Information Technology of Big Data in Crime Detection, Investigation, and Prevention. Theoretical and Applied Analysis of Individual Prospects and Application Problems

Ruslan Mikhailovich Ushakov
First and corresponding author
4th year student at the Institute of the Prosecutor's Office
Saratov State Law Academy
11 Druzhby Str., apt. 11, Volzhsk, 425001, Mari El Republic, Russian Federation

Dmitry Alekseevich Efremov
PhD in Law
Associate Professor at the Department of Criminalistics
Saratov State Law Academy

Olga Anatolyevna Gariga
PhD in Law
Associate Professor at the Department of Criminalistics
Saratov State Law Academy

Nikolay Aleksandrovich Finogenov
PhD in Law
Associate Professor at the Department of Criminalistics
Saratov State Law Academy

Rustam Batrkhanovich Khametov
PhD in Law
Associate Professor at the Department of Criminalistics
Saratov State Law Academy

Article History: Received: 10 November 2020; Revised 12 January 2021 Accepted: 27 January 2021; Published online: 5 April 2021

Abstract

The article discusses various aspects of the use of Big Data technology in forensic activities. Based on the analysis of legislation, the provisions of the legal doctrine, and the existing experience of using various forms of artificial intelligence in human life, the authors indicate possible directions for their implementation in forensic practice (first of all, in the work of an expert), and identify dialectically related risks and problems of a conceptual and legal nature. The necessity of developing and issuing several legal measures aimed at preventing the negative consequences of the spread of Big Data technology, in particular, a general legislative ban on the adoption of legally significant decisions by law enforcement entities based solely on the conclusions obtained by program methods, is substantiated.

Keywords: big data; artificial intelligence; neural networks; machine learning; expertise.

Introduction

The current state of activity to identify, disclose, investigate, and prevent crimes is characterized by the process of structural and substantive complication, differentiation of methods, methods, and means of their implementation. If you do not take into account the human factor, then, on the one hand, these are the ample opportunities available in the investigation of traditional types of crimes, based on vast practical experience and multiplied by the modern achievements of the sciences of the criminal legal cycle. On the other hand, it should be noted the constantly emerging difficulties in identifying and investigating new types of crimes (including those that have been known for a long time but have radically changed in the way they are implemented recently) at all stages of legal proceedings. To attempt to analyze the current situation through the prism of the aspects indicated in the title of this work, it seems necessary to consider many provisions concerning the concept and individual elements of the structure of the science of forensic science from the standpoint of the knowledge available in this area.

According to the capacious definition of the British Encyclopedia (Encyclopedia Britannica), in its most general form, forensic science is the application of methods of natural and physical sciences to issues of criminal and civil law (Siegel, 2020), which very accurately indicates its applied, interdisciplinary nature, notes the adaptability and readiness to perceive the achievements of scientific and technical progress. Specific technologies, before finally entering the forensic toolkit, as a rule, went through a 'thorny path' from their creation to approbation and widespread use in practice. The same can be said, in particular, to forensic photography (second half of the 19th century) (Bulkina, Patskevich, 2006) and fingerprinting (between 19th and 20th centuries) (Avramenko, 2019). Currently, these technologies include photography and video filming that are deeply integrated into life, promising, and future-oriented phenomena of essentially the same order: artificial intelligence, neural networks, robotics, etc.

The current and possible consequences of the accelerating expansion of advanced technologies into the mechanism of functioning of the existing system of social relations are increasingly being discussed in the legal doctrine; it is natural that they, having a huge potential for use in forensic technology, with widespread implementation in practice, hypothetically, will qualitatively improve the efficiency of detection, disclosure, investigation, and prevention of crimes. Therefore, it should be concluded that the so-called. 'Digital forensics' is a highly relevant area of research today (Ushakov, 2020).

Methods

The methodological basis of the research was formed by the dialectical-materialistic method of cognizing reality, which made it possible to analyze individual points of view on the subject of research. Methods of analysis, synthesis, analogy, and generalization of scientific, regulatory, and practical materials, systemic interpretation of the law, legal modeling were also used, which in their totality made it possible to study the essence and content of Big Data technology through the prism of forensic science and practice. Besides, other methods were used: historical, comparative-legal, formal-logical, etc.

