УДК 343.131
DOI https://doi.org/10.32782/2408-9257-2023-6-30

Bodunova O. M.,
Candidate of Law, Associate Professor,
Head of the Department of Legal Linguistics
State Tax University
https://orcid.org/0000-0001-9179-5985

Hrytsiuk I. V.,
Candidate of Law, Associate Professor,
Associate Professor of the Department of Criminal Justice
State Tax University
https://orcid.org/0000-0003-2253-4057

INVESTIGATION OF CRIMINAL OFFENCES: THE INTERNATIONAL DIMENSION

РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ: МІЖНАРОДНИЙ ВИМІР

The article examines the peculiarities of criminal offences investigation at the current stage of development of Ukraine and the world.

It is noted that in the modern legal system, evidence is becoming an increasingly important element in criminal proceedings, since its use reflects technological progress and development of society. However, Ukraine has not yet sufficiently developed the rules governing the use of evidence in criminal proceedings.

Clear and detailed rules on the collection, presentation and use of evidence are critical to ensuring a fair and efficient criminal justice system. Such rules should define what types of evidence are admissible, how their reliability can be verified, how they should be preserved and presented at trial, and how they can be used in the adjudication of cases.

The author establishes that the key areas of the State policy on investigation of criminal offences are: guaranteeing the independence of the information sphere of Ukraine; improving the State regulation of the information industry development through creation of legal and economic conditions for the development of national information infrastructure and resources, use of advanced technologies, filling the domestic and global information space with reliable information about Ukraine; active involvement of the media in preventing and combating criminal offences. Also, guaranteeing respect for the constitutional rights to freedom of speech, access to information, protection of personal data, prevention of unlawful interference in the activities of the media and journalists, prohibition of censorship, discrimination in the information sphere as well as persecution of journalists for political beliefs, professional duties and criticism; implementation of a set of measures to protect the national information space and counteract the monopolisation of the information sphere of Ukraine.

Key words: *criminal proceedings, criminal procedure, investigation, crime, criminal offence, European Court of Human Rights.*

У статті розглянуто особливості розслідування кримінальних правопорушень на сучасному етапі розвитку України та світу.

Зазначено, що в сучасній правовій системі докази стають все більш важливим елементом у кримінальному процесі, оскільки їх використання відображає технологічний прогрес і розвиток суспільства. Однак, в Україні ще не достатньо розроблені норми, які регулювали б використання доказів у кримінальному процесі.

Наявність чітких і детальних правил щодо збирання, представлення та використання доказів є критично важливою для забезпечення справедливого і ефективного кримінального судочинства. Такі правила повинні визначати, які види доказів є прийнятними, як їхню достовірність можна перевірити, як вони повинні бути збережені та представлені на судовому засіданні, і як їх можна використовувати в процесі вирішення справ.

Встановлено, що ключовими напрямами державної політики з питань розслідування кримінальних правопорушень є: гарантування незалежності інформаційної сфери України; удосконалення державного регулювання розвитку інформаційної галузі через створення правових та економічних умов для розвитку національної інформаційної інфраструктури та ресурсів, використання передових технологій, заповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; активне залучення засобів масової інформації до запобігання та протидії корупції, зловживанням службовим становищем та іншим явищам, що становлять загрозу національній безпеці України. Також гарантування поваги конституційних прав на свободу слова, доступ до інформації, захист персональних даних, запобігання незаконному втручанню в діяльність ЗМІ та журналістів, заборона цензури, дискримінації в інформаційній сфері та переслідування журналістів за полі-

тичні переконання, виконання професійних обов'язків та критику; проведення комплексу заходів для захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

Ключові слова: *кримінальне провадження, кримінальний процес, розслідування, злочин, кримінальне правопорушення, Європейський суд з прав людини.*

Statement of the problem. In the modern legal system, evidence is becoming an increasingly important element in criminal proceedings, as its use reflects technological progress and development of society. However, Ukraine has not yet sufficiently developed rules governing the use of evidence in criminal proceedings.

Clear and detailed rules on the collection, presentation and use of evidence are critical to ensuring a fair and efficient criminal justice system. Such rules should define what types of evidence are admissible, how their reliability can be verified, how they should be preserved and presented at trial, and how they can be used in the adjudication of cases.

