Евразийская адвокатура. 2023. № 3 (62). С. 101.
Eurasian advocacy. 2023;(3(62)):101.

Правосудие и правоохранительная деятельность в евразийском пространстве

Научная статья
УДК 343.985.2
doi 10.52068/2304-9839_2023_62_3_101

ИНДЕКСАЦИЯ ЭЛЕКТРОННЫХ СООБЩЕНИЙ В ХОДЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

ПЕЧНИКОВА Розалия Багдуевна
Аспирант кафедры криминалистики юридического факультета Московского государственного университета им. М.В. Ломоносова
119991, г. Москва, Ленинские горы, д. 1, стр. 13, Российская Федерация

Аннотация: Статья посвящена вопросам электронной переписки. В настоящее время электронная переписка занимает важное место в жизни людей и является наиболее популярным инструментом для обмена информацией. Поэтому электронные сообщения являются важной составляющей доказательной базы.

Большая значимость электронной переписки и распространение мобильных устройств предъявляют все новые и новые требования к ученым, юристам, криминалистам и следователям. Требуется освещение базовых особенностей и специфики электронной переписки, а также методов поиска относимых сообщений.

Статья посвящена исследованию большого массива электронных сообщений путем индексации. В статье описаны методы поиска по электронной переписке. Из-за популярности такого способа обмена информацией электронная переписка может быть довольно объемной и не всегда относимой к предмету доказывания. Для того чтобы отграничить круг относимых к доказыванию сообщений, необходимо применять индексацию электронных сообщений. Это один из способов поиска нужной информации. Индексация заключается в поиске по ключевым словам. В статье описаны инструменты и механизмы такого поиска, необходимое программное обеспечение. Также описывается алгоритм выявления наиболее полезных для поиска ключевых слов и порядок применения такого алгоритма для составления списка ключевых слов следователем.

Ключевые слова: расследование, индексация, электронные сообщения, цифровые доказательства, цифровые сообщения

Для цитирования: Печникова Р.Б. Индексация электронных сообщений в ходе расследования преступлений // Евразийская адвокатура. 2023. № 3(62). С. 101. https:// doi.org/10.52068/2304-9839_2023_62_3_101

Justice and law-enforcement activity in the eurasian space

Original article

INDEXING OF ELECTRONIC MESSAGES DURING THE INVESTIGATION OF CRIMES

PECHNIKOVA Rozaliia Bagduevna
Postgraduate student of Department of Criminalistics of Law faculty of Moscow State University
119991, Moscow, Leninskiye gory, 1, b. 13, Russian Federation

Abstract: The article is devoted to the issues of electronic correspondence. Currently, electronic correspondence occupies an important place in people's lives and is the most popular tool for information exchange. Therefore, electronic messages are an important component of the evidence base. The great importance of electronic correspondence and the spread of the use of mobile devices by people places new and new demands on scientists, lawyers, criminologists and investigators. It requires coverage of the basic features and specifics of electronic correspondence, as well as methods of searching for relevant messages.

The article is devoted to the study of a large array of electronic messages by indexing. The article describes the methods of searching by e-mail. Due to the popularity of this method of information exchange, electronic correspondence can be quite voluminous and not always relevant to the subject of proof. In order to delineate the range of messages related to proof, it is necessary to use indexing of electronic messages. This is one of the ways to find the right information. Indexing consists in keyword search. The article describes the tools and mechanisms of such a search, the necessary software. The article also describes an algorithm for identifying the most useful keywords for searching and the use of such an algorithm for compiling a list of keywords by an investigator.

Keywords: Investigation, indexation, e-messages, digital evidence, digital messages

For citation: Pechnikova R.B. Indexing of electronic messages during the investigation of crimes = Eurasian advocacy. 2023;3(62):101. (In Russ.). https://doi.org/10.52068/2304-9839_2023_62_3_101

© Печникова Р.Б., 2023

Technological progress does not stand still, modern technical achievements play a big role in people's lives. Currently, few people can live without a smartphone, almost everyone has a social media account and uses a computer. There has been a transformation from analog devices to digital ones, thus, some scientists argue about the emergence of a completely new and specific forensic category – «virtual traces». Unfortunately, such progress serves not only good purposes, but also helps to develop crime, creating new ways and means of committing a crime, ways of communication and interaction of criminals among themselves, the interaction of the criminal with the victim.

One of the results of this transformation was the increase in information exchange between people using electronic devices. It's not just about verbal communication, but about the exchange of thoughts expressed in a letter – about correspondence. The importance of the information stored in the correspondence cannot be underestimated. Nowadays, people communicate by correspondence even more often than live communication. Through electronic messages, people communicate, arrange meetings and even conduct business.

Today, the Internet network plays a huge role in people's communication. Such communication is also used to commit crimes. We are not talking about crimes in the field of computer information, but about absolutely any crime. Attackers plan crimes using the Internet, communicate and keep in touch with each other using electronic messages. Electronic messages contain a large number of forensic important traces of a crime, which can and should be used in the investigation, as well as in proving.