Contents

The effectiveness of detecting, disclosing, and investigating crimes directly depends on the quantity and quality of forensically significant information available for analysis, the sources of which are various (material, ideal and digital (virtual)) traces of a crime. Based on significance for the investigation in science, priority is given to its subspecies, actual forensic information, the concept of which covers factual information, data that are in a causal relationship with the event of a crime and characterizing the method of its commission, the personality of the offender, objects of criminal encroachment, instruments of crime, etc. (Filippov, Volynsky, 1998).

However, as Belkin R.S. (2000) rightly notes, information of any nature can be criminally significant. Consequently, all information that can become evidence in a criminal case or, in general, affect its resolution is of value. For example, the information accumulated in the system of criminal records contributes to the effective solution of diagnostic and identification tasks of the criminal investigation, the sufficiency of the evidence base. Currently, which is very significant, given the acceleration of technology development, the role of such a reference, i.e. indirect, not directly related to a causal relationship with a specific act, potentially forensically significant information in expert activities and criminal proceedings increases significantly.

It is obvious that of all sections of the science of forensic science, forensic technology has the broadest opportunities to integrate the achievements of many sciences to solve the problems it faces. This circumstance is based on the fact that such branches of this section as traceology, weapons science, photocopy, registration, and some others, maybe most in-demand in forensic activity in terms of their filling with the results of the achievements of some natural and technical sciences.

The branch of forensic technology, especially predisposed to the perception of the achievements of science and technology, is the system of criminal (forensic) registration, the purpose of which is to form a system of forensic records of certain objects - information carriers (sources - photographs, anthropometric measurements, description by the method of a verbal portrait, fingerprints and others (Tregubov, 2002)) used to disclose and investigate crimes (Chelysheva, 2017). Forensic registration, rooted in the ancient methods of punishing criminals in the form of mutilation (stigmatization and maiming) - usually for their subsequent identification - received rapid, but in many aspects extensive, rather than intensive development in the 20th and 21st centuries, expressed in a significant increase in the number of objects subject to accounting, as well as in the improvement of methods and methods of registration, the introduction of automated systems (a vivid example is the creation of genomic accounting in Russia in 2008 (Federal Law No. 242, 2008)). In this regard, it should be stated that by now forensic registration is an integral heterogeneous, complex structural formation, consisting of a set of several dozen records (Averyanova et al., 2001).

It should be noted that since, due to a significant increase in the volume of forensically significant information, the corresponding records are becoming more and more (Koisin, 2018) (this process, I think, will continue with a significant acceleration), it is logical that the criminal registration system needs to introduce more than just automated collection technologies, storage and systematization of information (this, as follows from the foregoing, is currently being successfully carried out), but also its resource-intensive effective analysis to further develop conclusions that are significant for the investigation and the court, which can be achieved by introducing various forms of artificial intelligence into forensic practice.

Within the framework of this study, we believe that the spread of Big Data (the so-called 'large, or complex, data', the term was introduced in foreign doctrine in 2008 (Lynch, 2008)) is of a certain interest both for the development of branches of forensic technology and for criminal proceedings; further BD-technology, which is based on a mechanism for collecting and processing large-volume, not directly interconnected structured and unstructured arrays of information from various sources, subject to constant updates, to improve the quality of decision-making (Savelyev, 2015). Based on this definition, BDs are understood in two meanings that make up a single whole: firstly, as a set of large segments of information that are different in content, and secondly, as a technology capable of processing it at relatively high speed (Volume, Variety, Velocity), which together ensures the admissibility of their use for analytics, modeling, and forecasting. Structurally, BDs combine, as processing methods and tools, in particular, data mining, machine learning, artificial neural networks, and other similar technologies that simulate human thinking (Manyika et al., 2011).

Back in the middle of the last decade, a topic devoted to the possibilities of using the technology in question in many spheres of public life becomes a popular topic in several media outlets. For example, there are claims that 'in the coming years, we are expecting a Big Data revolution in medicine, forensics, urban infrastructure, and other areas' (Schwarzkopf, 2014). Thus, it should be stated that the special properties of BD provide tremendous opportunities for optimizing various areas of life: production, commerce, government, medicine, and, of course, the law in all its manifestations as a form that mediates social relations. In other words, the directions for using BD are not exhaustive, since the technology is universal.

