Legal Issues in the Digital Age. 2024. Vol. 5. No. 4.
Вопросы права в цифровую эпоху. 2024. Т. 5. № 4.

Research article
JEL: K00
УДК:34
DOI:10.17323/2713-2749.2024.4.46.72

Keystroke Dynamics: Prospects for Comprehensive Law Regulation

Anna Denisovna Tsvetkova

Ural State Law University, 21 Komsomolskaya Street, Ekaterinburg 620066, Russia,

at@crimlib.info, https://orcid .org/0000-0002-1631-9265

Abstract

The rapid digitalization of all spheres of society leads to the appearance of large volumes of typed texts, as well as the formation of the task of determining the performers of such texts. In this regard, it is necessary to develop applied research on keystroke dynamics, including through the prism of jurisprudence. Author of the article identifies sector of public relations related to ensuring the rights of citizens to personal and family secrets, the secrecy of correspondence; protection and processing of biometric personal data; state registration of persons based on their keystroke dynamics; disclosure and investigation of crimes in which typed texts are the subject of encroachment or the means of committing an illegal act; procedural proof of the involvement or non-involvement of a particular person with the creation of a typed text; as well as with the control of labor discipline and ensuring safety of production processes. In all these areas the beneficial fruits of processing keystroke dynamics is potentially high, that, however, is accompanied by significant risks of protecting information that is harmful to human persons. In this regard, author proposes models of regulatory regulation of all these areas in order to maintain a balance of public and private interests. The author's goal was to justify that the prompt resolution of the problematic issues raised would improve the effectiveness of law enforcement, protect the rights of citizens, and ensure the national security of the state. For this purpose, methods of logical definition of concepts, modeling, questioning, analysis and analogy, as well as systemic legal method were used. Conclusions were formulated about the prospects of both voluntary and mandatory

state registration of users of computer devices and the Internet on the basis of their keystroke dynamics at the expense of the resources of the Center for Biometric Technologies. With the help of information from this database, as well as through investigative actions and operational search measures, it is possible to introduce keystroke dynamics into the field of forensic identification of the typist. To do this, it will be necessary to conduct a computer-technical examination, the results of that may be used as the basis for procedural evidence. Automated processing of information about keystroke dynamic can be used to monitor compliance with the work and rest regime by employees, independently fulfill their employer's orders, and prevent accidents at the workplace. Based on the totality of all the considered aspects, it is concluded there is a need for a deep understanding of keystroke dynamics in various fields of jurisprudence. It permits to form a regulatory system for the integrated regulation of public relations related to the processing of this phenomenon.

Keywords

keystroke dynamics; digitalization of law; digital forensics; personal rights; biometric personal data; behavioral biometrics; state registration; computer forensics.

Acknowledgments: The study was funded by grant of the Russian Science Foundation No. 23–78–10011, https: // rcf.ru/project/23-78-10011

The paper is published within the project of supporting the publications of the authors of Russian educational and research organizations in the Higher School of Economics academic publications.

For citation: Tsvetkova A.D. (2024) Keystroke Dynamics: Prospects for Comprehensive Law Regulation. Legal Issues in the Digital Age, vol. 5, no. 4, pp. 46–72. DOI:10.17323/2713-2749.2024.4.46.72

Introduction

Our lives go hand in hand with digital technologies. We use them for quick interpersonal communication, for entertainment, to resolve working questions, to contact government bodies, for education etc.—the list seems to be endless. As a result of this trend, the very concept of society and social interactions has been undergoing changes, and this definitely has its influence on laws and regulations. Progress in science and technology has been transforming individual spheres of law to one degree or another, in particular as new phenomena appear in our life that don't fit into the usual regulatory framework, but by their nature should be subject to legal regulation.

One example of such phenomena is operations in the digital environment related to the creation and dissemination of text materials. This in-

cludes, first of all, written (or, to be more precise, typed) Internet communications and work in computer programmes and interfaces where texts are keyed in (word processors, forms for filling in and submitting electronic reports, administration of websites and filling them with content, etc.). In any of the aforementioned cases, the computer device records the unique set of the user's skills and habits, the person's keyboard dynamics. This phenomenon reflects how the person works on the keyboard rather than what information this person types in [Zeid S., ElKamar R., Hassan S., 2022: 95]. Researchers in the information technology and information science spheres have been studying this phenomenon since the 1970s [Spillane R., 1975]; [Forsen G., Nelson M., Staron R. Jr., 1977: 116–122]. They have proven that keyboard dynamics are important for identification purposes and belong to the category of behavioural biometrics; analysed the nature of the phenomenon in sufficient detail; developed numerous ways to record and automatically process them, and designed special technical media for this. At the same time, jurisprudence has not paid enough attention to the questions of keyboard dynamics, their use and protection. This, author of article presented believes, is a major oversight, in particular in the times when electronic texts are becoming increasingly common.

Therefore, the research focuses relations in the sphere of keyboard dynamics processing[1] through a legal lens. Author considers various approaches to legal regulation of issues pertaining to this phenomenon in the sphere of material public relations, private-public relations, and procedural relations, and in this manner will outline the directions for further in-depth studies on this topic.

The aim follows from the hypothesis that electronic texts will only grow in amounts in the future and will gradually displace manuscripts. As a result, the need to identify clearly the author of a particular typed text will arise in various areas of life on a regular basis. Hence, even today it is sometimes necessary to assess the potential positive effects, risks, and limits of keyboard dynamics from a legal perspective.

To this end, it is used an extensive methodological base including exploration of fundamental studies on the theory of identification, physiol-

[1] Processing is understood in this paper as set out in Federal Law On Personal Data No. 152-FZ of 27.07.2006 (Collected Laws of the Russian Federation. 2006. No. 31. P. 3451): as any action (operation) with personal data, including collection, recording, systematisation, accumulation, storage, clarification (updating, modification), retrieval, use, transfer (distribution, provision, access), depersonalisation, blocking, deletion, and destruction.

ogy of higher nervous activity, biometrics, information security, protection of human rights and use of personal data; current laws regulating relations in the sphere of processing personal, in particular biometric, data; labour relations; issues of state registration activity management; it was also collected own empirical material by polling law enforcement officers on their awareness of keyboard dynamics phenomenon and their views on how it can be studied for solving the tasks facing justice. In the research it was used the system legal method as the main special method that allowed to consider the single phenomenon of keyboard dynamics from different positions. Also, author have relied to a large extent on the methods of mathematical statistics, cybernetics, programming, and system analysis, without which it is impossible to comprehend a phenomenon that for many years has been the subject of research exclusively in the computer science domain. Forecasting and modelling methods enabled to describe the situations in which it would be necessary to subject to legal regulation the relations in the sphere of the keyboard dynamics processing and to propose optimum ways for such regulation. In addition it was used the general research methods of analysis, synthesis, induction and analogy, as well as the universal dialectical method, that allowed to organize the research on basic scholar principles.

