an idea of the negative factors that contribute to fraud, to take timely measures to eliminate them based on the rational use of available forces and means. In addition, in the process of studying operational materials, changes and trends in the psychology of fraudsters and their tactics are revealed, which is one of the conditions for the correct organization of the work of persons assisting operational units in order to disclose fraud (Gurov, 1986).

Operations staff can, using overt and covert methods:

- to establish the circle of accomplices of fraud and the role in the crime of each of them;

- to identify the nature of actions for the preparation and implementation of criminal intentions, ways of committing fraud;

- to actively influence the persons involved in such crimes in order to persuade the latter to abandon illegal actions, to exert a preventive effect on them, to remove from the negative influence of criminals and other persons with a less persistent criminogenic motive;

- successfully identify persons who may be witnesses, victims, as well as various objects and documents of evidentiary value;

- to identify persons who are aware of crimes, methods and circumstances of their commission;

- detect places of shelter of property and valuables obtained as a result of committing fraudulent activities;

- participate in the verification of operational and other information;

- control the channels of information exchange between persons held in penal institutions and their accomplices who are at large, block (interrupt) the operation of communications on the territory of penal institutions.

The essence of the suppression of fraud is characterized, as it were, by a logical continuation of measures to prevent contemplated or planned crimes and comes down to the arrest of those being checked red-handed at the time of the crimes. The conditions for the successful implementation of such detention are:

- high-quality information support of ongoing activities (it is necessary to have information about when, where, in what way and in what composition the criminals intend to act, etc.);

- conducting a study of the object at which the fraudsters intend to commit a crime;

- determination of the forces, means necessary for the operation, briefing and placement of employees of operational units and other services carrying out the arrest of criminals red-handed;

- high secrecy of the conducted OSM.

The practice of disclosure shows that the activities of persons who specialize in fraudulent actions committed using mobile telephone means are distinguished by a high degree of criminal professionalism and legend of their illegal actions (Martin, Munksgaard, Coomber, Demant, Barratt, 2020). As a rule, the objects of investigation use several sets of SIM-cards used in the preparation and commission of crimes. Therefore, in the areas where crimes are committed, some subscriber numbers are used, and in everyday activities, others. At the same time, separate terminals can be used for everyday SIM cards. At the same time, in a number of cases, during the commission of a crime, criminals also have everyday mobile phones with them, on which they can receive calls or SMS messages. These telephones are identified by building time-space models and identifying multiple numbers simultaneously located in the same areas (Kemp, 2020).

The main feature of the operation of such sets of mobile phones is the use of terminals with several SIM-cards and the interconnected operation of several mobile phones in space and time. For complex processing of data obtained from several sources, a system of semantic-statistical processing of heterogeneous information can be used.

When conducting operational-search measures in relation to fraudsters, the following tasks are solved:

- identification and thorough examination of all participants in the commission of fraud, including the use of citizens who provide assistance to operational units;

- establishing the true role of each accomplice in committing fraud;

- establishing the facts of the criminal activity of criminals;

- documenting criminal acts;

- non-admission (suppression) of criminal acts;

- identification of the accomplices of fraudsters, as well as persons included in their circle of communication;

- taking measures aimed at compensation for material damage caused by the criminal actions of the inspected persons;

- identification and arrest of fraudsters red-handed;

- identification and elimination of the reasons and conditions conducive to the commission of fraud committed using the means of mobile telephone communications.

In the process of verification activities in relation to persons suspected of committing fraud as part of a group, it becomes necessary to document the criminal activity of the entire group of fraudsters. To accomplish this task, it is advisable to use the capabilities of specialized technical units, since with the help of their employees, the members of the criminal group, their roles, previously unknown episodes are established; places of storage and sale of money, jewelry and things acquired as a result of fraud, etc.

The analysis shows that the effectiveness of processing the information obtained in the course of technical measures depends on the level of interaction of the interested services. This relationship is largely due to the specifics of the tasks solved by the departments of technical measures, which consist in documenting criminal activity (Caneppele, 2019).

In the legal literature, based on an analysis of the practice of combating crime in general, an opinion has been expressed about the possibility of using two main tactics when documenting criminal activity, which can be successfully used when documenting fraudulent actions:

1. Identification and recording of actions that are criminal in accordance with the current criminal code, and committed by leaders and participants of criminal fraudulent structures;

2. Collection and recording of factual data confirming the existence and activities of a criminal community (criminal organization), an organized group.

In the context of the above, special attention should be paid to the issues of documenting the illegal actions of organizers and other leaders of criminal fraudulent groups. In this regard, one of the main tasks of documentation is to establish the activities of their leader in organizing specific crimes and guiding the activities of their members. Among the main actions of the organizers associated with their direct participation, the creation and management of a criminal group of fraudsters, we will include the following:

- selection of members of the fraudulent group, distribution of their roles and responsibilities;

- formation of a unified attitude and correct understanding of the criminal purpose among persons participating in fraudulent activities;
- supplying direct perpetrators of fraudulent actions with means of committing crimes;
- development of forms for reporting ordinary fraudsters to their leader and ways to maintain intragroup discipline;
- involvement of new members into the criminal group of fraudsters, prevention of the exit from the formation of individual participants;
- determination of the vector of the group's activities, including tactical and strategic aspects;
- determination of the scope of the criminal offense, as well as the search for a potential victim;
- building a latent system of corrupt relationships with government agencies;
- organization of counteraction to law enforcement structures (Meshkov, 2003).