Electronic messages are a huge array of information. It is quite difficult to find the necessary data in it that will be relevant to the case. For these purposes, keyword search or indexing is used. A keyword is a word that is contained in the desired message or characterizes it and allows you to find the desired message. An index is a number, letters, word, or other combination of characters, a data structure that contains information about a document (in our case, a message) and allows you to quickly and accurately search for the necessary information.

Continuous viewing of messages that have been compiled for a long time will take a lot of time, may lead to disruption of procedural deadlines. Therefore, software tools have been developed to solve this problem. At the moment, there is no more effective tool for finding relevant messages than indexing – keyword search. A keyword is a word that is contained in the desired message or characterizes it, so that the message can be highlighted and marked as having significance for the investigation.

The first stage of the indexed search begins with determining the circle of persons, e-mail addresses, correspondence with which may potentially contain the necessary information. With the help of already available data, the time interval to which correspondence containing the required information can relate is limited. After that, there is a search for correspondence directly (with certain persons and in a certain period of time). The found correspondence is already being searched by keywords.

The search is carried out using special software. Firstly, these are commercial software complexes designed for the study of electronic devices in general, such as AccessData FTK, EnCase, BelkaSoft and Archivist, Oxiom, BlackBag and others. These programs have an option to search using keywords, but this is only one of the tasks. Secondly, these are software complexes that allow you to search for keywords in large data arrays and such a search is their main task, and in addition, they have some analytical functions with which you can filter files by subject. Such programs include: ZyLAB, Relativity, Nuix, Ringtone and others. They are distinguished by the presence of great features, such as searching in files of various formats, searching for similar words, etc.

The search takes place as follows: the operator loads the volume of messages to be examined into the program, forms a list of keywords, sets them for search, and then checks the results issued by the software tool.

Of course, the software does not perform a primitive search for a combination of letters. For example, spelling mistakes, unfinished words, synonyms and consonant words with keywords – all this will be found. However, the list of keywords itself should be compiled by a person, in our case, an investigator or an expert.

Keyword compilation should be carried out in accordance with the following algorithm:

1. Formulation of the goal. At this stage, an idea is formed about the actual circumstances that can be reflected in the correspondence, and which can be used in proving the case. This stage helps to avoid unjustified viewing of messages that are not relevant to the case, which in one way or another is a violation of the secrecy of correspondence, which should be avoided unnecessarily.

So, in the USA there is a reservation to the Fourth Amendment to the US Constitution, which is called «plain view doctrine» – «open view theory». It allows police officers to inspect and seize only those evidences that are in plain sight, or those directly targeted by

the search. In the case of USA v. Carey [2], the police had a warrant that provided for their search during the search of computer files containing names, addresses, phone numbers related to the distribution of prohibited substances. During the search, one of the police officers began to look through all the files on the computer in general, and found child pornography. During the proceedings, the court for the first time applied the theory of an open view to the search of a computer and ruled that only those files and data that are relevant to the event under investigation should be seized. Part 1 of Article 88 of the Code of Criminal Procedure of the Russian Federation contains a requirement on the relevance of evidence. In the Comments to the CPC, it is said that a sign of the relevance of evidence in criminal proceedings is their logical connection with the circumstances listed in Article 73 of the CPC that are subject to proof, i.e. with the subject of proof. However, often, the data array in the correspondence is so large that it can be quite difficult to identify relevant messages.

In Russian criminal proceedings, information on devices is often obtained by investigators during an inspection of physical evidence (for example, an inspection of a smartphone). The procedure for such an inspection does not impose restrictions on the investigator as to which files he can view and what information he can receive. In our opinion, the messages examined by the investigator should be relevant to the event under investigation, by analogy with the US experience. And it is the correct indexing of electronic messages during the investigation that will help to limit the range of messages considered by law enforcement agencies, narrowing them to those related to the specific information sought.

2. Assessment of available information. At this stage, the investigator should analyze all the available information. Special attention should be paid to names, addresses, phone numbers, nicknames (if any), the age of the recipients, their education. Also, a valuable source of data can be interrogation recordings or materials of operational investigative measures that can help establish peculiar speech patterns, conditional expressions, words used in live speech by the person whose correspondence is being investigated. As a result, we get a reasonable idea about the intellectual level of development of the participants in the correspondence, about the vocabulary they use, etc.