1. Keyboard Dynamics: Definition

It was mentioned above keyboard dynamics were initially studied in the sphere of computer science, so it would be reasonable to borrow its definition from the works of researchers of this discipline. At the same time, despite the long history of research on the subject, there is still no single definition; foreign researchers, omitting the direct definition of keyboard dynamics, go straight to the description of its essence and possibilities of its applied use.

Author will not dwell in detail on the whole variety of the definitions. Instead, it was cited the most representative examples reflecting the approaches to the definition of this phenomenon. These may be divided into three groups:

definitions by means of listing the features that are specific to keyboard dynamics;

definitions in which representation is made through genus and species distinctions,

definitions by means of pointing to a synonymous category .

It is possible to assign to Group 1 the detailed description offered by A.I. Averin and D.P. Sidorov: "In the process of keying information in, a person develops his or her own personal style of typing certain words. This style is actually unrepeatable and depends on such parameters as the number of fingers involved in typing; the duration of key presses; the time between key presses; the use of the main or additional part of the keyboard; the nature of double or triple presses; the favourite combinations of hot keys, etc. Thus, keyboard dynamics is a set of dynamic characteristics of work on the keyboard" [Averin A.I., Sidorov D.P., 2015: 2].

S.A. Varlamova's and E.A. Vavilina's definition is an example of Group 2 definitions: "Keyboard dynamics is the dynamic human of a person that depends on the speed of character input, the time interval between releasing and pressing a key, as well as the interval between key presses (i.e., the time it takes to press neighbouring keys), the number of typos, and the use of hotkey combinations" [Varlamova S.A., Vavilina E.A., 2023: 68].

E.E. Turutina offers a notable example of a definition that belongs to Group 3: "Keyboard dynamics is an individual biometric characteristic of each individual user's behaviour" [Turutina E.E., 2021: 171].

Obviously, only individual examples are cited above, but analysis of other authors' works shows their definitions differ only slightly from the cited ones. At the same time all definitions of keyboard dynamics formed in science today, including those not mentioned, have one or more of the following drawbacks.

Susceptibility to obsolescence. This is characteristic of keyboard dynamics feature listing models because owing to the progress of science, new properties significant for identification are revealed or the irrelevance of the previously highlighted features is proven on a regular basis.

Incompleteness. Many definitions specifying characteristics of keyboard dynamics or give its generic differences, do not provide an exhaustive list of these characteristics.

Uncertainty. In an attempt to avoid the above-mentioned shortcomings, some authors add 'etc.' at the end of the definition; it raises quite a number of questions related to the content of this expansive provision.

Identification of the general and the particular. Some definitions equate keyboard dynamics, a complex systemic phenomenon, with its individual dynamic characteristics. However, a system cannot be reduced to a simple sum of its components.

Vagueness. When researchers list individual features of keyboard dynamics, they don't answer the question as to what it is. When trying to refer to a generic category, the specialists miss distinctive characteristics that would allow to distinguish keyboard dynamics from related phenomena.

These are only the main common disadvantages. If to go into a detailed analysis of each definition, this list could be continued. However, the examples demonstrated are sufficient to conclude the current definitions cannot be recognized as optimal ones.

For the purposes of jurisprudence, proceeding from the above positions and taking into account the shortcomings highlighted therein, author of the paper presents proposes the following definition below:

Keyboard dynamics: in the subjective sense, it is a biometric characteristic of a person, which combines a set of skills and habits of the user's interaction with a keyboard equipped with tactile symbolic keys while creating a text; in the objective sense (also, "keyboard dynamics information"), it is the external expression of the user's skills and habits of interaction with a keyboard equipped with tactile symbol keys when creating a text, which is manifested in relevant records both directly on the user's device and (if available) in specialised software or hardware-software systems.

2. Keyboard Dynamics from the Human Rights Perspective

Researches show keyboard dynamics describes through a set of diverse characteristics [Alsultan A., Warwick K., 2013: 2–4], how a person types. Although the content of the text typed does not matter for its identification significance, present-day technical means of fixing keyboard dynamics—keyloggers—function in such a way that they record all keyboard events, i.e. information about which key was pressed (released), and when [Matsubara Y., Samura T., Nishimura H., 2015: 230]; [Villani M., Tappert C. et al., 2006: 33]. Thus, even if the system records not the character transmitted to the monitor, but the ASCII code of the key, it will be quite possible to restore the original text, if necessary, and thus to get information on what's been typed. As a consequence, ever since keyloggers appeared, one of their uses has been to covertly (often, maliciously) monitor the information typed on a particular computer device. This has branded them as malicious software [Samsoni D.Z., Basir B.P., Hafidsyah P. et al., 2023: 869–870]; [Md A., Mohiuddin S., Jafrul H. et al., 2019: 18]; [Guryanov K.V., 2020:

81–82]. To protect the information valuable for the user, researchers suggest configuring the key logger in such a way that the final data recipient receives only generalised information characterising the person's profile, thus excluding the possibility of recovering the data typed [Paschenko D.V., Balzannikova E.A., 2020: 78]. Fully justified from a privacy perspective, this proposal mitigates the benefits of a key logger that can be used for law enforcement purposes when it is necessary to match typing and text features. It will be discussed in detail below. In this regard, it is very important to identify ways to balance between the interests of the individual and the state.

Individuals seek to keep secret any information about themselves and their lives, its attitude is supported by the relevant constitutional (Art. 23 of the Constitution of the Russian Federation), conventional (Art. 8 of the UN Convention of 4.11.1980) and other treaty norms at the national and international levels [Isaeva V.V., Sakharova Y.V., 2020: 139], reflecting the human rights to personal and family privacy, and confidentiality of correspondence. Moreover, with the widespread use of network services (in particular, the Internet), any secret may become known to an unlimited number of third parties at once, which makes the above rights even more important.

On the other hand, the unlimited nature of the above rights to personal privacy, correspondence and negotiation secrecy poses a significant threat to national security, as it allows perpetrators to conceal unlawful activities until the moment when it becomes impossible to prevent their consequences. In view of this, the legal provision establishing the rights in question also allows for their restriction by court order.

Taking it into account, it is admissible to believe in researching keyboard dynamics one ought to preserve the possibility of correlating its features with what was typed, if such a study is carried out under a court order, as part of an investigation, law enforcement intelligence operations, and in other similar cases. In all other cases, processing keyboard dynamics without consent from the person in question is inadmissible.

At the same time, however, today various commercial companies use keyboard monitoring without the direct purpose of collecting personal information, but, e.g., to develop customer-oriented products[2]. Such a pos-

[2] McAllister N. Windows 10's 'built-in keylogger'? Ha, says Microsoft — no, it just monitors your typing. The Register. 7.10. 2014. Available at: https://www.theregister.com/2014/10/07/windows_10_data_collection/ (accessed: 19.07.2024)

sibility is enshrined in the companies' policies, and the user is asked to give his or her consent. The practice is that only a small number of users study such documents. And, moreover, almost nobody does it to find the provisions concerning the processing of keyboard dynamics, due to unawareness of the existence of this phenomenon. Thus, the undefined (and, in fact, absent) legal status of keyboard dynamics leads to the formation of a grey area, when the insufficiently high level of the population's computer literacy and the absence of strict rules for keyboard dynamics processing lead to the actual violation of human rights. In The following chapters will look at possible solutions to the problem from different perspectives.

