ProAcademy

Volume 2021
Issue 1 *2021/1*

Article 2

2-19-2021

FORMATION AND DEVELOPMENT OF THE PROSECUTOR'S SUPERVISION OVER THE COMPLIANCE OF LAWS IN INVESTIGATION OF CRIMES IN THE SPHERE OF INFORMATION TECHNOLOGIES

Atobek Ravshanovich Davronov
Academy of the General Prosecution office, atodavr@gmail.com

Atobek Davronov
adamdavr@gmail.com

Davronov Atobek Ravshanovich
PhD student of the Academy of the General Prosecutor's Office of the Republic of Uzbekistan
E-mail: Adamdavr@gmail.com
Tel: +998946592657

FORMATION AND DEVELOPMENT OF THE PROSECUTOR'S SUPERVISION OVER THE COMPLIANCE OF LAWS IN INVESTIGATION OF CRIMES IN THE SPHERE OF INFORMATION TECHNOLOGIES

Abstract: the rapid growth of information technologies naturally determines the interest of researchers in them from various fields of science. Law, including criminal law, is no exception. Currently: a separate branch of law is being formed - information law. Despite this, until now in science unified approaches to the analysis of information and legal phenomena have not been developed. The article analyzes the formation and development of prosecutorial supervision over the execution of laws in the investigation of crimes in the field of information technology, and also studied the process of the emergence of information technology as a type of crime abroad. In addition, the article is devoted to the analysis of laws adopted on the activities of prosecutors since the independence of the Republic of Uzbekistan. The article indicates that, initially, faced with computer crime, law enforcement agencies began to fight it with the help of traditional legal norms on theft, misappropriation, fraud, and abuse of trust. However, this approach was not entirely successful, since many computer crimes are not covered by traditional crimes.

Keywords: Prosecutor, information technology, law, computer, Internet, crime, defense, defense, personal data, surveillance, sabotage, fraud, research

Introduction

The problem of the research lies in the fact that no one has yet studied the appearance and formation of prosecutorial supervision over the implementation of the law in the investigation of crimes in the field of information technology in the Republic of Uzbekistan.

In order to ensure the protection of sovereignty and in accordance with the Law of the Republic of Uzbekistan "On the Foundations of State Independence of the Republic of Uzbekistan"[1] as well as in accordance with the Presidential Decree "On the Prosecutor's Office of the Republic of Uzbekistan" dated January 8, 1992 No. UP-313, [2] the USSR Prosecutor's Office was transformed into an independent prosecutor's office. Republic of Uzbekistan.

January 8, 1992 is the date of the creation of the prosecutor's office. The structure of the central office of the prosecutor's office, issues related to local prosecutors were determined by the Resolution of the Cabinet of Ministers of the Republic of Uzbekistan dated January 24, 1992 No. 33 "On the organization of the activities of the prosecutor's

office of the Republic of Uzbekistan."[3] From this, it can be concluded that the prosecutor's supervision over the investigation of crimes in the Republic of Uzbekistan was the first in its manifestation to have been carried out since January 1992.

Materials and Methods

The work uses the following general scientific methods: dialectical, the method of analysis and synthesis of components, individual signs of concepts, generalization and classification. Special methods of legal research (including forensic): the method of comparative jurisprudence, historical, formal-logical, systemic-structural, etc. An additional methodological basis for the development of scientific categories was the laws of formal logic and linguistics.

Since the material studied and analyzed in the dissertation is at the junction of several areas of knowledge.

In accordance with the decision of the Supreme Council of the Republic of Uzbekistan dated January 4, 1992, the Constitution of the Republic of Uzbekistan, the laws of the USSR that do not contradict the laws, will be partially implemented until the adoption of the relevant laws in the Republic of Uzbekistan. The Law "On the Prosecutor's Office of the USSR", adopted on November 30, 1979, was in force until the adoption of the Law of the Republic of Uzbekistan " Prosecutor " on December 9, 1992 by the Supreme Council of the Republic of Uzbekistan [4].