In the course of BD functioning, all available information is subjected to program analysis, regardless of its selection and quality (format, type), and within the framework of this process, the search for correlations dominates, and not the establishment of cause-and-effect relationships between data (Channov, 2018, p. 113). Consequently, the content of the conclusions obtained by this method is characterized by a high degree of reliability, but only under the condition of a proper selection of empirical material (which, as a rule, is compensated by its volume concerning the scale of the operating data, the so-called law of 'large numbers' applies: the more significant and the more relevant the data, the more accurate the conclusion, since the machine continuously learns from their analysis), and in most cases cannot be explained from the standpoint of formal logic, which makes it possible to extract new knowledge from existing information at a fundamentally different level of cognition and to reveal many previously hidden for logical analysis, patterns.

The above technical aspects of BD make it possible to form a certain understanding of the multiplicity of the consequences of the widespread introduction of technology into human life, which is especially important now because of the state stimulation of digitalization processes in Russia (Decree of the President of the Russian Federation No. 203, 2017). And since scientific and technological progress is irreversible, it is natural that BDs, due to their special properties, are of great interest to forensic science. Due to the synthetic nature of forensic science and its pronounced integrative nature, it is natural that by now there are many sources in the doctrine that describe the possibilities of bringing forensic scientific knowledge, and with it the achievements of investigation practice to a qualitatively new level through the introduction and use of the properties of artificial intelligence.

Thus, the widespread development of BD and similar technologies brings certain opportunities for the further development of forensic knowledge. This thesis can be illustrated in more detail by the following provisions.

First, it seems that the developed forensic approach to the legal regulation of BD technology is directly predetermined by its structural features. As noted above, BD can be conventionally divided into two types: structured and unstructured. The collection of the former, carried out following the established criteria, is initially subordinated to a specific goal (which distinguishes them from the latter). It must be stated that such structured BDs, provided that they are understood in the original sense only as a set of large segments of information systematized according to some characteristics, have been used for a relatively long time in forensic activities, in particular, in the automated fingerprint information systems ‘Papillon’, the functioning of which is carried out within the framework of the creation of an electronic database of fingerprints and traces for its further use for solving some practical problems:

1. Identification of identity by prints and traces of fingers and palms;
2. Identification of unidentified corpses;
3. Associations in the wake of crimes committed by the same person (Zaitsev, 2008).

In this regard, it should be concluded that the informatization of fingerprinting and other branches of forensic technology is a relatively old trend. The first pilot development of automated fingerprint systems was initiated in the USSR in the late 1950s. (Repin et al., 2012), and extensive automation of fingerprinting records in Russia was implemented in 2002: more than 20 million fingerprint cards of the Main Information and Analytical Center of the Ministry of Internal Affairs of Russia were optimized. Currently, checking one trace against the specified database takes several tens of minutes, which saves thousands of man-hours of working time (Wikipedia. Automation of fingerprint records, 2020). However, it seems that until now the development of forensic registration was carried out mainly in the vector of improving the methods of storing and organizing huge arrays of forensic data to increase the efficiency of an expert’s search for the necessary specific information. Therefore, we believe that it is the introduction of BDs that, based on the analysis of databases, can independently identify forensically significant correlations, draw high-precision conclusions based on them, and thereby significantly facilitate (but not replace and exclude) the work of experts the most promising direction in the development of the criminal registration system.

Secondly, it can be stated that in the activities of state bodies as a whole, the positive use of BD technology, understood in its full proper meaning (at the same time as a set of large data arrays and tools capable of processing them), is already being carried out. The sources provide data on the use of profiling, in particular, in foreign practice (the USA) for a preliminary assessment of the threat that each individual poses as a potential offender in the framework of predictive police control (Thompson, 2010). The purpose of the domestic automated centralized database of personal data (Rostransnadzor Database, 2019) on passengers and personnel (or crew) of vehicles is to identify passengers who should be checked and, if necessary, not allowed to travel to ensure safety.