3. Keyboard Dynamics in the Biometric Personal Data System

All studies of keyboard dynamics point out it is a behavioural biometric characteristic [Vacca J.R., 2007: 27]; [Uimin A.G., Morozov I.M., 2022: 48].

To substantiate this statement, it has a sense to turn to the doctrinal interpretation of the biometric data category (however, it is necessary to note it offers a definition, which is somewhat broader than the one given in Art. 11 of the Federal Law On Personal Data mentioned above[3]. E.g., it states personal biometric data must meet two criteria: "First, <they> characterise the physiological and biological features of a person, on the basis of which it is possible to establish his / her identity and, second, they are used by the personal data operator to establish the identity of the person" [Salikov M.S., Nesmeyanova S.E., Kolobaeva N.E et al., 2022: 116]. It is important according to this definition that biometric personal data will only include information that is actually used for identification and not theoretically suitable for it. It may be the reason why keyboard dynamics is still outside of legal regulation: it is not in widespread use. However, it is used for identification and authentication of computer device users at the private level and in various commercial entities [Mashtanov P.N., Martynyuk M.V., 2021: 527–531]; [Banerjee S.P., Woodard D.L., 2012: 129–131]. The prospects for its wider application have already been covered many times in doctrine [Alsultan A., Warwick K., 2013: 7–9]; [Shadman R., Wahab A., Manno M. et al., 2023].

International sources formulate slightly different requirements. E.g., biometric personal data should be: universal; unique; stable; irreplaceable;

[3] Available at: URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (accessed: 21.07.2024)

suitable for recording and storage; sufficient for identification; accurate; easy to process; economically feasible; convenient to process; socially acceptable [Clarke R., 1994: 21].

As it is possible to see from the description above, not all requirements are related to biometrics per se. E.g., voice recordings and facial images, that many parties, including federal laws[4], indisputably recognise today as personal biometric data, would retain their uniqueness in describing the relevant behavioural and physiological properties of a person, even if there were no relatively cheap ways of their easy acquisition and fast automated processing. That is, most of the items in the above list of biometric data requirements relate to data processing technologies and public policies that determine social acceptability.

So, it is possible conclude both the Russian and international approaches point to the need for scholar research, legal regulation and practical use only of the unique features of a person that can be separated from the person for subsequent manipulations; the features that belong to the person but can't be exported to an external tangible medium are of no interest to science, law, and practice. While author is not challenging the approach, she believes it is worth mentioning keyboard dynamics meets most of the above requirements, and it is only a matter of time and efforts on the part of researchers to create relatively affordable and widespread devices to record and process it. Hence, it ought to be studied from the legal perspective already today.

Therefore it is necessary to introduce normative regulation for relations in the sphere of processing keyboard dynamics data, in particular their storage and access to them as this is information subject to special protection. This is particularly relevant due to the fact that commercial entities "are also interested in collecting and processing personal data in order to create new business models, personalise the goods and services provided, make the most effective use of innovative technologies in competition, and protect their own interests in dispute resolution" [Zuyev S.V., 2019: 78]. E.g., information about keyboard dynamics is used to develop easier-to-use, ergonomic keyboards (which creates a competitive advantage in the market of

[4] Federal Law On the identification and (or) authentication of individuals using biometric personal data, on amendments to legislative acts of the Russian Federation and invalidation of certain provisions of legislative acts of the Russian Federation No. 572-FZ of 29.12. 2022 (Part 4 Art. 3) // Collected Laws of the Russian Federation. 2023. No.1. Part I. `P. 19.

computer hardware components), to ensure information security in banks, etc. As long as the status of keyboard dynamics is not formally defined, as was stressed above, its use is not restricted in any way. This may violate fundamental human rights.

One of the possible measures to resolve the legal vagueness in question is to enshrine in the legislation the list of personal biometric data, which is quite clearly given in doctrine [Vacca J.R., 2007: 27]; [Zhukov M.N., 2021: 164–165]. It should be done not necessarily at the legislative level: technologies keep developing, so one can't rule out that a new way is invented to process a particular new characteristic that hasn't been described yet. It is possible and sufficient to regulate it at the level of subordinate legislation. Currently, Ruling of the Russian Federation Government of 1.04. 2024 No. 408 On the types of biometric personal data are covered by Law On the identification and (or) authentication of individuals using biometric personal data, on amendments to legislative acts of the Russian Federation and invalidation of its provisions is in force in Russia.[5] It stipulates the Federal Law in question applies to human facial images and voice recordings. Hence, it is possible to establish a general list of biometric personal data by bringing them under a specific legislative regulation in the Russian Federation Government Ruling, too.

The question under review can be resolved in a different way as well. E.g., we believe in the initial phase, it would be sufficient for the Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications to issue Clarifications that would attribute keyboard dynamics to the personal biometric data category as it was the case previously with photographic and video images, and fingerprint information[6].

If the proposed measures are taken, everything related to the processing of keyboard dynamics will fall under the relevant provisions of Federal Law No. 152 regulating both general questions of personal data protection

[5] Collected Laws of the Russian Federation. 2024. No. 15. P. 2042.

[6] Clarification of the Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications "On issues of attributing photo and video images, fingerprint data and other information to biometric personal data and peculiarities of their processing" // Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications. 02.09.2013. Available at: URL: https://25.rkn.gov.ru/news/news54167.htm (accessed: 17.07.2024)

and particular aspects of operations with biometric identifiers, which are stricter.

At the same time, as legal studies on keyboard dynamics develop and deepen, there may arise the need to approve the Federal Law On state registration based on keyboard dynamics features. The study of this issue in detail is in the next section of paper. Suffice it to say here that the significance of this registration is explained by the fact that at present any person can create lots of typed texts (posts in social media, comments on various web resources, formal requests to government institutions, texts relation to the persons' education or work, etc.). These texts constitute the persons' digital profile (i.e., a unique set of characteristics, from the avatar selected to particular features of verbal communication typical of a particular person in the virtual domain [Ivanov V.V., Zuyev D.I., 2022]). This profile can be used to ascertain the identity is important for investigating crimes, identifying various offenders and solving other tasks, which will be discussed in more detail below. And it is specialized records that will be the best source of obtaining information about the properties of the "digital twin" to identify the real person behind it.

Considering issues that pertain to formalizing status of keyboard dynamics touch upon another issue: where it should belong. E.g., Russian literature on biometric data has traditionally broken them up into two categories: the static (anatomic) biometrics, and the dynamic (behavioural) biometrics [Shangina I.Y., 2020: 152]. In international literature, the dichotomy "physiological vs behavioural characteristics" prevails [Guo J., Mu H. et al., 2024: 209]. At times, one can come upon slightly different approaches [Syed Idrus S.Z., 2014: 2], but the behavioural biometrics group keeps its name and content, including the keyboard dynamics. The Russian legislator, in defining personal biometric data, divides them into two groups: physiological and biological characteristics, which obviously does not correlate with provisions of science.

