Check for updates

DOI: https://doi.org/10.34069/AI/2024.76.04.19

How to Cite:

Babikov, O., Smirnov, A., Chernysh, M., Syrovatka, S., & Pylypenko, I. (2024). Use of electronic search systems in the investigation of corruption crimes in Ukraine: opportunities and challenges for human rights. *Amazonia Investiga*, *13*(76), 236-246. https://doi.org/10.34069/AI/2024.76.04.19

Use of electronic search systems in the investigation of corruption crimes in Ukraine: opportunities and challenges for human rights

Використання електронних пошукових систем під час розслідування корупційних злочинів в інтересах кримінального судочинства: можливості та загрози для прав людини

Received: March 1, 2024 Accepted: April 28, 2024

Written by:

Oleksandr Babikov[1]
https://orcid.org/0000-0003-4003-5198

Anton Smirnov[2]
https://orcid.org/0000-0002-1562-4591

Maryna Chernysh[3]
https://orcid.org/0009-0000-6416-7617

Serhii Syrovatka[4]
https://orcid.org/0009-0008-4547-533X

Ihor Pylypenko[5]
https://orcid.org/0000-0003-2098-1283

Abstract

The purpose of the article is to study the use of electronic search systems during the investigation of corruption crimes in the context of the balance of interests of criminal justice and ensuring guarantees of human rights and freedoms. Methodology. In the process of scientific research, the following methods were used: dialectical, logical, dogmatic, monographic, systemic and structural, comparative and legal, sociological, legal modelling. Research results. It was established that in accordance with the developed and tested methods investigators use various information systems when investigating on corruption crimes; the content and features of these schemes were studied. International documents establishing the limits of the possible use of artificial intelligence in criminal proceedings were considered. The decisions of the

Анотація

Метою статті є дослідження використання електронних пошукових систем під час розслідування корупційних злочинів в контексті балансу інтересів кримінального судочинства та забезпечення гарантій прав і свобод людини. Методологія. У процесі наукових пошуків були використані наступні методи: діалектичний, логічний, догматичний, монографічний, системно-структурний, порівняльно-правовий, соціологічний, правового моделювання. Результати дослідження. Встановлено, що відповідно до розроблених та апробованих методик, під час розслідування кримінальних проваджень про корупційні злочини слідчі використовують різноманітні інформаційні системи; вивчено зміст і особливості застосування останніх. Розглянуто міжнародні документи, які

[1] Candidate of Legal Sciences, Professor of the Department of Criminal Law and Procedure of Kyiv National Aviation University (Kyiv, Ukraine).

[2] Candidate of medical Science, Associate Professor, President of Kharkiv Institute of medicine and biomedical sciences (Kharkiv, Ukraine).

[3] Ph.D in Law, Associate Professor of the Department of Criminal and Legal Disciplines of Dnipropetrovsk State University of Internal Affairs (Dnipro, Ukraine).

[4] Ph.D in Law, Associate Professor of the Department of Criminal and Legal Disciplines of Dnipropetrovsk State University of Internal Affairs (Dnipro, Ukraine).

[5] Candidate of Legal Sciences, Expert of analytical department of training of prosecutors of the Prosecutor's Training Center of Ukraine (Kyiv, Ukraine).

ECtHR on the need for a balanced approach to interference with privacy and delimitation of such interference, were studied. Practical implementation. The ways to achieve a balance of the interests of the parties in the criminal procedural legislation of European countries were investigated in order to implement their positive experience in Ukraine. Value/originality. The principles, on which the process of regulating the use of electronic search systems, databases, algorithms and artificial intelligence in the criminal procedural legislation of Ukraine should be based, are proposed.

Keywords: corruption crimes, criminal justice, electronic search systems, ECtHR, human rights.

встановлюють межі можливого використання штучного інтелекту у кримінальному судочинстві. Вивчено рішення ЄСПЛ, які стосуються необхідності збалансованого підходу до втручання у приватного життя та визначення меж такого втручання. Практичне значення. Було досліджено шляхи досягнення балансу інтересів сторін у кримінальному процесуальному законодавстві країн Європи з метою імплементації позитивного досвіду в Україні. Цінність/оригінальність. Запропоновано принципи, на яких повинен базуватися процес регламентації використання електронних пошукових систем, баз даних, алгоритмів та штучного інтелекту в кримінальному процесуальному законодавстві України.