Identification and fixation in the course of documenting the above actions will make it possible to establish the fact of the creation and management of the activities of an organized criminal structure, and the circle of its members.

When documenting the actions of the organizers of fraud, it is necessary to record the presence of corruption ties that provide the criminal structure with a certain level of security (Bordilovsky, 1993).

An analysis of the experience of combating fraudsters with corrupt connections shows that in the course of identifying corrupt officials and documenting their illegal activities, it is necessary to establish data indicating such facts and circumstances as (Kornoukhov, 1995):

- direct participation of officials of state authorities and administration in criminal activities;
- use of official position to cover up fraudulent activities.

Documenting in this case involves the identification, verification and consolidation of data objectively confirming the action or inaction in connection with which the fraud was carried out (Ryabkov, 2001). Through tacit opportunities or with the help of technical means, it is also necessary to find out in whose interests the transfer (or transfer) of the bribe is supposed to be.

4 CONCLUSIONS

In conclusion, it should be emphasized that only the comprehensive use of the capabilities of law enforcement agencies, tactically competent and qualified and justified use of both public and private

capabilities of units carrying out operational-search activities, can achieve positive results in disclosing fraud committed using communications.

The results obtained in the course of the study allow us to formulate a number of recommendations for practitioners and heads of institutions and authorities of the penal system involved in direct counteraction to telephone fraud:

It is necessary to conduct a survey of the territory of each institution of the penal system, in which suspects and those accused of committing crimes are kept, as well as those sentenced to imprisonment are serving a criminal sentence. As part of the survey, identify premises that are suitable for committing crimes related to telephone fraud.

Strengthen surveillance in the premises identified during the survey by installing permanent video surveillance.

If it is possible to exclude access to the premises of the risk group for persons included in the circle of potential fraudsters.

On the part of the PS authorities, there should be constant monitoring of persons who have access to premises suitable for committing crimes related to telephone fraud.

The introduction of the formulated recommendations into the practice of the institutions and bodies of the PS will significantly reduce the number of cases of telephone fraud carried out from their territory, as well as ensure an effective fight against telephone fraud without attracting additional forces and funds.

REFERENCES

- Ammar, J., 2019. Cyber Gremlin: social networking, machine learning and the global war on Al-Qaida-and IS-inspired terrorism. *In International Journal of Law and Information Technology*. 27(3). pp. 238-265.
- Bordilovsky, E. I., 1995. Operational-search support of the crime investigation process: lecture. p. 5.
- Caneppele, S., 2019. Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes. *In Policing: A Journal of Policy and Practice*. 13(1). pp. 66-79.
- Galakhov, S. S., 1989. Fundamentals of crime prevention by units of the criminal police: author. dis. 21 p.
- Gurov, A. I., Yurko, E. I., 1986. Combating fraud in transport: a tutorial. 38 p.
- Kemp, S., 2020. The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain. *In European Journal on Criminal Policy and Research*. 26(3). pp. 293-312.
- Kirilenko, V. P., Alekseev, G.V., 2020. Harmonization of Russian criminal legislation on countering cybercrime

- with the legal standards of the Council of Europe. *In All - Russian Criminological Journal*. 14(6). p. 901.
- Lavorgna, A., 2019. Cyber-organized crime. A case of moral panic? *In Trends in Organized Crime*. 22(4). pp. 357-374.
- Martin, J., Munksgaard, R., Coomber, R., Demant, J., Barratt, M. J., 2020. Selling Drugs on DarkwebCryptomarkets: Differentiated Pathways, Risks and Rewards. *In British Journal of Criminology*. 60(3). pp. 559-578.
- Melnikov, D. A., 2015. *Organization and security of information and telecommunication networks and systems*. p. 598.
- Merzigitova, Yu. A., Mayorova, E. I., 1998. *Qualifications of an organized criminal community (criminal organization)*. pp. 14-15.
- Meshkova, B. C., 2003. Exposing the leader (organizer) of a criminal group in its creation and management of criminal activity: author. dis. pp. 12-13.
- Miroshnikov, B. N., 2015. *Network factor. Internet and Society*. p. 288.
- Paramonov, I. M., 1998. Prevention and disclosure of fraud by criminal investigation apparatus: stock lecture. p. 24.
- Presser, L., Sandberg, S., 2019. Narrative Criminology as Critical Criminology.
- Ryabkov, E. M., 2001. Neutralization of counteraction in the field of operational-search activities of internal affairs bodies (legal, organizational and tactical issues): dis.
- Stepanenko, D. A., Bakhteev, D.V., Evstratova, Yu. A., 2020. Use of artificial intelligence systems in law enforcement. *In All-Russian criminological journal*. 14(2). p. 212.
- Sukhodolov, A. P., Ivantsov, S.V., Borisov, S.V., Spasennikov, B. A., 2017. Actual problems of preventing crimes in the economic sphere, committed using information and telecommunication networks. *In All-Russian Criminological Journal*. 11(1). p. 16.
- Kornoukhov, V. E. and others. The course of criminalistics. pp. 109-117.
- Yakovlev, A. M., 2017. Theory of criminology and social practice. p. 248.
- Zharova, A. 2019. Ensuring the Information Security of Information Communication Technology Users in Russia. *In International Journal of Cyber Criminology*. 13 (2). pp. 255-269.