Also, no explanation is given anywhere of what "physiological" or "biological" characteristics are. The Dictionary of the Russian Language proposes the following definition:

"Biological: relating to physical or physiological aspects of the existence of living organisms[7]."

[7] Kuznetsov S.A. The Great Explanatory Dictionary of the Russian Language. Saint Petersburg, 2000. P. 78.

"Physiological: relating to the physiology of the body, or its vital activity; based thereupon[8]."

While not giving here all the meanings of the words, but the remaining ones can't be related to biometric characteristics.

So, biological and physiological are almost synonymous. Moreover, if to turn to the experience of foreign researchers, it is easy to establish under physiological biometric data they understand static features (fingerprints, facial image, etc.), and the term "biological" can't characterise the features that are manifested in the process of activities (behaviour). The legislator has essentially split one type of biometrics into two synonymous words, ignoring the layer of dynamic identifiers — it is probably a technical error. The state processes behavioural biometrics as it records voices in the Unified Biometric System. Therefore, it is necessary to amend Part 1, Art. 11 of FZ No. 152 to read as follows: "1. Information that characterises a person's physiological and behavioural features, which enable to establish his/her identity (personal biometric data) and which the operator uses to establish the identity of the holder of personal data, may be processed only with the written consent of the holder of personal data, except in cases provided for in Para 2 of this Article."

Until such changes are made, the definition of keyboard dynamics should be given without species attribution, simply by means of the category "biometric characteristic of an individual."

Going back to the applied aspects, it has to note the state is interested in the processing of keyboard dynamics data, and therefore it is necessary to consider their storage. To this end, a special government database must be established. Perhaps, the optimum solution would be to allocate space in the Unified Biometric System as this will enable accumulating data collected not only by government agencies but also by commercial entities. It is particularly relevant because as of April 2024, after Government Ruling No. 408 was passed, it is now legally possible to expand the list of biometric personal data processed by the System. Relying on the System's resource capacities helps to guarantee the security of information, to use latest licensed domestic technical means for its processing, and to provide access to the keyboard dynamics of representatives both of public and private sector entities (if such a possibility is provided).

[8] Ibid. P. 1422.

The legal experts need to extensively explore peculiarities of keyboard dynamics processing from the point of view of its representation as a biometric characteristic to ensure that such processing is possible in applied activities.

4. State Registration on the Basis of Keyboard Dynamics Features

Very probably such registration through the resources of the Biometric Technology Centre (UBS operator[9]) or on the basis of an individual stand-alone database will significantly increase the force of the fight against crime, and control over content distributed on the Internet; i.e., it will ensure the national security of the state. At the same time, it will make it possible to withdraw from various organisations the bits and pieces of "sensitive" information that they store thus increasing its security in the interests of IT system users.

It is a place to present view on the individual main aspects of how state registration is to be implemented on the basis of keyboard dynamics. After appropriate additions and extensions, they may in the future form the basis of a corresponding Federal Law.

The state registration in question can be both voluntary and mandatory. The latter would be related to a conscious decision by an individual based on his/her wish to prevent potential falsification of his/her role in the creation of any typed texts, and by other personal motives. Surely, for law enforcement purposes the option of having a significant part of the population voluntarily register for keyboard dynamics is preferable. However, the practice established in the field of fingerprinting and genomic registration [Solomatina E.A., Cherkashina A.V., Dreval B.V., 2021: 237] indicates probability of that scenario is low. At the same time, there are situations where it is appropriate to resort to mandatory registration based on keyboard dynamics features. It must cover the following persons:

suspected or accused of committing an offence where a typed text is the means of committing it or the object of the offence;

[9] RF Government Ruling No. 834 of 21.06. 2024 On Determination of the Organization Functioning as Operator of the Unified Biometric System. Available at: URL: https://www.consultant.ru/document/cons_doc_LAW_479247/ (accessed: 21.07.2024)

who have committed an administrative offence where a typed text is the means or subject of the unlawful infringement;

authorized to work with legally protected information stored and processed in electronic form;

involved in fulfilling functions of the state through e-government structures (persons processing and/or registering incoming applications, interacting with applicants, preparing official responses, etc.);

wishing to use a digital platform involved in an administrative offence or through which a crime has been committed, where typed texts have been the means or object of infringement.

The list may be expanded and refined through further research. However, at present it is final. Above it was comments on its individual items, now it is a time to clarify registration based on keyboard dynamics, that is a behavioural characteristic, can be carried out in two ways: continuously or intermittently

In the former case, it was shown there is a risk of infringement on the rights to personal and family privacy, confidentiality of correspondence, and other unique information, and it was stated it was necessary to indirectly attribute, based on the dynamics, to the device used to create the text. Here, it is implied that the keyboard dynamics is recorded continuously, at pre-set intervals (e.g., once a day), and the data are then submitted to the government database. This approach is considered favourable; it helps to record a person's involvement or non-involvement in the creation of a text and guarantees the user profile is updated regularly and the variability of typing parameters is recorded. On the other hand, it is highly vulnerable from the technical viewpoint as it requires huge amounts of memory to store all the data, and computing capacity to process and select the required data, and does not guarantee the correct answer to questions of a person's involvement in the creation of a text generated on a different, unregistered computer device.

The former case implies a person's keyboard dynamics is collected for recording only once, and then updated from time to time (e.g., when the person is detained again in accordance with a legal procedure). The samples thus received are then attributed to a concrete person because they are collected in specially created conditions when the text is typed in under supervision, so the samples are definitely clean of any personal information. These data are then used to form the person's profile, and it is automatically

compared in other electronic systems. In other word, this model functions on the basis of automated authentication where information about the keys pressed is presented in human-readable form exclusively at the moment of state registration. In this scenario, the above-described technical problems are resolved, but the possibility of obtaining free samples of keyboard dynamics for a comparative study reduces almost to zero.

These forms of registration should be combined in a reasonable manner.

Public sector workers (persons belonging to Categories 3 and 4) can be registered in two steps: first, when they are hired, they type texts of a certain size; these samples then form the basic employee profile. After that, their activities on computer devices are constantly monitored, and the system automatically checks the features of the keyboard dynamics for their correspondence to those recorded in the beginning and included in the employee profile. The initial samples are stored in the state database, but the periodic data is not uploaded there. If, at a certain point in time, the system sees that the keyboard dynamics on a certain computer device issued to a particular employee don't match the stored profile, then the department manager receives a notification-request to react to this incident properly. In our opinion, to keep the precision of automated identification at a high level in this scenario, it would make sense to update employee profiles stored in the state database regularly.