Thirdly, it should be concluded that samples of artificial intelligence technologies to collect and process BDs for decision-making within the framework of expert practice are already being carried out and are showing significant results. In particular, as Bakhteev D.V. (2019, p. 106) notes, the Department of Criminalistics of the Ural State Law University is implementing a project aimed at creating an artificial neural network that performs a preliminary analysis of handwriting material (which, I think, can potentially be applied to the recognition of other objects) to identify signs of forgery of signatures made without the use of technical means, i.e. in this case, it should be stated about the development of the very possibility of making high-precision decisions, similar to those made by experts. The developed model, as noted above, is based on the use of artificial neural networks that reproduce the work of the human brain, due to which a transition from the linearity of traditional mathematical algorithms to adaptability, the heuristic nature of decisions made by the program is possible. The creation and tuning of the functioning of the BD system, built on these initial premises, consists of three sequential stages:

1. Collection of the necessary material (digitized experimental samples of signatures and their handwritten counterfeit copies);
2. Selection and adjustment of parameters, following which the objects will be compared when training the network (which are individual general and particular handwriting signs, the ratio of the slope angles of strokes, their horizontal and vertical lengths, etc., with a deviation from the normally established possible values the signature is considered fake);
3. Training the network and checking its operability (i.e. a pair of signature samples is presented, one of which is always genuine, the other is genuine or false, while the system knows the quality of the signature in advance, this operation is repeated several hundred thousand times).

As a result, the system recognizes the variation characteristics of signatures made by one person, and the differences that appear between original and forged signatures. At the final stage, the operation of the network is checked by presenting it with two signature samples, one of which is genuine, and the authenticity of the second is unknown, which brings its work closer to real conditions and meets the needs of practice (Bakhteev, 2019, p. 106). Thus, with high accuracy, the corresponding signs are revealed that distinguish between genuine and fake signatures, as well as characterizing the person who executed them, provided that the initial parameters were chosen correctly.

It seems that such tools in the future can be used in the forensic study of documents in general (not only in handwriting studies, but also, for example, in the author’s examination (Shatalov, 2015)), in forensic registration (i.e. based on the program analysis of structured databases, it is possible to draw criminally significant conclusions), in habitoscopy, traceology and other branches of forensic technology, since in this case it is also necessary to establish implicit patterns and correlations by constructing mathematical models, which are most effectively identified and investigated by BD, the functioning of which is based on the use of computer vision and artificial neural networks that mediate the process of recognition and subsequent analysis of patterns from available and, as a rule, unstructured empirical forensic material.

At the same time, the broad possibilities of using BD entail certain difficulties and risks of a conceptual and legal nature. Without going into the problem of identifying traces of certain types of crimes, wherever, based on the peculiarities of the investigation, the use of BD would be successful, we will try to characterize some of them available at the present stage. It is advisable to dwell on the obvious problems arising in relation to the process of proving in the implementation of the tasks set in this area.

Bessonov A.A. (2018) mentions that ‘the purpose of using big data in forensic science is to search in large volumes of information that are non-obvious, objective and useful for use in this science, the practice of investigating crimes and forensic activities of patterns and specific facts’.

It is quite obvious that in the modern conditions of public life transformation the above process of searching for patterns and specific facts necessary for the purposes and tasks of investigation cannot remain unchanged or, more correctly, qualitatively not change. Realizing this, and taking into account the complex nature of the problems arising in connection with this, we single out, in particular, the following ones.

The psychological aspect of the problem

One cannot but agree with the opinion existing in the psychology of investigative activity that ‘the professional activity of an investigator is characterized by procedural regulation of the means and timing of the investigation, cognitively - search orientation, efficiency, and conspiracy of actions, the need to overcome possible opposition of interested persons, the presence of power, a wide range of communications, increased personal responsibility for decisions made. It is also characterized by the diversity and creative nature of the tasks to be solved, a kind of combination of collegial and individual principles, lack of time for decision-making, the uniqueness of external conditions, and the presence of overloads in the investigator’s activities, as well as their procedural independence’ (Krugova, 2010).

In the context of the problem under consideration, from the above judgment, it should be especially noted the mention of the ‘creative nature of the tasks being solved’. For obvious reasons, the use of the capabilities of BD technology in investigative activities will have the aforementioned character for some time. From this follows the predicted very limited use of the technology under consideration by the subjects of proof in the absence, unfortunately, of many of them of this nature in solving problems.

The reason for this attitude (especially among investigators with a long experience of investigative work) lies, among others, in the unwillingness to learn something new in a short time, respectively, the desire to preserve the usual algorithm of investigative activity, consisting of long-known and approved by the subject of procedural and non-procedural actions aimed at solving everyday problems.