This step on the part of the Government of the Republic allowed lawyers to take an active part in legislative work, taking into account international experience, practice and national characteristics of the people. Chapter 24 of the Constitution of the Republic, adopted on December 8, 1992, defines the powers and status of the prosecutor's office. The Attorney General and his subordinate prosecutors are responsible for the accurate and uniform application of laws throughout the country. On the basis of this constitutional norm, on December 9, 1992, the Law of the Republic of Uzbekistan "On the Prosecutor's Office" was adopted.

In the period 1991 - 2001, the Prosecutor's Office of Uzbekistan was withdrawn from the Prosecutor's Office of the USSR, the status, goals and objectives of the Prosecutor's Office were fixed at the constitutional level, the legal framework for the organization and activities of the Prosecutor's Office was created, the main directions of prosecutorial supervision were determined, the corresponding institutional changes were made in the structure of the Prosecutor's Office of the Republic of Uzbekistan created the Office for the fight against corruption, embezzlement and other abuses in the field of foreign economic activity, etc. This is described in detail in the work of M. Makhbubov "Creation and Development of Prosecutor's Office in Uzbekistan"[5].

On August 29, 2001, in the spirit of modernity, a new edition of the Law of the Republic of Uzbekistan "On the Prosecutor's Office" was adopted. The law covered new democratic processes. The function of monitoring the observance of laws by citizens was excluded from the activities of the prosecutor's office. Concepts such as “The

prosecutor’s office is a criminal prosecution body” or, more simply, “the prosecutor’s office as an accusatory body” was abolished.

Now the protection of the rights and legitimate interests of citizens has become one of the main tasks of the prosecutor's office. In accordance with this law, new norms were introduced regarding the liability of prosecutors. In this law, much attention is paid to ensuring the protection of the rights and freedoms of citizens, the legitimate interests of society and the state, the criterion for assessing the work of the prosecutor's office is strengthened.

In the period from 2001 to 2017, the goals, objectives, main directions of prosecutorial supervision, the role and place of the prosecutor's office in the system of state bodies, and especially prosecutorial supervision were legislatively defined. One cannot but agree with the opinion of M.Kh. Rustambaev and E.N. Nikiforova, who assert that during this period legislative work was carried out to form the legal basis for the implementation of prosecutorial supervision, taking into account the international experience and practice of developed democratic countries [6].

During this period, the attitude of the prosecutor to the protection of the rights and freedoms of citizens, as well as entrepreneurship, was completely revised.

In the period 2017 to this day, more than 30 amendments and additions have been made to the Law "On the Prosecutor's Office". In particular, the prosecution authorities carry out their activities publicly by regularly informing the public about their activities to supervise the implementation of laws and combating crime, ensuring access of individuals and legal entities to information about their activities in the manner prescribed by law.

Changes have been introduced to exercise the powers of the prosecutor. Information technologies developed in parallel with the development of prosecutorial supervision.

Simultaneously with the concept of the enormous value of information, there is a need for its protection. Over time, social transformations led to the need for legislative regulation of new social relations. The problem of protecting information and information systems is now one of the most urgent in the world.

The history of the development of legislation regulating public relations in the field of high technologies is inextricably linked with the emergence and improvement of computers and the global Internet [7].

One of the first computer crimes was committed in the United States in the late seventies of the last century. Stanley Rifkin, a computer security consultant at Security Pacific National Bank, deciphered the code governing the Los Angeles bank's system and instructed the computer to transfer $ 10 million to his checking account. According to another version, the first computer crime in 1969 was committed by Alfonse Confessore (USA). Having illegally gained access to information on an electronic computer network, he committed a tax crime, the damage from which amounted to 620 thousand US dollars [8].

This fact has attracted close attention of law enforcement agencies and scientists to the field of computer information. Intensive research has begun on this phenomenon.

Initially, faced with computer crime, law enforcement agencies began to fight it with the help of traditional legal norms on theft, appropriation, fraud, and abuse of trust. However, this approach was not entirely successful, since many computer crimes are not covered by traditional crimes.

So, for example, the simplest type of computer fraud - moving money from one account to another, by "cheating the computer" - is not covered by the theft (due to the absence of the object of theft - material property, since money exists here not in the form of things, but in the form information on a computer medium); nor the composition of fraud, since in reality it is possible to deceive the computer only in the sense in which it is possible to deceive the lock at the safe.