As for persons undergoing criminal or administrative proceedings (Categories 1 and 2), it is preferable when both registration methods should be implemented at the same time: one, when the person is accused of a crime, is assigned the status of a suspect, or of a person held administratively liable; and two, the person's keyboard dynamics must be constantly related to the main computer device this person uses. Then, even if the person changes the device, it will still be possible to establish his/her involvement in the generation of a delinquent text because individual characteristics of the typing are stored locally in keyboard event logs (system logs) [Smushkin A.B., 2019: 32]; [González N., Calot E., 2023].

Last but not least, in the latter situation, special attention must be paid to mandatory state registration on the basis of keyboard dynamics where a person wishes to use a digital platform in any way related to the perpetration of an unlawful act.

In this case, a keylogger built into the interface should be used to record and transmit the keyboard dynamics data of the platform's users to the state data-

base. The data should have a reference to the MAC-address of the computer device used to access the platform, and the user must be notified in advance that about such data collection. If a person does not wish to transmit his/her keyboard dynamics data, he/she should be able to opt out of using the platform. As a result, the keyboard behaviour of all deliberate users during their active session on such a platform will be transferred to the state database.

Of course, the above scenarios of state registration based on keyboard dynamics are only a rough approximation of the situation that may take place in real life. Therefore issues raised here require additional research.

5. Using Keyboard Dynamics to Identify Perpetrators

Identification of computation device users on the Internet by means of keyboard dynamics analysis is a highly relevant task facing law enforcement scientists, criminal intelligence officers and forensic experts seeking to solve crimes and identify perpetrators.

Forensic processing of keyboard dynamics is highly significant due to the ever-increasing number of computer-related offences. According to A.M. Karimov, they all have one distinctive feature in common: "It is not the subject of criminal offence but it is the mechanism and the tool used to inflict harm to various social relations, whose generic characteristics differ, or it is the medium in which an unlawful act is committed" [Karimov A.M., 2023: 79]. In other words, if you apply an expansive interpretation of this category is more accurate, computer crime includes acts that were committed with direct involvement of information and communication technologies. And, as E.R. Rossinskaya notes, almost any "conventional" crime can be committed this way at present [Rossinskaya E.R., 2019: 33]. This makes the list of "computer-related" subjects of the offence almost endless, where only the scope of criminal law is the limit.

At the same time, in practically any offence of this type, typed texts may occur which are significant from the law enforcement perspective and which can be the subject of criminal trespassing (investigation reports; official documents in cases related to falsification or forgery thereof, etc.); which are used to commit an offence (exhortations to commit suicide; defamatory materials, extremist materials etc.); which are part of preparations for illegal activities (correspondence in social networks conducted as the perpetrator looks for accomplices, raises funds etc.); they are generated in the course of committing an offence but are not related to the objective ele-

ment of the offence (correspondence between accomplices conducted to coordinate their actions etc.); which contain additional information about the circumstances significant for uncovering the crime and solving the case (a post on the personal page in a social network where the perpetrator expresses the intent to commit the offence etc.).

According to the survey author of the paper have conducted, 68.6% investigators (73 respondents) are confronted with the need to analyze typed texts with varying degrees of regularity, and 76.7% (56 respondents) have had to resolve the task of identifying the person that typed a certain text. And since there is no methodology to solve this task, the officers have to resort to additional interrogations (53.3%), authorship examination (28.3%), or presume that the owner of the computation device is the person who typed the text (33.3%). However, none of these methods is flawless because it either fails to ensure objectivity, or is designed to resolve tasks that are close but not identical to the task in question. E.g., testimony at the interrogation may be false; authorship examination decides the question of the who is the author of the text, which does not always coincide with the person who typed it; and the presumption is destroyed in cases of multi-user equipment or malicious (including remote) access to another person's device.

Keyboard dynamics analysis can become the required special method, by analogy with analysing handwriting in handwriting analysis. We deem it possible to obtain samples of keyboard dynamics for comparative studies by means of the respective crime investigation procedures (Art. 202 of the Russian Federation Criminal Procedure Code) or by means of law enforcement intelligence operations; to use in crime investigation activities free samples stored in the above-mentioned state database (after it has been created), and then to conduct a computer-based expert assessment of information on keyboard dynamics according to the methodology of comparative identification studies.

However, keyboard dynamics should not necessarily constitute evidence; it will explore in details in the following sections. Many researchers agree the phenomenon under review (either per se, or as a biometric characteristic) is an inseparable part of a person's digital profile [Foygel E.I., 2023: 105]; [Zaytsev O.A., Pastukhov P.S., 2022: 295]. Hence, if it is analysed by various means, including forensic diagnostics, in combination with other data about the perpetrator operating in the digital environment, it can give directions for investigation and help to narrow search for the potential offender.

6. Keyboard Dynamics as Evidence

In description of the significance of keyboard dynamics for crime investigation it was pointed out it offered a tool to identify the person that typed a certain text that had been used in criminal activities in any fashion— similar to the way in that the question of the perpetrator of a handwritten text has been resolved over the long history of forensic science. Still, texts are typed not only in connection with criminal activities, and the identity of the person that has typed a text can become the issue in any court proceeding: criminal, civil, arbitration, or administrative. Constitutional proceedings are the only exception here due to their special nature.

In all the proceeding the model for using data on the keyboard dynamics is standard, so it will not describe each of them in a separate section.

Keyboard dynamics can be used in a court proceeding to prove a person's involvement or non-involvement in the creation of a particular typed text. The only way to attach evidential significance to the data about such dynamics is to conduct special computer-based examination, which would answer the following questions:

Have the texts submitted for examination been typed by one person?

Has the disputed text been typed by the person whose keyboard dynamics samples are submitted for examination?

Has a certain text been typed on the personal computer (keyboard) submitted for examination?

Has one or several persons worked on the personal computer (keyboard) submitted for examination during a certain period of time?

What is the approximate age of the person who typed the text?

What psycho-emotional and physiological state was the person in at the time of typing the text?

Has the text been typed in an environment unfamiliar for the person? etc.

In addition, the examination must necessarily address questions about the presence or absence of key loggers[10] on the computer device submitted for examination, which may also be significant for establishing the circumstances of the case in court.

[10] Standard expert techniques for physical evidence examination. Part I. Y.M. Dildin (ed.). Moscow, 2010. P. 199.

In considering theme of evidential significance of an expert assessment, it is of need to turn attention to of automatic data processing. Current researches focuses on creating tools to identify users by their keyboard dynamics on the basis machine learning [Zeid S., ElKamar R., Hassan S., 2022: 95–104]; [Matsubara Y., Samura T., Nishimura H., 2015: 230]. Thus, it is proposed use AI to solve most of the applied tasks when working with the phenomenon under review. It is quite justified, because in 30 minutes of work, in the course of typing an unfamiliar text about 800 characters long, more than 10,000 keyboard events can be generated. At the same time, today all AI intelligence systems operate according to the "black box" principle [Suman R.R., Mall R. et al., 2010]; [Smushkin A.B., 2024: 136–137]. Therefore, the user will not know for sure how the information at the input has been processed to produce the concrete result. But expert opinions presented in court must be verifiable, and all participants in a trial should be able to assess this opinion, and understand how a particular conclusion has been made. Otherwise, such an opinion will not be recognized as admissible evidence [Branovitsky K.L., Renz I.G., 2019: 43–54]. This imposes limitations on the possible use of AI systems in forensic computer-based examination of keyboard dynamics, although it does not rule out the possibility of using auxiliary technical means that simplify computations of large amounts of data.