In this regard, we should also mention the subjects of forensic activity, which, as it seems, will look more advantageous in comparison with investigators in terms of using the opportunities under consideration, which is associated, among other things, with the peculiarities of obtaining an education and the specifics of subsequent work in the profession.

The ethical aspect of the problem

Back in the early 2000s, the literature noted that ‘in recent years, various kinds of publications describe the problem of legal and moral insolvency of law enforcement in general and criminal procedural activities in particular, which allegedly is a source of massive violations of the law, about the allowed in this activity not quite morally clean methods’ (Antonov, 2003).

Indeed, at all times, one of the most important, and at the same time sometimes difficult to solve in practice, problems are the observance of ethical standards in the conduct of an investigation. The emphasis on this aspect of the problem is not at all accidental: the previously mentioned opening prospects in the possession and use of an array of information hitherto unknown to the investigation creates the basis for its abuse in solving any problems and at all stages of criminal proceedings. And, again, as in the case of the psychological aspect, there are reasonable assumptions that all this may to a greater extent affect the procedural figure of the investigator.

Institutional problems

If, about structured BDs, there is an insignificant number of problems of their legal regulation (there is precisely a lack of factual nature: the development of this group of data depends mainly on the lag in the implementation of scientific and technological progress in forensic practice), then concerning unstructured BDs, the opposite can be stated. Unstructured BDs, which include, in particular, multimedia (a combined combination of video, sounds, text) transmitted by cellular and Internet operators (Meshcheryakov, Khorunzhiy, 2018), can also be used in the expert, operational-search, and investigative activities since there is a possibility that contains potential forensic information.

The collection and processing of unstructured data at the initial stage are carried out without regard to the goals and interests of law enforcement agencies. But if the need arises, they can be used to analyze the behavior of individuals and their groups, to identify and track the movement of the offender, their actions (Bakhteev, 2019, p. 105). Biometrics, based on BD technology and aimed at recognizing and identifying people by their physical and behavioral traits, is increasingly being introduced into forensic activities (Barkovskaya, 2011). In general, as follows from the analysis of existing practice, unstructured BDs are used by various, both private and public actors in the profiling process, i.e. collection of information about individuals (personal data) for its further use (including a commercial one (Larionova, 2018)), while often these actions are carried out without ascertaining the consent of the investigated person.

It must be stated that the digitalization process has revealed a deep conflict between the requirements for the protection of personal information and the actual impossibility of complying with them if it becomes publicly available. As Talapina E.V. (2018) rightly notes, there is an increase in contradictions between private and public principles in law, openness and closedness of information, transparency, and secret private life. Therefore, it is natural that the above-described ways of using BD cause the emergence and aggravation of a conflict between the interests of individuals and the state (as well as various organizations) using technology in their activities, in the aspect of a possible violation of the fundamental constitutional right of specific individuals to privacy (and a derivative of his rights to the protection of personal data), which is especially relevant to unstructured BDs, which are often collected without the knowledge of the person and can be used in forensic activities.

Indeed, the unrestricted collection and processing of personal information by BD technology are, in essence, contrary to the key principles of the Federal Law ‘The Protection of Personal Data’ (2006, July 27). In particular, BDS is incompatible with the principle of limiting the processing of personal data to predetermined purposes established in the above law (Article 5), since when they are applied, due to the technical properties and the very purpose of the technology, as a rule, all information about the person which available to the state or organization is processed, including those collected earlier for other purposes. And, therefore, BD also contradicts the concept of informed, specific and conscious consent as the main basis for legitimizing the processing of personal data, since its key element - awareness - consists in providing and understanding an exhaustive list of purposes for which the information obtained as a result will be used the action of technology, which is difficult to ensure in practice. Finally, the depersonalization of personal data is not a guarantee of their anonymity in the era of modern technologies, because BDs allow with a high degree of probability to identify the identity of a specific person by establishing correlations between pieces of data of a different nature (there is no need to know, for example, name, date of birth, etc.) information) (Santos, 2020).

Results

Thus, the uncontrolled, not limited by law, the use of this technology both in public practice in general and in forensic activity in particular, brings certain threats to human rights and freedoms, which necessitates the advance development of appropriate legal regulation.