In 1973, Sweden introduced computer crime liability into its legislation, becoming the first country to legally enforce such norms. It provided for criminal liability for illegal penetration into a computer system and the introduction of false information into computer information, allowing theft of money, securities, property, services or valuable information[9].

However, the greatest success in this area has been achieved in the United States.

In 1979, in Dallas, the Conference of the American Bar Association was held, at which the main elements of computer crimes were defined and formulated, which were subsequently included in the US Criminal Code.

In 1983, in the United States, in the state of Milwaukee, there was the first arrest of a publicly known Internet criminal. The first recorded internet hacking was perpetrated by a group of six teenagers who called themselves "group 414" (414 is the Milwaukee area code). Within nine days, they "hacked" 60 computers, including computers at Los Alamos State Laboratory (nuclear weapons research center).

In the 1980s, a quantitative increase in computer attacks began. The Center for Internet Security Research (CERT), which opened in 1988, records an increase in the number of computer attacks reported by Internet users. If in 1988 there were only six appeals to the center, in 1989 - 132, and in 1990 - already 252. Around this time, the process of division of specializations among Internet criminals begins.

In 1986, the United States passed The Act Computer Fraud and Abuse No. 8. It constitutes the primary computer crime regulation and is incorporated as 18 USC §1030[10]. This law prohibited unauthorized access to any computer system and the receipt of classified military information[11].

In addition, the law protected three types of unclassified information:

1. Information owned by financial institutions (for example, information about credit cards and accounts);

2. Data owned by government agencies;

3. Information owned by international or interstate organizations.

The law also contained provisions prohibiting data corruption (for example, the spread of viruses).

By the late 1980s and early 1990s, an increase in Internet crime was noted in almost all countries. The authorities of most developed countries realized the need to create a regulatory framework for combating crimes in the field of high technologies, since the existing legislation did not allow to adequately fight hackers. So in 1986 the Criminal Code of the Federal Republic of Germany was supplemented with norms providing for liability for computer crimes.

For the UK, this problem became clear when it failed to secure an indictment in the case of Stephen Gold and Robert Schifreen, who in 1984 gained unauthorized access to British Telecom's Prestel service. They were charged under the Forgery and Counterfeiting Act of 1981. The perpetrators were acquitted at the court of appeal, and the acquittal was subsequently confirmed by the House of Lords.

The first law in the United Kingdom to specifically target the misuse of computer technology was the Computer Misuse Act of 1990[12].

In accordance with it, the following are classified as criminal offenses:

a) intentional unlawful access to a computer or the computer information or programs contained therein (Art. 1);
b) intentional illegal access to a computer or the computer information or programs contained in it for their subsequent use for illegal purposes (Art. 2);
c) unlawful access to computer information on a machine medium, in a computer, computer system or network, if this entailed the destruction, blocking, modification or copying of information, disruption of the computer, computer system or network (Article 3)[13].

The Law establishes that the jurisdiction of the prosecution authorities and the courts of Great Britain is subject to extension to any of the listed acts, in the commission of which at least one of the elements of the crime took place in the country. Thus, in cases where only the act itself or only its consequences take place on the territory of the UK, the crime is recognized as completed in the UK (Articles 4-7). This provision is necessary in circumstances where the crime was committed from a computer located in a country that has not established responsibility for such crimes, or when criminal law orders are material in nature. The corpus delict is recognized as completed only in the event of the occurrence of harmful consequences on the territory of the state where the criminal act was committed.

Since the 80s. XX century many countries have concluded that the legal protection of computer information through general provisions of national criminal law is insufficient.

In 1983-85. in the Organization for Economic Cooperation and Development (OECD), a special committee was created to discuss the possibility of harmonizing the criminal legislation of different countries on liability for computer crimes[14].

In the period from 1985 to 1989. on the problem of computer crimes, the Council of Europe's Separate Committee of Experts on Computer Crimes worked. As a result of the committee's work, on 13 September 1989, the Council of Europe adopted Recommendation No. R89 (9) of the Committee of Ministers of the Council of Europe member states on computer-related crimes. It defines practically all crimes related to the use of computer technologies, and also provides a classification of computer crimes with a recommended and optional list for their inclusion in national legislation. So among those recommended for inclusion in the domestic criminal legislation, the document distinguishes the following types of computer offenses: computer fraud, computer forgery, damage to computer data or computer programs, computer sabotage, unauthorized access, unauthorized interception, unauthorized reproduction of a copyrighted computer program, unauthorized reproduction of a microcircuit.