Further use of an expert opinion falls completely under the general rules stipulated in the procedural rules of each relevant law, so it does not need a separate description. However, some scientists deem otherwise.

E.g., I.Z. Fyodorov considers it necessary to amend Article 5 of the Criminal Procedure Code containing terms and definitions, and to enshrine in it the definition of keyboard dynamics with all its individual characteristics. He also suggests introducing a number of other amendments to certain articles, specifically stipulating the obligation to appoint a forensic expert examination to examine keyboard dynamics, recognise electronic carriers of keyboard dynamics data as material evidence, etc. [Fyodorov I.Z., 2019: 113–114]. However, that such clarifications are unnecessary because keyboard dynamics and methods of dealing with it as part of legal proceedings (including criminal proceedings) may well be included into general procedural provisions. On the other hand, a detailed elaboration of this kind would invariably lead to the transformation of a law into an instruction, which is contrary to the meaning of acts of such level.

7. Keyboard Dynamics in Labour Relations

Relations between the employer and the employee are one more area where is useful to analyse the use keyboard dynamics from the legal perspective. Automatic recording and continuous monitoring of keyboard dynamics allow, unlike more conventional means of authorisation (password, fingerprint, access key, enhanced electronic signature, etc.), to see if the actual user is working at the computer throughout the session [Vasilyev V.I., Kalyamov M.F. et al., 2018: 399]; [Bryukhomitsky Yu.A., Kazarin M.N., 2006: 154]; [Paschenko D.V., Balzannikova E.A., 2020: 74–75]. It makes the phenomenon under review highly relevant in the field of labour relations. For example, it can be used to ensure that employees complete their tasks diligently and independently, rather than stealing innovative ideas from their colleagues. This is especially important in creative professions (designer, sales manager, etc.), where the development of a new project contributes to career growth and is a condition for receiving a bonus. In addition, as E.E. Turutina notes, "an authentication system (*which can be based, among other things, on analysing the attributes of keyboard dynamic.* (italics are mine.–A.Ts.*)* solves many problems, such as <...> keeping track of working hours and the location of staff at a given time" [Turutina E.E., 2021: 168]. In this case, processing keyboard dynamics will make it possible to determine who is working on a certain computer device at a particular point in time; what the person is doing: whether he / she is really working or is engaged in some unrelated activity; whether the employee is working overtime, etc.

However, the phenomenon under review plays a more important role in cases related to occupational safety and discipline control. E.g., Yu.A. Bryukhomitsky and M.N. Kazarin note analysing keyboard dynamics allows "to detect temporary psychophysical deviations of operators from their normal behaviour resulting from stress, sickness, ailments, taking pharmaceutical substances, etc." [Bryukhomitsky Yu.A., Kazarin M.N., 2006: 154]. Studies by other scholars support similar conclusions [Vasilyev V.I., Sulavko A.E., Borisov R.V. et al., 2017: 21–23]; [Lozhnikov P.S., Sulavko A.E., 2015: 32–33]; [Ivanov A.I., 2000: 8]. It may help to determine if an employee is over-fatigued, is under influence of alcohol or other substances, and, based on this information, to decide to suspend this person. This is especially important "when, for example, users are working with potentially hazardous computer systems or life support systems

(nuclear power plants, medical institutions, emergency services, etc.)" [Mashtanov P.N., Martynyuk M.V., 2021: 529].

These measures can improve work processes, ensure compliance with the work and rest schedule, and provide the interested parties with objective evidence during individual labour dispute. However, the controversial legal nature of such control should be taken into account.

On the one hand, the legal regulations (Clause 1, Part 1, Art. 86 of the Russian Federation Labour Code[11]) allows the employer to undertake all the above-mentioned measures if these aim to protect the employees and the assets of the employer (in case it is established the employee is in a state that prevents him/her from fulfilling his/her duties in compliance with all the requirements), exercise control over the volume and quality of the work performed (in course of recording data on the employee's real activities at work and when checking the person's identity). However, in any case, all employees must be notified at the stage of concluding an employment contract that their keyboard dynamics will be subject to processing (Clause 8, Part 1, Art. 86 of the Labour Code). In addition, it is the possibility granted to the employer to exercise control over the employee that is considered a distinctive feature of labour relations [Ofman E.M., 2021: 130–131]. Foreign legislators in many countries even use the electronic monitoring concept [Siegel R., König C., Lazar V., 2022]; [Lira Í., Schiavon L., Freguglia R., 2024: 205–221]. This concept proceeds from a set of actions by the employer aimed at obtaining information about employees' activities and their condition through specialized technical means and by collecting information from various electronic media, and communication networks (including monitoring network activity, electronic communications, telephone conversations, etc.).

On the other hand, such control may violate the right to personal privacy, which was discussed in detail above. Automated information processing can be a solution. E.g., many key loggers may be part of a complex software module with an integrated intelligent data processing function. I.e. the data on keyboard dynamics is analysed by means of machine learning algorithms. Then, on this basis, the system establishes, for instance, the person in question is in an abnormal psychophysiological state, and temporarily suspends him/her from work. In this case, the employer will not know what the person

[11] Labour Code of the Russian Federation of 30.12. 2001 No.197-FZ (as amended 06.06.2024). Available at: URL: https://www.consultant.ru/document/cons_doc_LAW_34683/ (accessed: 21.07.2024)

was typing but will only receive a generalized analytical review. However, it is of need to clarify here that at present legally binding decisions may not be made on the basis of an employee's personal data obtained exclusively through automatic data processing. In view of this, the software module that we describe here may not determine if an employee should be held accountable, suspended from work etc., but can only send an alarm: working conditions are being violated and that this must be double-checked by other means.

However, if the task arises to establish the identity of the person who produced a text (wrote a department development project, entered financial indicators into reporting documents, etc.), the employer may turn to the corporate technical service (IT department), as its representatives have the necessary competences to evaluate keyboard dynamics and conclude if its features belong to a particular person.

In this regard, scholars engaged in the labour law should pay attention to the issue of using keyboard dynamics to implement automated control over employees, particularly to address the issues of economic and technological feasibility, and compliance with ethical values. May I believe technology under review will prove to be totally acceptable: it has already shown a successful performance at some enterprises and is "the easiest to implement and administer, because it doesn't require any additional hardware, except for a computer keyboard" [Nikulicheva E.O., 2019: 57–59].

Conclusion

There are various areas of social relations where keyboard dynamics can be implemented. But, to respect citizen's rights in a reasonable manner and protect privacy, while at the same time ensuring aims of national and public security are achieved, a comprehensive legal framework must be established to regulate social relations in connection with keyboard dynamics. Probably today the following model is the optimum.