It should also be noted that, hypothetically, it may be illegal not only to collect and process information directly or indirectly related to a person (including a potential forensic value). It is quite obvious that, due to the technical features of BD, in practice, it is possible to make incorrect and illegal legally significant decisions based solely on logically unconfirmed conclusions obtained as a result of the use of technology, or abuse of their use, which violates the general legal principle of formal equality. And since profiling based on the identification of characteristic associations with a particular person makes it possible to predict his behavior, theoretically there is a threat of infringement of constitutional rights, freedoms, and legitimate interests of citizens based on highly accurate assumptions about their past or future behavior obtained as a result of using BD. The opinion is expressed that if there is a certain political will, it is possible both through preventive legal means to prevent a potentially possible unlawful act (which in general is a progressive way of using technology), and, before committing it, to proactively bring to legal responsibility, that is, to punish the person concerned for more an imperfect offense (Channov, 2018, p. 118), which is unacceptable from a legal point of view.

At the same time, it should be remembered that within the framework of public relations based on imperative principles, the sphere of dispositiveness, free discretion of the individual is significantly limited, which reduces the range of possibilities of the latter in the event of arbitrariness on the part of the law enforcement officer, and therefore, in our opinion, the process of spreading BD and other similar technologies in the practice of an expert and legal proceedings based on his conclusions requires a scientifically grounded, balanced approach.

Conclusion

Thus, it should be stated that the introduction of BD technology into forensic activity has tremendous prospects for development since it is hypothesized that it will increase the relevance of the acquired and processed forensic information, and, therefore, will significantly increase the chances of detecting, disclosing, investigating and preventing crime.

It seems that it is necessary to continue the development of an appropriate regulatory framework governing the relations developing in the use of BD, and the priority area of legal policy should be precisely the elimination of some problems and risks indicated above. In our opinion, it is necessary to legislate a general ban on decision-making by the subjects of law enforcement that generate legal consequences for citizens, which are based solely on automated data processing, since even a highly developed model that reproduces human thinking is capable of making a mistake with a low probability of making a mistake. In this regard, we consider it fair to agree with the position expressed in the legal doctrine that in several situations that may arise in practice, it may be necessary to introduce the requirement for the mandatory establishment of causal relationships that were not identified in the program analysis, and the proof of the conclusions made using logical reasoning (Channov, 2018, p. 121).

The above, however, clearly cannot serve as an exhaustive solution to all the problems of legal regulation of BD, which requires further scientific research in the vector of finding a balance between a decision made in a fully automatic mode and a decision made by a person.

Surely, in the foreseeable future, the analyzed technology cannot and should not replace the subject of law enforcement, fully determine its legally significant decisions. Its purpose is to serve as a special tool for an investigator, an expert, capable of independently generating forensically significant conclusions, which will allow him, taking into account other available data, to significantly facilitate the adoption of the final decision. Therefore, with the positive development of BD, we can talk about optimizing the speed and quality of work of the above persons, and, ultimately, about reducing the negative impact of the human factor in forensic practice by transferring a part of the predominantly 'mechanical' functions of an expert to the information system, which has already been, as follows from the above, has several specific forms of expression.

References

[1]. Antonov, I.A. (2003). *Nravstvenno-pravovye kriterii ugolovno-protsessualnoy deyatelnosti sledovateley* [Moral and legal criteria of criminal procedural activity of investigators]. St. Petersburg: Legal Center Press. P. 118. In Russian.

[2]. Averyanova, T.V., Belkin, R.S., Korukhov, Y.G., Rossinskaya, E.R. (2001). *Kriminalistika:uchebnik* [Forensic science: textbook]. In R.S. Belkin (ed). (pp. 368–385). Moscow: Norma. In Russian.

[3]. Avramenko, O.I. (2019). *Istoriya razvitiya daktiloskopii kak metoda identifikatsii lichnosti i ee sovremennoye sostoyaniye v Rossii* [The history of the development of fingerprinting as a method of personal identification and its current state in Russia]. *Concept*, 11, 140. In Russian. https://doi.org/10.24411/2304-120X-2019-13070

[4]. Bakhteev, D.V. (2019). *Bolshiye dannye i iskustvennyi intellekt v sledstvennoy i ekspertnoy deyatelnosti* [Big data and artificial intelligence in investigative and expert activities]. Actual problems of criminalistics and forensic examination: materials of the International Scientific and Practical Conference. (Irkutsk, March 15-16, 2019, pp. 104-107). Irkutsk: East Siberian Institute Ministry of Internal Affairs of Russia. In Russian.