Recommendation No. R 89 (9) provided that the provisions of the criminal law should contain as precise a description of the criminal offense as possible. This principle of clarity is extremely important, but unfortunately not all states follow it[15].

In 1995, a second recommendation followed, dealing with the procedural aspects of the problem. It was the first to put forward the idea of developing an international treaty on cybercrime. Having assessed the threat posed by the growth of this phenomenon, the European Committee on Crime Problems commissioned a group of experts to study the problem. They proposed to develop a Convention that considered not only purely legal issues related to the fight against cybercrime, but also the procedural requirements for solving this problem. In February 1997, the Committee of Ministers of the Council of Europe instructed the newly created Committee of Experts on Cyberspace Crime to prepare a set of legal obligations, addressing the issues of corpus delicti, the rule of law, the use of coercive measures (including at the international level) and state jurisdiction in regarding the crimes committed.

April 1997 to December 2000 The committee held 10 plenary meetings and its drafting group met 15 times. In April 2000, the project was unclassified and posted on the Internet so that both specialists and users could familiarize themselves with it. In March 2001, the Parliamentary Assembly joined the process of drafting the Convention by organizing special hearings on this issue. The Committee of Ministers applied to the Parliamentary Assembly for an opinion on the draft, which was adopted at its April 2001 session. The text of the Convention was approved at the meeting of the Committee of Ministers in the rank of permanent representatives on September 19, 2001 and adopted by the foreign ministers at the meeting on November 8, 2001. And already on November 23, 2001 in Budapest, the Convention on Cybercrime was open for signature by states. The day of its entry into force was the first day of the month following the expiration of a 3-month period from the day when it was ratified by 5 states. Lithuania ratified the Convention on Cybercrime on March 18, 2004, and after this, fifth ratification, the Convention entered into force on July 1, 2004[16].

Results

The results of the study showed that the process of adopting specific regulatory legal acts regulating prosecutorial supervision over the execution of laws in the field of investigating crimes in the field of information technology was very slow and criminals easily began to use these entities.

In the early 90s. an attempt to create a unified classification of computer crimes was undertaken by the working group of the International Criminal Police Organization Interpol. The approved codifier of computer crimes highlights: unauthorized access and interception, alteration of computer data, computer fraud, illegal copying, computer sabotage and other computer crimes. The problem of the unification of criminal legislation was repeatedly raised at the conferences of the G8 countries (G-8).

Discussion

In the USSR, the first crime was committed in 1979 in Vilnius. The damage to the state then amounted to 80 thousand rubles - with this money it was possible to buy 8 Volga cars. In Russia, one of the first major computer crimes is considered to be a criminal case of embezzlement of 125.5 thousand US dollars and preparation for theft of more than 500 thousand US dollars in «Vnesheconombank» of the USSR in 1991[17].

April 29, 1996 is considered the birthday of Uznet. It was on this day that the UZ domain was registered, and the Republic of Uzbekistan was officially recognized as a state represented on the Internet. Information, which is the main wealth of society, is naturally the object of various types of criminal encroachments. The history and development trend of criminal law in the field of information and communication technologies are conditionally divided into three stages:

The first stage includes the period from the moment of gaining independence in 1991 until the adoption of the Criminal Code (CC) of the Republic of Uzbekistan in 1994. During this period, legislative acts were adopted that generally regulate the issues of informatization and relations in the field of information technology (for example, the Law of the Republic Uzbekistan "On the legal protection of programs for electronic computers and databases")[18].

The second stage covers from 1994 to 2007. During this period, the Criminal Code of the Republic of Uzbekistan was adopted, which provided for liability for violation of the rules of informatization, theft, fraud, theft by misappropriation and embezzlement using computer technology, as well as general laws in the field of information technology - "On the principles and guarantees of freedom of information"[19], "On Telecommunications"[20], "On Informatization"[21]. The nature of informatization was determined, a mechanism for protecting this process was developed, and the necessary legal basis was created. Also, with the adoption of the Civil Code of the Republic of Uzbekistan, the legal nature of information as a thing was determined.