Ключові слова: корупційні злочини, кримінальне судочинство, електронні пошукові системи, ЕСПЛ, права людини.

Introduction

The use of databases, electronic search systems, special technical means of removing information, application of software complexes and artificial intelligence for their systematization and analysis is becoming more widely used every year. Such means are constantly being improved, and the trend of digitalization of social relations is regularly increasing sources of data for law enforcement and intelligence agencies. In this regard, more and more attention is drawn to the issues related to ensuring the balance of the interests of criminal justice and the rights and freedoms of persons who experience intruding into private life. In the context of the protection of human rights and freedoms, automatic retrieval of information and creation of databases on individuals, regardless of whether they are the objects of investigations, investigative or intelligence activities, is of particular concern.

At the same time, little attention is paid to the issues of preservation, use, destruction of information that cannot be used in the interests of law enforcement, guarantees of non-interference or restrictions on interference in the private sphere, and their legal regulation. Law-making activity, the introduction of mechanisms of supervision and control over the legality of the accumulation and use of digital information, is significantly lagging behind the processes of improvement of technical means, used for this purpose.

Therefore, the aim of our article is to study the use of electronic search systems during the investigation of corruption crimes in the context of the balance of interests of criminal justice and ensuring guarantees of human rights and freedoms.

In view of the organizational problems of pre-trial investigation, in particular the investigation of corruption offenses, which affect its full and prompt implementation, the application of AI is justified and appropriate. In order to properly use modern technologies, as well as avoid the breach of human rights in the course of their application, it is necessary to examine international legal instruments governing this issue, study foreign experience on this matter, clarify how this problem is regulated in Ukrainian legislation and formulate the respective conclusions and recommendations.

Methodology

The methodological basis for the study is dialectical method of scientific knowledge, on the basis of which the examination of the application of electronic search systems in the investigation of corruption crimes is considered as a multi-stage, complex and contradictory process requiring proper regulation. Other methods used in the article are:

Logical method (analysis, synthesis, induction, deduction, analogy, etc.). It was applied for the research of the process of proving the circumstances of the commission of a corruption crime by performing a set of secret measures of obtaining information (control over the commission of crime, audio and video monitoring, interception of telephone conversations and other investigative actions, in particular, the seizure and analysis of documents, conducting interrogations, expert studies, etc.).

Dogmatic method helped to examine the content of international legal instruments regulating the limits of the possible use of artificial intelligence in criminal justice (Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Recommendation CM/Rec (2020)1 to Member States regarding the impact of algorithmic systems on human rights, Recommendation on the Ethics of Artificial Intelligence, etc.).

Monographic method made it possible to consider the works of the scholars, who investigated the issues of using electronic search systems and ensuring the balance of State interests and guarantees of human rights and freedoms during this process.

System and structural method was useful when studying informational systems used by the investigators during the investigation of criminal proceedings on corruption crimes (Unified State Register of Declarations of Persons Authorized to Perform the Functions of the State or Local Self-Government; information System “Arkan”; information and telecommunication System “Hart 1”; databases of the State Migration Service of Ukraine; State Registry of Real Property Right; Unified State Register of Vehicles; “Safe City” et al.).

With the help of comparative and legal method the rules of criminal procedural legislation of other countries ensuring a balance of the interests of criminal justice and guarantees of human rights and freedoms in the course of electronic search of information were reviewed (Germany, Great Britain, China, Singapore).

Sociological methods were applied when studying the decisions of the ECHR on this topic (Szabó and Vissy v. Hungary (2016); Centrum för rättvisa v. Sweden (2021); Tretter and others v. Austria (2010); Ringler v. Austria (2010); “Azer Ahmadov v. Azerbaijan” (2021); “Big Brother Watch and Others v. the United Kingdom” (2021)).