In addition, it is important to ensure that the privacy and confidentiality of evidence, including electronic evidence, is protected and that it is not improperly obtained or manipulated.

The development and implementation of appropriate legislation to regulate the lawful receipt and use of evidence in criminal proceedings is an important task to ensure the efficiency and fairness of justice in Ukraine.

The state of the art of this issue. Investigation of criminal offences has been studied by M. Hutsaliuk, I. Kalancha, N. Luhina, O. Sirenko, A. Skrypnyk, A. Stolitnyi, V. Khakhanovskyi and others.

The purpose of the article is to analyse and study the legislative sources and practice of application of criminal offences investigation, and to study foreign experience on this issue.

Outline of the main material. The detection, disclosure and investigation of «cross-border» criminal offences via the global Internet network face major challenges, including the distribution of traces in different territories and their temporary storage. The anonymity of Internet participants and the temporary nature of information make it difficult to establish the location of new criminal offences Cooperation between operational units at various levels, including interaction with representatives of law enforcement agencies of other countries, plays an important role in increasing the efficiency of operational documentation of criminal offences in the field of information technology [1, p. 518–519].

To improve cooperation, the Convention provides for the establishment of a national authority under the Convention that will be available to provide immediate assistance in the investigation or prosecution of criminal offences involving computer systems and data or the collection of electronic evidence.

This assistance may include facilitating or, where permitted by domestic law and practice, directly carrying out the following activities

a) providing technical advice;

b) preservation of data pursuant to Articles 29 (Urgent preservation of stored computer data) and 30 (Urgent disclosure of stored data on the movement of information)

c) collecting evidence, providing legal information and locating suspects in accordance with Article 35 [2].

The Convention establishes mandatory requirements for implementation in the legislation of the acceding countries:

– granting law enforcement agencies the authority to issue binding orders for urgent registration and further storage of computer data necessary for the detection of a criminal offence (part 1 of Article 16, Article 17);

– retention of data on information traffic by provider institutions for up to 90 days with the possibility of further extension of this period (part 2 of Article 16);

– imposing on entities that store computer data the obligation not to disclose the fact of conducting operational and investigative and procedural actions during the period determined by the legislation of the country (part 3 of Article 16, part 3 of Article 20, part 3 of Article 21) [2].

The issue of detecting criminal offences is a key one for the United Nations bodies and institutions. This problem is actively discussed within the framework of the General Assembly (A/RES 63/195), the Economic and Social Council (res. 2009/22), the Commission on Crime Prevention and Criminal Justice (doc. E/CN.15/2009/15) and the UN congresses on crime prevention and criminal justice. These bodies make decisions aimed at developing ways and means to address

this problem. A number of interstate legal acts also address these issues [3].

It is recognised that today cybercrime poses a threat not only to the national security of a particular country, but also threatens the entire humanity. That is why this aspect attracts great attention in many countries. After analysing the experience of police in several countries in combating cybercrime, it can be noted that this is achieved by giving additional functions to existing police units or creating special units. In many countries, such as Australia, Belgium, Canada, Denmark, Estonia, Finland, France, Germany, India, Malaysia, the Netherlands, Norway, Poland, Sweden, Switzerland, the United Kingdom, the United States and others, special police units are created to combat cybercrime. The main functions of these units include:

– Cyberspace monitoring to detect cybercrime, viruses and malware.

– Operational, investigative and intelligence activities to record the illegal activities of cybercriminals.

– Investigating cybercrime and providing support to other industry services and law enforcement agencies within its competence.

– Collecting, summarising and analysing information on cybercrime.

– Preventing cybercrime through cooperation with the public and the media.

– Training of police officers.

– Some special police units dealing with cybercrime (also called special units for combating criminal offences related to the use of information technology) perform additional tasks, including

– Investigation of cybercrime.

– Prevention and control of telecommunication services.

– Expert analysis of evidence collected on electronic media.

– Creation and updating of a relevant database on cybercrime.

– Provision of services to banks to ensure the protection of clients' personal information, etc.