[5]. Barkovskaya, E.G. (2011). *Kriminalistika i biometriya: problemy integratsii nauchnogo znaniya* [Forensics and biometrics: problems of integrating scientific knowledge]. *Philosophy of law, 3*(46), 27–31. In Russian.

[6]. Belkin, R.S. (2000). *Kriminalisticheskaya entsiklopediya* [Forensic encyclopedia]. Moscow: Megatron XXI. In Russian.

[7]. Bessonov, A.A. (2018). *Ispolzovaniye bolshih dannyh v rossiiskoy kriminalistike: sovremennoye sostoyaniye i perspektivy* [Use of Big Data (BIG DATA) in Russian Forensic Science: Current State and Prospects]. I Minsk Forensic Readings: materials of the International Scientific and Practical Conference. (Minsk, December 20, 2018, pp. 56-61). Minsk: Academy of Ministry of Internal Affairs. In Russian.

[8]. Bulkina, N.V., Patskevich, A.P. (2006). *Istoriya vozniknoveniya i razvitiya kriminalisticheskoy fotografii* [The history of the emergence and development of forensic photography]. *Bulletin of Polotsk State University. Series D: Economic and Legal Sciences*, 8, 232–233. In Russian.

[9]. Channov, S.E. (2018). *Bolshiye dannye v gosudarstvennom upravlenii: vozmozhnosti i ugrozy* [Big Data in Public Administration: Opportunities and Threats]. *Journal of Russian Law, 10*(262), 111-122. In Russian. http://doi.org/10.12737/art_2018_10_11

[10]. Chelysheva, O.V., editor. (2017). *Kriminalistika: uchebnik* [Forensics: textbook]. Sankt-Peterburg: R-KOPI. In Russian.

[11]. Decree of the President of the Russian Federation No. 203. (2017, May 9). *O strategii razvitiya informatsionnogo obschestva v Rossiyskoy Federatsii na 2017-2030 gody* [Strategies for the development of the information society in the Russian Federation for the years of 2017 – 2030]. In Russian. http://kremlin.ru/acts/bank/41919

[12]. Federal Law No. 152 (2006, July 27). *Zaschita personalnykh dannykh* [The Protection of Personal Data]. In Russian. http://www.kremlin.ru/acts/bank/24154

[13]. Federal Law No. 242. (2008, December 3). *O gosudarstvennoy genomnoy registratsii v Rossiyskoy Federatsii* [State genomic registration in the Russian Federation]. In Russian. https://rg.ru/2008/12/09/genom-registracia-dok.html

[14]. Filippov, A.G., Volynsky, A.F., editors. (1998). *Kriminalistika: uchebnik* [Forensic science: textbook]. Moscow: Spark. In Russian.

[15]. Koisin, A.A. (2018). *Istoriya stanovleniya i razvitiya ugolovnoy (kriminalisticheskoy) registratsii* [The history of the formation and development of criminal registration]. *Siberian legal bulletin,* 2, 111. In Russian.

[16]. Krugova, N.V. (2010). *Psihologicheskiye osobennosti professionalnoy deyatelnosti sledovatelya kak subekta truda v khode proizvodstva sledstvennyh deystviy* [Psychological features of the professional activity of the investigator as a subject of labor during the production of investigative actions]. (Master's thesis). Tver. In Russian.

[17]. Larionova, V.A. (2018). *Informatsionnyi broker kak novyi subekt informatsionnogo prava v epokhu Big Data* [Information broker as a new subject of information law in the era of Big Data]. *Law in the field of the Internet: Collection of articles*. In M.A. Rozhkova (ed). Moscow: Statute, 2018. PP. 63-65. In Russian.

