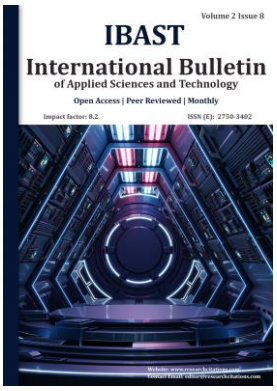

ETHICAL PRINCIPLES FOR ORGANIZING DIGITAL INVESTIGATION IN THE PROCESS OF DIGITAL TRANSFORMATION : UZBEKISTAN AND FOREIGN EXPERIENCE

Khamidov Bakhtiyor Khamidovich
Tashkent State Law University Senior teacher of the department of Criminalistics and Forensics Science
E-mail: Bahtiyor1984bsj@mail.ru
Askerov Bakhsheish Mamed ogly
associate professor of the Department of Criminalistics and Forensic Expertise at the Baku State University
E-mail: tuncer55@rambler.ru
https://doi.org/10.5281/zenodo.7877979

Annotation
This article discusses the ethical (etiquette) issues of organizing a digital investigation in the process of digital transformation. In particular, the study put forward proposals for improving the methodological support of investigative practice in the conduct of digital investigation. The study analyzed the experience of Germany, England and the Republic of Uzbekistan in implementing the rules of digital ethics (etiquette).
The researcher puts forward the idea that in the process of digital transformation, it is fundamentally important to introduce ethical (etiquette) rules for organizing digital investigation into investigative practice. The author believes that in order to protect personal data during investigative activities in the digital environment, first of all, it is necessary to establish ethical (etiquette) principles for working with electronic evidence, therefore, he gives recommendations on adapting investigative practice to advanced foreign practices.
The article was prepared on the basis of scientific and practical research, the opinions of theorists and practitioners on ethical (etiquette) issues of digital investigation in the process of digital transformation.
Keywords: digital investigation, digital ethics (etiquette), legality, fairness, transparency, freedom, accountability.

1. Introduction

The active implementation of digital transformation processes makes it possible to widely use modern information technologies in public administration, the economy, the judiciary, education, healthcare, agriculture and other areas. Today, these processes are applied in almost all spheres of public life, and it has become the most active means of meeting daily needs. Daily tasks of a person, lifestyle, interests, plans, actions and activities in general are closely related to digital technologies. At the same time, humanity is active both in the virtual and in the material world [1]. This situation is especially evident during the Covid-19 pandemic. In particular, the transition to online forms of labor markets and wage payment provides an opportunity for state and non-state organizations to widely use, monitor and control information about the privacy of citizens.
According to Article 27 of the Constitution of the Republic of Uzbekistan, everyone has the right to be protected from interference in his personal life [2]. At the same time, according to the current legislation, personal information relating to individuals is classified as confidential information [3]. Therefore, human life and personal data are rights elevated to the highest

degree of value! On the other hand, in the digital society, government and non-government organizations need this information when exercising certain powers.

During the coronavirus pandemic, these situations create psychological and legal conflicts of interest dilemmas. In particular, on the one hand, the priority of the constitutional rights of citizens related to privacy and protection of personal data, on the other hand, issues of ensuring the interests and security of state and non-state organizations cause conflicts between legal norms. The reason is that the enforcement of one of these norms in the fight against cybercrime inadvertently leads to the violation of the other.

2. Research results

Ethical (etiquette) issues when organizing a digital investigation

The processes of implementing digital transformation also cover the moral (ethical) requirements associated with the use of digital technologies in the investigative process. The reason is that ethical issues are closely related to the privacy of citizens and the protection of personal data. Therefore, it is absolutely impossible that the legislator or persons applying it do not pay attention to these criteria when preparing, adopting or applying normative legal documents. The reason is that the Constitution of the Republic of Uzbekistan clearly recognizes that the rights and freedoms of the individual are higher than the interests of society and the state. This situation is also directly related to the processes of organizing a digital investigation.

In fact, establishing a code of conduct for civil servants is nothing new in legislation. The reason is that the Resolution of the Cabinet of Ministers of the Republic of Uzbekistan dated March 2, 2016 No. 62 “On Approval of Model Rules of Conduct for Employees of State Administration Bodies and Local Executive Bodies” approved model rules. Based on this, each law enforcement agency has adopted its own code of conduct. However, these rules are not taken into account when determining the admissibility of digital evidence.

The rules of etiquette for working with digital evidence define the rules that an expert, an official of an inquiry body, an investigator, an investigator, a prosecutor, courts should follow when collecting, examining and evaluating digital evidence in a case. specific case. The high level of compliance with these rules by these entities is essential when conducting a digital investigation. The reason is that these cases are directly related to the privacy of citizens and the protection of personal data.