For example, in India, crime investigation units can engage professional hackers to solve crimes. It is important to note that during the investigation of cybercrime, much attention is paid to helping the victim recover damaged or lost information and taking all necessary measures to preserve evidence in the case [4, p. 193]. Moreover, in recent years, several strategies have been introduced in different parts of the world to prevent crime in the field of information technology.

The European Union carries out coordination work to harmonise crime legislation in force in the territory of its member states. This work includes the adoption of a number of documents, in particular: Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, including electronic commerce in the internal market; Council Framework Decision 2000/41/JHA on combating fraud and counterfeiting of non-cash means of payment; Council Framework Decision 204/68/JHA on combating sexual exploitation, etc. (paras. 20–21).

It is important to note that in order to improve the legal support for the investigation of criminal offences, it is necessary to study the positive experience of law enforcement agencies of other countries in this area. In particular, the Canadian police are actively fighting computer and telecommunications criminal offences. The Royal Canadian Mounted Police (federal police, RCMP) is responsible for investigating computer-related criminal offences and cooperates with other countries using data from the Canadian Police Information Centre. The unit's activities are aimed at investigating and detecting computer and telecommunications-related crimes. The Information Technology Protection Section ensures the security of federal government computer centres and the private sector, and provides advice and training on computer security. Employees of this unit assist police officers in investigating criminal offences related to computer systems. Given the speed of information transfer between terminals, there are about 2,500 access points in Canada, including 1,285 federal and provincial police stations. There are 1180 specialised RCMP units connected to the network to ensure efficient use of the system [5].

Undoubtedly, this area of police activity is extremely important, as the damage to the economy has already reached a significant level and some criminals are conducting organised activities on an international level. At the same time, it must be acknowledged that Canada's computer crime legislation needs to be improved. As the challenges faced by the police in the fight against computer crime are international in nature and not unique to Canada, they are actively working with other coun-

tries and Interpol to improve their legislation in this area. Investigating crimes is challenging, especially because of the time factor, as data can be transferred almost instantaneously and it is often difficult to find evidence of a violation of international law.

According to the RCMP, a large number of computer crimes are currently committed by minors under the age of twelve. According to the Criminal Code of Canada, in order to establish criminal liability, it is necessary to prove the unauthorised use of a computer system and the intent to cause harm. This approach requires a clear definition of the parameters of access to computer equipment to prevent violations. It is necessary to take into account data on individuals and access parameters with restrictions, as well as the possibility of employees «experimenting» with programmes. The Ministry of Justice or the relevant RCMP unit can provide expert advice on possible misconduct in this regard. It should be noted that the methodology for investigating unauthorised remote access to computer networks is technically complex and is a task for specialised police units. In connection with the threat of computer crime, its trends and impact on the global community, the UN regularly holds symposia on the prevention and suppression of computer crime. Experts point to software methods of protecting information in shared computer systems by improving the automatic control system as one of the ways.

The Economic Crime Department is working to reduce crimes related to the illegal use of telecommunications systems at the inter-provincial, national and international levels. The Information Centre provides assistance to police units.

Police activities to prevent and solve crime-related acts are also aimed at developing relations with various groups of society through the media, consultative meetings with members of the public, cooperation with government and administration, NGOs and individual citizens. Thus, the police are an important partner in the community of agencies that fight crime, including cybercrime, and ensure the observance of human rights and the protection of federal government computer centres and the private sector [5].

It should be emphasised that successful prevention of crime in the field of information technology requires effective and well-organised cooperation between law enforcement agencies of different countries, including cooperation within INTERPOL. We agree with the point of view of scholars such as V. V. Koriak and V. R. Slyvenko on the definition of interaction in law enforcement agencies as coordinated in time, methods and means of activity of units (or employees) that are not directly subordinate to each other, in order to achieve common goals and solve tasks.