The third stage covers the period from 2007 to the present. During this period of informatization and computerization, it became necessary to improve the mechanism of criminal-legal protection of relations in the field of information technology. Taking into account the positive experience of foreign countries, a new Chapter XXI was introduced

in the Criminal Code, providing for new elements of crimes in the field of information technology.

If we look at other countries then in as a starting point, it is relevant to clarify the term "suspect" since the rules of coercion in both criminal justice systems imply that a person is suspected of an offence. Under the French criminal law, a suspect is defined as "any person against whom there exist one or more plausible reasons that he or she has committed or attempted to commit an offence.

Under the Swedish law, a suspect is a person against whom there exists a "reasonable suspicion" that he or she has committed or attempted to commit an offence. These definitions cover, under the two legal systems, the first degree of suspicion. A second and more serious degree does exist in both systems and is applicable only to suspects involved in a judicial examination and against whom there is "probable cause" under the Swedish law or "strong and concordant evidence" under French law, that they may have participated, as perpetrator or accomplice, in the commission of the offences.

Coercion is allowed and may be resorted to upon merely meeting the requirements of the first degree of suspicion, although these two situations carry different tools and degrees of coercion. But, either way, whether there is a 'plausible reason' or a 'reasonable suspicion', such terminology does not allow us to define in specific terms the notion of suspect and leaves the police a wide range of discretionary powers according to the circumstances of the case. Yet when a decision to detain someone is made, the prosecutor has to ensure that there are sufficient reasons to believe that the person held in the police station is, in one way or another, involved in the criminal offence. Consequently, in both legal systems, the terms "plausible reason" and "reasonable suspicion" need to meet the requirements of fairness and due process of law and have, as such, to be interpreted in an objective way, thus avoiding any subjective suspicion.

Despite a few specificities, the powers of coercion held by the French and the Swedish prosecution authorities, in the course of a criminal investigation, are quite similar. Police custody and pre-trial detention powers will be considered here below to underline the similarities between the two systems. Both French and Swedish prosecutors have the power to hold a suspect in custody. While the police have the power to stop, search and arrest someone who is suspected to have committed a criminal offence, they need to report any police detention to the prosecution service. In France, any judicial police officer is entitled to hold a suspect in custody for up to 24 hours. When necessary an extension may be allowed for a second period of 24 hours if the request is sent and agreed to by the district prosecutor prior to the first 24 hours' deadline.

Regardless of the length of custody, the district prosecutor is under a more general duty to supervise police custody measures by visiting the places where suspects are held". In Sweden, if the power to arrest someone of whom there is a reasonable suspicion is given to police officers, the suspect can be held at the police station for a period which will not exceed six hours. For any extension the police are under the obligation to report to the prosecutor who is the only one competent to extend the length of custody up to

three and a half days. Hence while detention decided by a judicial police officer may last for a longer period in France the maximum legal length of custody, including any extension, is usually more important in Sweden.

Consequently, regardless of the authority competent in the course of a criminal investigation-the prosecutor and the judge under Swedish law, or the investigating magistrate, the liberty and custody judge and the investigating chamber under French law - any person involved in a criminal offence benefits from some rights that shall be considered as a counterbalance of the existing powers of coercion granted to relevant authorities.

The role and status of a prosecutor not only places duties on those performing that role in the office or in court. It extends to other professional capacities and to their lives outside the office. This section addresses the issues of what prosecution services should expect from prosecutors and what prosecutors should expect from their respective prosecution services.

Prosecutors have the right to pursue their private lives as they see fit but must do so within the bounds of the law and within the peculiar constraints of their profession. The independence that is so important to prosecutors in effectively performing their duties places some limits on activities that may compromise or give the appearance of compromising the independence of their office: activities such as outside employment that could lead to a conflict of interest, running for political office while still employed as a prosecutor, consorting with known criminals or frequenting venues where criminals may be found or engaging in activities that may bring the office of the prosecutor into disrepute are considerations that prosecution services may need to address with their staff.