[18]. Lynch, C. (2008). Big data: How do your data grow? *Nature*, 455, 28–29. https://doi.org/10.1038/455028a

[19]. Manyika, J., Chui, M., Brown, B. et al. (2011, May 1). *Big data: The next frontier for innovation, competition, and productivity*. Report. McKinsey Global Institute. PP. 27–31. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation#

[20]. Meshcheryakov, V.A., Khorunzhiy, S.N. (2018). *Vliyaniye kontseptsii Bolshih Dannyh na kriminalisticheskuyu teoriyu prichinnosti* [Influence of the 'Big Data' concept on the forensic theory of causality]. Causality in criminalistics: a collection of scientific and practical articles. In I.M. Komarov (ed). Moscow: Jurlitinform. PP. 166-167. In Russian.

[21]. Repin, A.V., Loboyko, Y.D., Zyryanov, V.V. (2012). [The current state and problems of using automated fingerprint information systems 'Papilon' in the activities of the Federal Drug Control Service of the Russian Federation in the Krasnoyarsk Territory]. *Bulletin of the Siberian Law Institute Ministry of Internal Affairs of Russia, 2*(11), 69. In Russian.

[22]. Rostransnadzor Database. (2019, April 24). *Baza personalnykh dannykh o passazhirakh i ekipazhe avtobusov* [Database of personal data on passengers and crew of buses]. In Russian. https://smugadn.tu.rostransnadzor.ru/poleznaya-informacziya/baza-personal-nyx-dannyx-o-passazhi

[23]. Santos, J. (2020, January 25). The Myth of Anonymization: Has Big Data Killed Anonymity? https://docplayer.net/14450176-The-myth-of-anonymization-has-big-data-killed-anonymity-white-paper-by-jessica-santos-ph-d-march-2015.html

[24]. Savelyev, A.I. (2015). *Kommentariy k federalnomu zakonu ot 27.07.2006 №149 FZ Ob informatsii, ifnormatsionnykh tekhnologiyakh i zaschite informatsii (postateinyi)* [Commentary to Federal Law No. 149 of July 27, 2006. Information, Information Technology and Information Protection (itemized). P. 60]. Moscow: Statute. In Russian.

[25]. Schwarzkopf, A. (2014, January 16). *Big Data calls for a revolution*. In Russian. https://www.kommersant.ru/doc/2384586

[26]. Shatalov, A.A. (2015). *Modeli i metody vyiavleniya zakonomernostey v informatsionnom potoke na primere rukopisnogo teksta s tselyu ustanovleniya ego avtorstva* [Models and methods for identifying patterns in the information flow using the example of handwritten text in order to establish its authorship]. (Master's thesis). Tambov. 170 p. In Russian.

[27]. Siegel, J.A. (2020, June 01). Forensic science. *Encyclopedia Britannica*. https://www.britannica.com/science/forensic-science

[28]. Talapina, E.V. (2018). *Zaschita personalnukh dannykh v tsifrovuyu epohu: rossiiskoye pravo v evropeyskom kontekste* [Personal data protection in the digital age: Russian law in the European context]. *Works of the Institute of State and Law the Russian Academy of Sciences*, 5, 145. In Russian.

[29]. Thompson, T. (2010, July 25). *Crime Software May Help Police Predict Violent Offences*. The Guardian. http://www.theguardian.com/uk/2010/jul/25/police-software-crime-prediction

[30]. Tregubov, S.N. (2002). *Osnovy ugolovnoy techniki, nauchno-tekhnicheskiye priemy rassledovaniya prestupleniy* [Fundamentals of criminal technology, scientific and technical methods of crime investigation]. Moscow: LexEst. In Russian.

[31]. Ushakov, R.M. (2020). *Tekhnologiya Big Data kak vektor razvitiya kriminalisticheskoy tekhniki: perspektivy primeneniya v kontekste ikh pravomernosti* [Big Data technology as a vector for the development of forensic technology: application prospects in the context of their legitimacy]. *Ural Journal of Legal Research*, 2, 54–70. In Russian.

[32]. Wikipedia. (2020, January 19). *Avtomatizatsiya daktiloskopicheskikh uchyotov* [Automation of fingerprint records]. In Russian. https://ru.wikipedia.org/?curid=1134856&oldid=106677709

[33]. Zaitsev, P.A. (2008). *Prakticheskiye voprosy vybora effektivnoy avtomatizirovannoy daktiloskopicheskoy identifikatsionnoy sistemy (ADIS)* [Practical issues of choosing an effective automated fingerprint identification system]. *Forensic expert*, 2, 20. In Russian.