In international practice, the method of collecting and verifying digital evidence in the course of a trial is of great importance. The courts have the right to explain how this evidence was obtained in the course of the preliminary investigation and examination, and to require their demonstration (presentation). This institution was introduced to ensure impartiality and transparency in the administration of justice. Therefore, an expert, an official of the body of inquiry, an investigator, an interrogator, a prosecutor must carefully prepare for the presentation of any type of digital evidence to the court. At the same time, these subjects refrain from expressing any inappropriate or unverified opinions about digital evidence research.

Today, the privacy of personal data is considered one of the problems of great concern not only in the country, but throughout the international community. The reason is that the digital transformation of all spheres of society, in turn, gives rise to the need for the use of personal data [4]. Various services provided by state bodies, state bodies or non-state enterprises,

institutions and organizations are directly related to the personal (confidential) information of citizens. These cases also allow these organizations to monitor and control the privacy of citizens or personal information. In this context, it is advisable to regulate the protection of the rights and freedoms of citizens not only by legal and technical requirements, but also by the rules of etiquette.

Typically, this information includes the person's name, year of birth, social security number, passport, driver's license, bank account number, credit or plastic card numbers, biometric or genetic data, socioeconomic status, political opinions, religious beliefs, health. ., information about sex life or sexual orientation, PIN codes, electronic signature or passwords can be entered. This information is extremely dangerous, as it gives the right to control a person or his financial means, or passes the victim off as a criminal. Accordingly, it is advisable for the investigator to ensure the confidentiality of this information when conducting a digital investigation.

The study analyzed a number of advanced foreign experience and international standards in this case. In this regard, the experience of regulating ethical (etiquette) relations in the process of digital investigation in the USA, England and European countries has been studied.

The "Code of Digital Etiquette" adopted by the German Republic when organizing a digital investigation includes 5 principles - justice, freedom, usefulness, non-harm and transparency [5]; The Association of Police and Crime Commissioners of England, Scotland and Northern Ireland (APCC) has defined 6 principles: legality, accuracy, openness and transparency, good governance, fairness and accountability [6]. By clearly defining the tasks to be carried out under each principle, it was possible to avoid possible ambiguities in the scope of the law.

According to the regulations established in the Republic of Uzbekistan, civil servants must carry out their professional activities based on the following principles: legality; fidelity to the Motherland and devotion to duty, full fulfillment of the assigned functional duties, strict observance of performing discipline; priority of the rights, freedoms and legitimate interests of citizens; loyalty to the interests of the state and society; fairness, honesty and impartiality; intolerant attitude and fight against corruption situations; strict observance of service confidentiality; do not abuse official powers; Avoiding conflicts of interest [7].

The results of the analysis show that there are certain gaps in these rules of etiquette. These gaps are related to personal responsibility, conflict of interest prevention, and digital evidence research, and it is worth revisiting and refining these requirements from today's point of view. Therefore, in traditional investigative and judicial practice, there are no sufficient skills and experience in the methodological rules for working with electronic evidence in the investigation of cybercrime. Therefore, the law enforcer is forced to rely on his intellectual and legal consciousness when regulating relations that arise in practice. This, in turn, leads to the formation of various practices in investigative practice and the use of methods and means that do not have a full scientific justification when evaluating digital evidence in relation to a case.

3. Conclusion

The results of the study show the need to adapt the rules of etiquette adopted by law enforcement agencies in our country to foreign best practices.

At the same time, it is advisable to establish the following ethical rules when organizing a digital investigation:

ensuring the inviolable rights to life, health, honor and dignity of a person during a digital investigation;
maintain a high degree of impartiality and honesty;
comprehensive and complete study and analysis of digital evidence and the correct presentation of facts;
conduct a digital investigation and follow the principles of working with digital evidence;
draw conclusions based on provable facts [8];
non-disclosure of facts that may entail liability.

References:

1.Истам Астанов, & Бахтиёржон Хамидов (2021). Общетеоретические вопросы, связанные с электронными или цифровыми доказательствами: проблема и решение. Общество и инновации, 2 (7/S), 259-278. doi: 10.47689/2181-1415-vol2-iss7/S-pp259-278
2.Ўзбекистон Республикаси Конституцияси 27-модда. https://lex.uz/docs/20596
3.Ўзбекистон Республикасининг “Ахборот эркинлиги принциплари ва кафолатлари тўғрисида”ги Қонуни. 13-модда.
4.Ўзбекистон Республикаси Президетининг “Рақамли Ўзбекистон 2030” стратегияси.
5.https://www.merckgroup.com/company/responsibility/us/products-businesses/CoDE-Code_of_Digital_Ethics.pdf 2021.
6.https://www.apccs.police.uk/about-the-apcc/
7.Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2022 йил 14 октябрдаги “Давлат фуқаролик хизматчилари томонидан одоб-ахлоқ қоидаларига риоя этилишини таъминлаш бўйича қўшимча чора-тадбирлар тўғрисида”ги 595-сон қарори билан тасдиқланган “Давлат фуқаролик хизматчилари одоб-ахлоқининг намунавий қоидалари” 2-банди.
8.Международная ассоциация специалистов по компьютерным расследованиям.