This is perhaps the case now more than ever as the digital age has allowed anyone practically anywhere to take photographs or video recordings and disseminate them worldwide with the press of a button. This has the potential to intrude upon every person’s private life, including prosecutors.

In addition, prosecutors should not allow their personal or financial interests or family, social or other relationships to improperly influence their conduct. A prosecutor should not play any part in a case in which the prosecutor or the prosecutor’s family or business associates have a personal, private or financial interest or association. It is unacceptable behavior for a prosecutor to accept any gifts, prizes, benefits, inducements or hospitality from third parties or carry out any task that may be seen to compromise the prosecutor’s integrity, fairness and impartiality, as is using the official capacity of the prosecutor’s office to obtain a personal advantage. In some States prosecutors are required to declare their assets and all sources of income to their employer as a method of preventing corruption. This can be a valuable safeguard against corruption as well as tending to draw the individual prosecutor’s attention to any potential conflict of interest. Management should ensure that procedures are in place to guide prosecutors who seek advice concerning possible conflicts of interest.

The roles that prosecutors perform during the investigative phase of a criminal case may differ depending on the legal tradition of each State. In most civil law and

some common law systems, the prosecutor has control over the entirety of the investigation and directs the police in what course of action they should take in their investigation and what charges will be brought against an accused. The involvement of prosecutors in the investigation varies depending on the legal system and complexity and seriousness of cases. They may conduct the investigation and carry out some investigative steps, such as interviews or searches. They may have control of the investigators either directly when investigators are assigned to the prosecution office or indirectly. For example, prosecutors may be consulted about the performance of an investigation unit or individual investigators. Historically, in the common law and some civil law systems, the police investigated crime and could decide whether charges should be laid against an individual. The prosecution has decided whether the evidence gathered is sufficient to prove the crime alleged and if so, presented the case before the court for adjudication by the judiciary and may barely intervene in the police investigation.

In these systems, the relationship between the police and the prosecutor at the investigative stage was traditionally an exclusive and independent one. For example, in Thailand, prosecutors have no role in the investigation of the case, this being left solely to the police even in large, complex cases (although there are exceptions).

Experience has shown, however, that strict adherence to this methodology is proving to be problematic. The advent of new and sophisticated methods of perpetrating crimes and increasing complexities within the law have led to increased prosecutorial intervention in the police investigation and greater cooperation between these two groups where previously such intervention or cooperation did not exist:

All the problems mentioned above] caused a gradual change of thinking regarding the prosecutors' involvement in investigations. Before reflecting on this, it should be mentioned that the police themselves were gradually forced to seek prosecutors' advice more often. The appearance of new forms of criminality (organized crime, especially money-laundering and drug trafficking) and the ever-increasing complexities of substantive and procedural law made the police more dependent on the prosecutors for legal advice. In many common law jurisdictions, this has evolved into forms of cooperation that provide the prosecutor with some influence in the investigation process itself. In most jurisdictions, however, this form of cooperation has remained on an informal level and is usually ad hoc, without changing the constitutional relationship between the two institutions.

In some common law jurisdictions (e.g. the Crown Prosecution Service of England and Wales), the decision to initiate proceedings in all but minor cases is now the province of the prosecutor. In Ireland, all prosecutions are in principle controlled by the Director of Public Prosecutions. General directions issued by the Director require the police to refer certain categories of cases to the Director before charges are preferred; these include sexual offences and terrorism.

The Guidelines on the Role of Prosecutors and the IAP Standards do not take a preferential position on the issue of prosecutorial intervention in the investigation of crime. Throughout the world today there is a wide spectrum of prosecutorial involvement at the investigative stage, ranging from no involvement at all to being in

charge of and taking an active role in criminal investigations. However, there is an increasing tendency for prosecutors to become involved at an earlier stage, particularly in complex cases such as fraud or corruption, even in countries where the prosecutor has no formal role in investigations, using the mechanism of the police seeking advice at the investigative stage. The following excerpt provides an example of the breadth of responsibility that prosecutors have in various jurisdictions around the world and emphasizes the point that there are no hard and fast rules for prosecutorial involvement, even in jurisdictions sharing the same legal tradition:

In Germany, prosecutors are by law responsible for leading investigations by themselves, and the police are only an investigatory body of the public prosecution office, whereas in reality it is the police who are actually leading investigations in most cases. Prosecutors are vested with similar responsibility in the Republic of Korea. In Japan, prosecutors are also empowered to carry out investigations, but at the same time, the Code of Criminal Procedure states that the primary responsibility of investigation lies with the police. On the contrary, in other countries with common law traditions such as Kenya, Pakistan, Papua New Guinea, the United Republic of Tanzania and the United Kingdom, prosecutors play no role in investigation as such, but do exercise their advisory or supervisory authority to guide the police investigation in such ways as advising or instructing the police to carry out their investigation to certain direction. In this context, it should be kept in mind that the development of new forms of cooperation between the police and prosecutors should not be viewed as just an adjustment for the sake of convenience, on the contrary, such developments in many countries are structured upon the deep consideration as to the independently entrusted roles of the police and prosecutors in the course of realizing the rule of law. The relationship between the police and prosecutors inevitably and desirably involves, to some extent, a conflicting nature. Accordingly, close collaboration between the police and prosecutors should be only developed on such a challenging, though positively stimulating, relationship.

The spectrum of evidence to be excluded on the ground that it was illegally or improperly obtained differs from State to State and is subject to different legal tests for admissibility. In modern criminal law, regardless of legal tradition, evidence acquired by unlawful methods that constitute a grave violation of the suspect's human rights is absolutely excluded, although such exclusions are based on different theories in each legal system. In this regard, prosecutors must examine the proposed evidence to see if it has been unlawfully or improperly obtained and should consider refusing to use evidence reasonably believed to have been obtained through unlawful or improper methods, according to the gravity of unlawfulness or impropriety and the standards described in their own State's rules of evidence. In particular, when those methods constitute a grave violation of the suspect's human rights, such as the obtaining of evidence through torture or cruel, inhuman or degrading treatment or punishment, prosecutors should not use the evidence against anyone other than in proceedings against those who used such methods. Further, in States where prosecutors participate in, conduct, direct or supervise investigations, they themselves should not use unlawful or

improper methods in obtaining evidence, and should give appropriate instructions and advice to police or investigators to do likewise. As “essential agents of the administration of justice”, prosecutors should always be mindful of human rights violations in the whole course of obtaining evidence and take appropriate actions against those responsible for them. Thus, for example, when prosecutors come to know or suspect that evidence was obtained using unlawful methods, such as torture or inhuman treatment, or improper methods of lesser severity, they should consider the investigation of those who implemented or directed such methods, and disciplinary action should also be considered, if applicable.

Prosecutors should give due consideration to diverting criminal cases, in particular those involving young offenders, offenders charged with minor offences and first-time offenders, from the formal justice system, where such action is appropriate and permitted by law. When prosecutors decide to employ alternative measures, they should ensure that alternative measures are consistent with preventing re-offending, assisting redress of the damage incurred by society, having regard to the interest of victims, upholding the rights of the defence, and forming a response to illegal acts that is in the public interest. There should be no undue intervention in the activities of prosecutors when they use their discretionary powers in relation to such measures. In some States the prosecuting authority has not only a discretion whether to prosecute or not, but also the ability to conditionally discontinue the case, that is to bind over or sanction the suspected offender. Where prosecutors are vested with the power to impose penalties without court intervention, they should ensure that the rights of the accused are safeguarded by affording the latter the right to be heard and to give his/her consent before the prosecution imposes a penalty.132 The imposition of conditions should not be oppressive for the offender.

Examples of alternatives to prosecution are drug or alcohol treatment, community service orders, victim compensation, written warnings and restorative justice mechanisms such as indigenous conferencing programmes.

Asset restraint and forfeiture is becoming an increasingly common component of many criminal investigations and prosecutions as States look to combat an increasingly sophisticated criminal element that embraces globalization and capitalizes on the benefits and protections it can offer. Many States have domestic legislation designed to trace, freeze and seize proceeds of crime, and many States have also ratified international conventions such as the United Nations Convention against Corruption and the United Nations Convention against Transnational Organized Crime. Legislation and conventions of this type provide powerful tools to combat domestic and international crime but they require prosecutors who are well versed in complex crime and multidisciplinary teams with specialist knowledge. In many cases, this knowledge will have to go beyond the domestic legal framework and enter the realm of international legal cooperation.