3. Comparison of available and required information. According to Koldin V.Ya. [1, c. 3], investigative actions «without an information search model of the desired and a clear representation of the tasks of the investigative action, as a rule, do not lead to the goal, but most often cause tactical harm.» This also applies to the indexing of electronic messages during the investigation process. It is the comparison and comparison of the available information with the desired one that will determine the further tasks of the investigator on the way to the formulation of keywords. So, for example, the investigator knows that he does not have enough evidence about the transfer of a bribe, at this stage he compares the available data (testimony that the bribe was transferred to a certain person, documents confirming the performance of certain actions by a person) with the missing ones (the amount of the bribe, confirmation of the fact of its transfer, an agreement on the performance of actions, the person's ability to perform these actions, etc.), after which he will get a clearer idea of the information he is looking for: he will have to find messages confirming the meeting or agreement. This will allow the investigator to identify gaps in the array of evidence and understand whether potential messages will be able to fill them.

4. Identification of the main words and phrases. Having determined what evidentiary information the investigator expects to find in the correspondence, he, to begin with, in general terms, forms a list of words and phrases that may be contained in the alleged information, and which indicate the circumstances of interest to the investigation.

5. Identification of features and formulation of synonyms. Modern software is capable not only of searching for specific words, but also of searching for messages that include similar words or synonyms. However, any search for such words is based on the database of a specific program, which includes words and their synonyms. Such programs cannot take into account, for example, all the slang of the criminal world or certain ciphers. That is why, during the formulation of keywords for the investigator, the social group to which the addressees of the messages belong, and even the individual features of the vocabulary of the participants in the correspondence, phraseological phrases that are used, or can be used by them, in relation to the event under investigation, are also of great importance. For example, if we are talking about indexing corporate email messages, we should not forget about corporate slang. So, the word «bribe» in corporate language is often replaced by the word «kickback», «fit», «kick-back».

6. Formation of the final list of keywords. At this stage, the investigator, having summarized his ideas about the terminology used in the correspondence and its place in the event under investigation, makes a complete list of keywords, taking into account all the existing gaps and features.

The Code of Criminal Procedure of the Russian Federation provides for the possibility of attracting a specialist. During the formulation of keywords for indexing, we suggest not to neglect the involvement of a specialist, if required. So, it is possible to involve a data encryption specialist, a linguist or, for example, a translator.

Modern indexing software tools are based on logical search operators. Some, for example, allow you to search for several keywords simultaneously, which allows you to exclude possible omissions related to spelling errors or abbreviations made when composing the messages themselves, as well as expand the search by using synonyms. For example, to search for information about a bribe in messages using the ZyLAB program, the following keywords can be used: kickback OR bribery OR «on the paw»…

The indisputable advantage of the ZyLAB program is the ability to search for words in embedded files, including not only text, but also graphic ones. But, at present, this program is not always available to employees of the investigative apparatus.

The results of the survey conducted within the framework of this dissertation research showed that most law enforcement officials are not familiar with the concept of indexing electronic messages and do not apply it in practice. However, there are also those who are familiar with and successfully use indexing during the investigation. They use the following software: ZyLAB, dtSearch Desktop, Archivist.

Search by keywords in electronic correspondence can be carried out both as part of a computer-technical examination, and directly to investigators as part of an inspection of the device. To do this, the investigator needs to install a program that provides indexed search on his work computer, connect the device under investigation to it and use the program to download the array of messages to be investigated to his computer, after which he will conduct his research by indexing. Modern programs have a fairly user-friendly interface that is understandable to everyone, and do not require special knowledge that goes beyond the skills of an ordinary user. Of course, such actions cannot always be carried out by an investigator, since access to the data on the device is not always easy to obtain, and if this requires special knowledge, the device must be sent for examination. The found messages should be recorded in the inspection report or in the expert's opinion. The electronic messages themselves must be transferred to an electronic medium and attached to the case materials.

Indexing of electronic messages can greatly facilitate the search for the necessary information and reduce the time for this search. Modern indexing software does have serious capabilities, however, human participation is still the most important aspect, since it is the person who makes the list of keywords. Such compilation should be built in accordance with a clear algorithm so as not to miss important words and information. Limiting the range of words, you are looking for will not only help you focus on important evidentiary information, but will also help you avoid violating the rights of the author of the investigated messages.

Список источников

1. Вещественные доказательства: Информационные технологии процессуального доказывания / под. общ. ред. В.Я. Колдина. М.: НОРМА, 2002.

2. США против Кери, 110 (Список дел Верховного Суда США) 51(1884) [Электронный ресурс]. URL: https://supreme.justia.com/cases/federal/us/110/51/.

References

1. Veshhestvenny`e dokazatel`stva: Informacionny`e texnologii processual`nogo dokazy`vaniya / pod. obshh. red. V.Ya. Koldina. M.: NORMA, 2002.

2. SShA protiv Keri, 110 (Spisok del Verxovnogo Suda SShA) 51(1884) [E`lektronny`j resurs]. URL: https://supreme.justia.com/cases/federal/us/110/51/.

Статья поступила в редакцию 16.05.2023; одобрена после рецензирования 26.05.2023; принята к публикации 26.05.2023.

The article was submitted 16.05.2023; approved after reviewing 26.05.2023; accepted for publication 26.05.2023.