In the early stages, until the legal status of keyboard dynamics is precisely defined and enshrined in law, all persons involved in its processing, irrespective of the key logger localization (in the desktop software or on a digital platform in the world-wide web), must be obliged to obtain informed consent from the users, similar to the consent required when the website wants to store cookies on the user's device. Perhaps the best approach would be to create big pop-up windows with general description of the data to be processed and the purpose of this processing, not to hide

information in many pages of data policies. Users should be given an option both to limit the list of data collected and to deny access to their keyboard dynamics completely while retaining access to the programme and/or services in question.

Next, is should be enshrined that keyboard dynamics is a biometric characteristic, and this dynamics must be included in the list of data that only a authorised person is entitled to process (e.g., the operator of the Unified Biometric System; at present, it is the Centre for Biometric Technologies). At the same time, the technical and legal capacities of the UBS can be used to carry out state registration of keyboard dynamics along two lines: voluntary, and mandatory. Mandatory registration will apply to persons who committed crimes or administrative offences with the use of typed texts, who knowingly use a digital platform previously used to commit such unlawful acts, or who hold public service positions involving work with information that constitutes a state secret or with e-government services. A corresponding Federal Law should be passed to implement the measures for state registration.

Next, measures must be taken to exclude a possibility of unauthorised correlation of keyboard dynamics with a specific typed text, since otherwise the right of citizens to personal and family privacy, confidentiality of correspondence, etc., would be unjustifiably violated. In this field, it would seem promising to use method of indirect recording of keyboard dynamics, linking its features to the computer device on which these features were recorded, rather than to a specific person who is their carrier. Hence, to solve the tasks facing law enforcement agencies (identify a person guilty of committing a crime or administrative offence, where typed texts were the subject of encroachment or means of committing an offence), requests will have to be sent to the operator, which aggregates data about keyboard dynamics in their relation to the MAC-address, and to the network connection services provider, which stores data about the owner of a device with a specific MAC-address. Perpetrators, in their turn, to link valuable information to a particular person, would need to make a significantly greater effort to gain unauthorised access to several secure databases, that seems very unlikely, if not impossible.

Implementing all the above described preparatory measures will make it possible to include the processing keyboard dynamics into the activities of crime investigation, procedural proof of the involvement or non-involvement of a particular person in the creation of a typed text, and into the

sphere of labour relations to control the integrity of employees and their proper medial state, ensuring the safety of working processes.

Keyboard dynamics is a phenomenon of reality should not be locked in the narrow framework of one branch of scholar knowledge. It should be researched by a wide range of specialists, including the legal profession, where individual sciences may take an interest in the phenomenon and develop their own approaches to defining it, describing its place and the possibilities of using their knowledge about it.

References

1. Averin A.I., Sidorov D.P. (2015) User authentication by keyboard dynamics. *Ogaryov-Online*, no. 20, pp. 1–5 (in Russ.)

2. Alsultan A., Warwick K. (2013) Keystroke dynamics authentication: a survey of free-text. *International Journal of Computer Science Issues*, vol. 10, no. 1, pp. 1–10.

3. Banerjee S.P., Woodard D.L. (2012) Biometric authentication and identification using keystroke dynamics: a survey. *Journal of Pattern Recognition Research,* vol. 7, pp. 116–139. DOI: 10.13176/11.427.

4. Branovitsky K.L., Renz I.G. (2019) May an expert be trusted? On forensic expertise quality (comparative analysis). *Zakon*=Law, no. 10, pp. 43–54 (in Russ.)

5. Bryukhomitsky Yu.A., Kazarin M.N. (2006) Covert keyboard monitoring system. *Vestnik Taganrogskogo radiotechnicheskogo universiteta*=Taganrog Radiotechnical University Bulletin, no. 9, pp. 154 (in Russ.)

6. Clarke R. (1994) Human identification in information systems: management challenges and public policy issues. *Information Technology & People,* vol. 7, pp. 6–37.

7. Forsen G., Nelson M., Staron R.Jr. (1977) Personal attributes authentication techniques. Technical Report. Rome: Air Development Center, 333 p.

8. Foygel E.I. (2023) Modern trends and prospects of development of the forensic doctrine of the personality of participants of criminal proceedings. *Akademicheskiy juridicheskiy zhurnal*=Academic Juridical Journal, no. 1, pp. 101–108. DOI: 10.17150/1819-0928.2023.24 (1) (in Russ.)

9. Fyodorov I.Z. (2019) Searching persons typed electronic text by keyboard dynamics in the detection and investigation of crimes. *Vestnik Barnaulskogo intituta MVD*=Bulletin of Barnaul Law Institute of Internal Ministry, no. 2, pp. 113–116 (in Russ.)

10. González N., Calot E. (2023) Dataset of human-written and synthesized samples of keystroke dynamics features for free-text inputs. *Data in Brief*, vol.

11. Guo J., Mu H. et al. (2024) Federated learning for biometric recognition: a survey. *Artificial Intelligence Review*, vol. 57, pp. 208–247. DOI: 10.1007/s10462-024-10847-7.

12. Guryanov K.V. (2020) Project 'Strelok': the first key logger. *Bazis*=Basics, no. 2, pp. 79–91 (in Russ.) DOI: 10.1016/j.dib.2023.109125.

13. Ivanov A.I. (2000) *Biometric identification of personality by dynamics of subconscious movements.* Penza: University, 188 pp. (in Russ.)

14. Ivanov V.V., Zuyev D.I. (2022) Digital twin and digital identity: concept, correlation, meaning in the process of committing cybercrime and in law in general. *Pravo i gosudarstvo*=Law and State: Theory and Practice, no. 4, pp. 138–144. DOI: 10.33184/pravgos-2022.4.19 (in Russ.)

15. Isaeva V.V., Sakharova Y.V. (2020) International and national aspects of legal regulation of private life and the right to private life. *Vestnik Bryanskogo universiteta*=Bulletin of Bryansk University, no. 2, pp. 136–142 (in Russ.)

16. Karimov A.M. (2023) Crimes in the sphere of computer information and crimes with using information and communication technologies: comparative aspect. *Vestnik Kazanskogo intituta MVD*=Bulletin of Kazan Institute of Internal Ministry, no. 1, pp. 75–82. DOI: 10.37973/KUI.2023.93.91.010 (in Russ.)

17. Lozhnikov P.S., Sulavko A.E. (2015) Technology of identification of computer system users by dynamics of subconscious movements. *Avtomatizatcia*. *Sovremennye technologii*=Automation. Modern Technologies, no. 5, pp. 31–36 (in Russ.)

18. Lira Í., Schiavon L., Freguglia R. (2024) Electronic monitoring of working time and labour market outcomes: evidence from Brazil. *Industrial Relations Journal*, vol. 55, pp. 205–222. DOI: 10.1111/irj.12423.

19. Matsubara Y., Samura T., Nishimura H. (2015) Keyboard dependency of personal identification performance by keystroke dynamics in free text typing. *Journal of Information Security,* vol. 6, pp. 229–240. DOI: 10.4236/jis.2015.63023.