Conclusion

In our opinion, with the adoption of the Law of the Republic of Uzbekistan "On the Legal Protection of Programs for Electronic Computers and Databases" and Art. 173 of the Criminal Code of the Republic of Uzbekistan, crimes in the field of information technology become the object of prosecutorial supervision.

Computer crimes are dynamic in nature. As a result of the rapid development of new technologies, new forms of computer crime are emerging at an equally fast pace, spreading through the use of new methods.

REFERENCES

1. The Law of the Republic of Uzbekistan "On the Foundations of State Independence of the Republic of Uzbekistan" dated 31.08.1991. https://www.lex.uz/acts/127879. Date of access: 06/29/2020
2. Decree of the President of the Republic of Uzbekistan "On the Prosecutor's Office of the Republic of Uzbekistan" dated January 8, 1992 No. UP-313 https://lex.uz/docs/147166. Date of access: 29.06.2020
3. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan dated January 24, 1992 No. 33 "On the organization of the activities of the prosecutor's office of the Republic of Uzbekistan" https://lex.uz/docs/386218. Date of access: 29.06.2020
4. Pulatov B.X. Procurator control. Textbook. T .: “Uzbekistan” 2009. B. 12-34.
5. Makhbubov M. Creation and development of prosecution bodies in Uzbekistan. Diss .. for the degree of Doctor of Law.-Tashkent, 1993
6. Rustambaev M.Kh., Nikiforova E.N. Law enforcement agencies of the Republic of Uzbekistan. Textbook for universities. T., 2003
7. Yastrebov D.A. Institute of Criminal Liability in the Field of Computer Information (Experience of International Legal Comparative Analysis) // State and Law. 2005. No. 1. Pp. 53-63
8. Medvedev S.S. Fraud in the field of high technologies: dis ... cand. jurid. sciences. Krasnodar, 2008.P. 31.
9. Dremlyuga R.I. Internet Crime: Monograph. Vladivostok: Far East Publishing House. University, 2008.P. 173
10. United States Computer Fraud and Abuse Act 1986 United States 1030 Section 18 Code.
11. Dashyan M.S. Law of information highways: question. legal regulation in the field of the Internet. M .: Walters Kluver, 2007.
12. Computer Misuse Act. 1990. official web-site of legislation United Kingdom http://www.legislation.gov.uk /ukpga/1990/18/contents. Date of application: 10.10.2019
13. Cybercrime and the Law: An overview of the UK computer crime legislation. URL: http://www.viruslist.com/en/analysis?pubid=204007656. Date of treatment 12/04/2018
14. Zhidelev V.G. Evolution of legislation on criminal responsibility for committing crimes in the field of high technologies. Zh .: Bulletin of the Udmurt University. Series "Economics and Law" Vol. 4. 2011.P. 114-118.
15. Council of Europe Committee of ministers Recommendation No. R (89) 9. Official web-site of legislation: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f1094. Date of application: 10.10.2019
16. Zinina U.V. International cooperation in the field of combating computer crimes // Law and Security. 2005. No. 3. P. 14-17.
17. Minaev V.A., Sablin V.N. The main problems of combating computer crimes in Russia // Economy and production. 1999.P. 10-12.

18. Law of the Republic of Uzbekistan dated 06.05.1994. № 1060-XII "On the legal protection of programs for electronic computers and databases." https://www.lex.uz/acts/143970. Date of access: 26.07.2019
19. Law of the Republic of Uzbekistan dated 12.12. No. 439-II "On the principles and guarantees of freedom of information" https://lex.uz/docs/52709. Date of access: 26.07.2019
20. Law of the Republic of Uzbekistan dated 20.08.1999. No. 822-I "On Telecommunications" https://www.lex.uz/acts/33152. Date of access: 26.07.2019
21. Law of the Republic of Uzbekistan dated 11.12.2003. "On informatization" https://www.lex.uz/acts/82956. Date of access: 26.07.2019