Legal and modelling method was used for determining the principles of regulating the application of electronic search systems, databases, algorithms and artificial intelligence in criminal procedural legislation.

Literature Review

The issues of using electronic search systems, ensuring the balance of State interests and guarantees of human rights and freedoms are the object of the research by a number of recognized experts and scientists. In particular, Hans Born and Aidan Wills (2012) examined them in the activities of intelligence services.

Cahn and Veiszlemleinin (2020) studied these problems within the application of digital technologies to monitor human movement, which were used during the COVID-19 pandemic. The authors stated that different biases in various types of surveillance operations should be taken into account as they may result in significant discrimination.

The issue of ensuring the rights and interests of the person under “digitalization” of criminal proceedings became the subject matter of scientific research in the work by Demura, Klepka and Krytska (2020). The article identifies and characterizes perspective vectors of digital transformation of pre-trial investigation through the prism of ensuring the rights and legitimate interests of the individual.

The research by Kaplina, Raimundas and Shumylo (2019) deals with the topical for modern science of criminal procedural law and law enforcement practice question of use in criminal procedure digital evidence.

Kireeva, Makhlai and Basalyk (2023) studied the issue of using of databases in the work of a criminal analyst of an operational search unit. They provided the concept of information-analytical system and characterized the main databases used by criminal analysts in their daily work and the procedure for their application.

Problematic issues related to the use of electronic evidence in the criminal procedural law of Ukraine were considered by Anheleniuk (2023). The Author draws special attention to the shortcomings of the regulation of the electronic evidence use in the legislation of Ukraine and the possibilities of their overcoming.

The monography by Skrypnyk (2022) is devoted to the use of information from electronic media in criminal procedural evidence. The author analysed theoretical foundations and foreign experience of using digital information in criminal procedural evidence. The emphasize is placed on digital information as a means of proof under the criminal procedural legislation of Ukraine.

Despite a significant number of works, the key theoretical and practical aspects of the use of databases on the benefit of criminal justice when investigating corruption offences have not yet been covered. The reason for this is the lack of comprehensive scientific work aimed at highlighting and finding solutions to the most significant problems in this area.

Results and Discussion

The conventions of the UN and the Council of Europe emphasize the need for law enforcement agencies to have effective means of effective means of evidence collection, with the possibility of conducting covert surveillance, the use of special investigative tools, access to financial information, means of detecting, tracking and seizing proceeds of crime. Accordingly, specialized bodies to combat corruption have special powers that are not available to ordinary law enforcement officers. At the same time, the implementation of such broad powers should be carried out in compliance with international human rights standards and be subject to external control (OECD, 2007).

Ensuring objective and comprehensive investigation of the circumstances of corruption crimes requires the prosecution to direct the investigation in such main areas as: 1) establishing the circumstances of the wrongful benefit, the wrongful removal/misappropriation of funds, property, providing preferences to third parties, which is defined as the direct object of the evidence of elements of a criminal offence; 2) investigation of the suspect's life style, his or her circle, the range of his (her) responsibilities, ownership of assets, including those held by front-line persons, which enables to reveal other facts of corrupt acts and enforce the sentence on the confiscation of property; 3) taking measures to locate the person suspected of committing a corruption criminal offense and is evading investigation and trial.

Proving the circumstances of the commission of a corruption crime is carried out by conducting a complex of covert measures for obtaining information: control over the commission of crime, audio and video monitoring, interception of telephone conversations and other investigative actions, in particular, the seizure and analysis of documents, conducting interrogations, expert studies, etc.

Establishing the facts of corruption, the circumstances contributing to it, as well as investigation of the suspect's lifestyle, his or her circle, ownership of assets and his (her) whereabouts in case of evading the investigation and trial, requires first of all the use of investigative measures involving electronic resources to obtain information. A significant part of information about the person, his (her) lifestyle, connections, status is contained in open sources (Internet), as well as in special software complexes and databases of law enforcement agencies, State institutions, and commercial enterprises.