20. Mashtanov P.N., Martynyuk M.V. (2021) Review of current issues of biometric identification based on the features of keyboard dynamics. Information systems and technologies-2021: proceedings of a conference. Nizhny Novgorod: Technical University Press, pp. 527–531 (in Russ.)

21.Md A., Mohiuddin S. et al. (2019) Key logger detection using memory forensic and network monitoring. *International Journal of Computer Applications,* no. 11, pp. 17–21.

22. Nikulicheva E.O. (2019) Analysis of keyboard dynamics as a method of personal identification. Issues of forensic psychological examination and complex examination with participation of a psychologist. In: Prospects of fundamental and applied research of handwriting: papers of international conference. Kaluga: University Press, pp. 56–60 (in Russ.)

23. Ofman E.M. (2021) Transformation of the employer's right to control the employee's behaviour in the digital economy. *Yearbook* of *Labour Law*, no. 11, pp. 130–145 (in Russ.)

24. Paschenko D.V., Balzannikova E.A. (2020) Continuous user identification by keyboard dynamics using state-context based representation. *XXI vek*: *itogi proshlogo i problemy nastoyaschego*=XXI Age: Past Results and Present Issues, no. 3, pp. 74–79. DOI: 10.46548/21vek-2020-0952-0012 (in Russ.)

25. Rossinskaya E.P. (2019) Special knowledge in the judicial examination of computer crimes in the digital age. *Vestnik Kutafin University*=Bulletin of Kutafin University, no. 5, pp. 31–44. DOI: 10.17803/2311-5998.2019.57.5.031-044 (in Russ.)

26. Salikov M.S., Nesmeyanova S.E. et al. (2022) State regulation of the Internet and human rights. Ekaterinburg: University Press, 220 pp. (in Russ.)

27. Samsoni D.Z., Basir B.P. et al. (2023) Key logger threats in computer security aspects. *International Journal of Integrative Sciences,* vol. 2, no. 6, pp. 867–872. DOI: 10.55927/ijis.v2i6.4520.

28. Shadman R., Wahab A. et al. (2023) Keystroke dynamics: concepts, techniques, and applications. Preprint. DOI: 10.48550/arXiv.2303.04605.

29. Shangina I.Y. (2020) Biometric identification technologies: global and the Russian practices. *Innovatcii*. *Nauka*. *Obrazovanie*=Innovations. Science. Education, no. 18, pp. 151–156 (in Russ.)

30. Siegel R., König C., Lazar V. (2022) The impact of electronic monitoring on employees' job satisfaction, stress, performance, and counterproductive work behaviour: a meta-analysis. *Computers in Human Behaviour Reports,* vol. 8. Article 100227. DOI: 10.1016/j.chbr.2022.100227.

31. Smushkin A.B. (2019) The issue of "digital alibi" in forensic science. *Problemy ugolovmogo protcessa*=Issues of Criminal Procedure, no. 2, pp. 28–33 (in Russ.)

32. Smushkin A.B. (2024) Concept of remote criminalistics. Moscow: Yurlitinform, 256 pp. (in Russ.)

33. Solomatina E.A., Cherkashina A.V., Dreval B.V. (2021) Fingerprint registration in administrative law of Russia. *Vestnik Moskovskogo universiteta MVD*=Bulletin of Moscow University of Internal Ministry, no. 4, pp. 234–240. DOI: 10.24412/2073-0454-2021-4-234-240 (in Russ.)

34. Spillane R. (1975) Keyboard apparatus for personal identification. *IBM Technical Disclosure Bulletin*, vol. 17. Article 3346.

35. Suman R.R., Mall R. et al. (2010) Extracting state models for black-box software components. *Journal of Object Technology*, no. 3, pp. 25– 29.

36. Syed Idrus S.Z. (2014) Soft biometrics for keystroke dynamics. Computer vision and pattern recognition. Caen: Universite de Caen, 134 p.

37. Turutina E.E. (2021) Analysis of electronic and biometric authentication methods in access control systems. *Vestnik akademii nauk tatarstana*=Bulletin of Tatarstan Academy of Sciences, no. 2, pp. 168–175 (in Russ.)

38. Uimin A.G., Morozov I.M. (2022) Comparative analysis of continuous online authentication tools and anomaly detection systems for continuous confirmation of user identity. *Telekommunikatcii i transport*=Telecommunications and Transport, no. 5, pp. 48–55. DOI: 10.36724/2072-8735-2022-16-5-48-55 (in Russ.)

39. Vacca J.R. (2007) Biometric technologies and verification systems. Burlington: Elsevier, 625 p.

40. Varlamova S.A., Vavilina E.A. (2023) User identification on the basis of keyboard dynamics. *Innovatcionnoe priborostroene*=Innovations in Instrumentation

Engineering, vol. 2, no. 3, pp. 67–71. DOI: 10.31799/2949-0693-2023-3-67-71 (in Russ.)

41. Vasilyev V.I., Kalyamov M.F., Kalyamova L.F. (2018) User identification by keyboard dynamics using frequent bigram registration algorithm. *Modelirovanie, optimizatcia i indormatcionnye technologii*=Modeling, Optimization and Information Technologies, vol. 6, no. 1, pp. 399–407 (in Russ.)

42. Vasilyev V.I., Sulavko A.E., Borisov R.V. et al. (2017) Recognition of psychophysiological states of users by hidden monitoring in computer systems. *Iskusstvennyi intellect i prinyatie resheniy*=AI and Decisions, no. 3, pp. 21–37 (in Russ.)

43. Villani M., Tappert C. et al. (2006) Keystroke biometric recognition studies on long-text input under ideal and application-oriented conditions. Proceedings of international workshop computing and computational statistics. DOI: 10.1109/CVPRW.2006.115.

44. Zaytsev O.A., Pastukhov P.S. (2022) Digital profile of a person as an element of information-technological strategy of crime investigation. *Vestnik Permskogo universiteta*. *Pravo*=Bulletin of Perm University. Legal Sciences, no. 56, pp. 281–308. DOI: 10.17072/1995-4190-2022-56-281-309 (in Russ.)

45. Zeid S., El Kamar R., Hassan S. (2022) Fixed-Text vs. Free-Text keystroke dynamics for user authentication. *Engineering Research Journal*, vol. 51, pp. 95–104. doi:10.21608/erjsh.2022.224312.

46. Zhukov M.N. (2021) Validity of biometric data using in forensic science: historical background and legal protection of personal data. *Mezhdunarodnyi naucho-issledovatelskyi zhurnal*=International Scholar Research Journal, no. 12, pp. 164–167. DOI: 10.23670/IRJ.2021.114.12.148 (in Russ.)

47. Zuyev S.V. et al. (2019) Basics of theory of electronic evidence. Moscow: Yurlitinform, 653 pp. (in Russ.)

Information about the author:

A.D. Tsvetkova — Researcher.

The article was submitted to editorial office 21.04.2024; approved after reviewing 17.06.2024; accepted for publication 02.09.2024.