Given the specifics of criminal offences in the field of information and communication technologies, the effectiveness of prompt documentation of these unlawful acts depends heavily on the cooperation of law enforcement agencies at all levels:

1. in terms of intra-agency cooperation – with other operational units of the cyber police, research and forensic centres and investigative units;

2. at the domestic level – with other law enforcement agencies of Ukraine, labour collectives, public organisations and the public;

3. at the international level – with law enforcement agencies of other countries. The main forms of cooperation between law enforcement agencies of Ukraine and law enforcement agencies of other countries are:

– exchange of operational information;

– providing legal assistance in criminal cases;

– travelling of members of investigative teams abroad to participate in investigative actions and operational activities;

– travelling for the exchange of operational information;

– Travelling abroad to participate in investigative and other activities within the framework of legal aid;

– travelling abroad to accompany wanted and detained persons;

– departure of employees of border guard and internal affairs departments of Ukraine to neighbouring regions of neighbouring countries in the framework of operational cases;

– arrival of law enforcement officers of foreign countries in Ukraine for investigative and operational activities;

To sum up, the current stage of civil society development is determined by Ukraine's entry into the world's leading technologically advanced countries and the global information space. That is why we have to use the experience of countries that already have quite serious developments in the field of information security [6, p. 225].

Since the creation of an information society is an integral part of this, it is important not only to expand the possibilities of technological exchange of information, but also to ensure that all participants in information relations – owners, users and producers of information technologies, service providers, and the state – are deeply aware of the need to protect information resources and ensure national security. This also includes taking into account international experience in combating crime in the field of information technology in the field of legal support.

Only through joint efforts of organisations and agencies regardless of ownership and the establishment of international cooperation, using modern information security technologies, can benefits be achieved not only in the field of e-business, but also in the overall information revolution, while ensuring the information security of the state and its citizens. It is important to note that the improvement of legal support for combating crime in the field of information technology in Ukraine should take into account the national cultural, historical and socio-economic characteristics of the country, based on a detailed analysis of international legislation and the experience of other countries in combating cybercrime, with a view to optimal implementation in the European and global legal field [7].

Thus, at the present moment, it is important for Ukraine to focus on two main areas:

– to consider the Ukrainian internal space as modern, full-fledged and competitive.

– guarantee the active presence of the state in the world and maintain a positive image.

– national security should be ensured with due regard to the priority of national interests and timely adoption of adequate measures corresponding to the nature and scale of threats to these interests. This should be based on the principles of a law-based democratic state. Since information security is an integral part of national security, national interests should also be given priority in this area.

Thus, the key directions of the state policy on detection of criminal offences are as follows:

– guaranteeing the independence of the information sphere of Ukraine;

– improvement of state regulation of the development of the information industry through the creation of legal and economic conditions for the development of national information infrastructure and resources, the use of advanced technologies, filling the domestic and global information space with reliable information about Ukraine;

– active involvement of the mass media in preventing and combating corruption, abuse of office and other phenomena that pose a threat to the national security of Ukraine. It also guarantees respect for the constitutional rights to freedom of speech, access to information, protection of personal data, prevention of unlawful interference in the activities of the media and journalists, prohibition of censorship, discrimination in the information sphere and persecution of journalists for their political beliefs, professional duties and criticism;

– implementing a set of measures to protect the national information space and counteract the monopolisation of the information sphere of Ukraine.

REFERENCES:

1. Користін О. Є., Бутузов В. М., Василевич В. В. та ін. Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. посіб. Київ : Скіф, 2012. 728 с.

2. Конвенція Ради Європи про кіберзлочинність : від 23 листоп. 2001р.; ратиф. Україною 7 верес. 2005 р. // *Офіційний вісник України.* 2007. № 65. Ст. 2535

3. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : від 28 січ. 2003 р. ; ратиф. Україною 21 серп. 2006 р. Офіційний сайт Верховної Ради України. URL: http://zakon.rada.gov.ua/laws/show/994_687.

4. Сень Р. Ю. Досвід іноземних країн у сфері розслідування кіберзлочинів. *Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності* : матеріали між-нар. наук.-практ. конф., м. Харків, 12 листоп. 2014 р. / МВС України, Харків. нац. ун-т внутр. справ. Харків : Права людини, 2014. С.192–194.

5. Варунц Л. Д. Досвід організації діяльності Королівської канадської кінної поліції та шляхи його використання в Україні : дис. канд. юрид. наук : 12.00.07. Дніпропетровськ, 2012. 203 с.

6. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: навч. посіб. Київ : КНТ, 2006. 280 с.

7. Марков В.В. До питання щодо зарубіжного досвіду протидії кіберзлочинності. *Право і безпека*. 2015. № 2(57). С. 107–113.