According to the developed and tested methods, in the investigation of corruption crimes, investigators use various information systems: the Unified State Register of Legal Entities, Individual Entrepreneurs and Public Organizations containing information on registered business entities, ownership structure, including beneficiaries;

The Unified State Register of Declarations of Persons Authorized To Perform The Functions Of The State Or Local Self-Government, where the information on property, income, expenses, financial obligations, private interests of all public servants can be found;

The Information System "Arkan" and the Information and Telecommunication System "Hart 1" are used to establish the fact of crossing the state border of Ukraine, as well as the vehicle and persons who crossed the border with the suspect;

Application of the databases of the State Migration Service of Ukraine allows the investigators receive information on the provision of any administrative services, including those related to the issuance or exchange of passport or temporary residence document.

State Registry of Real Property Right provides information on real estate objects owned by the person on the property rights, are either leased or otherwise entitled to use.

The subdivisions of the Ministry of Internal Affairs receive information regarding the possession of vehicles from the Unified State Register of Vehicles.

Information on the person’s travel routes, in particular using vehicles, can be obtained upon the request from the “Safe City” information system.

Information about mobile terminal telephone connections is obtained for the purpose of establishing contacts and location during communication. Business entities providing services related to the delivery of correspondence may, can, upon request, present necessary information for the purpose of establishing the telephone numbers used by the person or his (her) location, addressees of postal correspondence.

Profiles in social networks are also investigated to establish the photo and video materials, other information that can be used to determine the persons’ location and connections.

On behalf of investigators and prosecutors, National Agency of Ukraine for finding, tracing and management of assets derived from corruption and other crimes (ARMA) is authorized to collect information about the person’s assets. ARMA has access to information, documents, automated information and reference systems, registers and data banks that are at the disposal of local self-government; data on the availability and status of accounts, transactions in banking institutions, professional capital market participants, organized commodity markets, foreign States agencies, enterprises, institutions and organizations, including banks, depository and financial institutions, private executors, auditors, notaries, appraisers, as well as experts, arbitration managers, liquidators, persons authorized by the Fund for Guarantee of Deposits of Natural Persons.

ARMA can receive information in an automated, remote mode and perform analysis of open data sources (OSINT) both in Ukraine and abroad. It also gets access to paid databases, uses information from social networks, mass media, journalistic information and other data from open sources. The basis for collecting and analysing information is a written request from an investigator, prosecutor or head of a pre-trial investigation body (Babikov et al., 2024).

The application of the “ANDE RAPID DNA” system enables law enforcement agencies to perform automated interpretation of DNA identifiers directly at the scene, as well as their profiling in less than two hours, which is actively used by investigative units of the National Police and Security Service for the purpose of identifying the person. With the help of this equipment, it is possible to examine samples of epithelium from the oral cavity, blood stains, saliva, other biological traces from objects touched by the person.

The information subsystem “BLOKPOST” provides an opportunity (based on the relevant request), to search for the person on the territory of Ukraine by guiding and providing access to information about the wanted person to all police officers on their own technical devices.

A significant amount of information about the person is also contained in the search systems of technological IT giants: Google, Facebook, Apple, Microsoft, which accumulate and store information about the user’s location, behavior, requests, income, political views, racial and ethnic affiliation, correspondence and metadata text messages (Forklog, 2020).

The information accumulated in the “Diia” electronic application makes it possible to explore a fairly wide range of issues related to social behaviour: bringing to administrative responsibility, participation in legal proceedings, existence of enforcement proceedings, tax debt. Taking into account that the entry to the "Diya" application is related to the provision of banking services, such as “Privat24”, it is additionally possible to establish the IP addresses from which the person entered with the verification of his (her) identity.

Along with this, information gathering can be carried out by using malicious software, the application of which is performed by separate installation on the computer equipment of the subject of the investigation, with the aim of obtaining information contained on his (her) devices or using them as covert means of receiving and recording audio and video information on the content of conversations or events occurring around such a device by unauthorized activation of the user’s microphone and webcam.

It is the amount of information contained in electronic information systems, databases, as well as obtained from other technical means and software complexes, that determines the need to use certain algorithms and artificial intelligence to optimize the search and systematize data important for criminal proceedings.

This led to the spread of OSINT information search systems, implementing the technology of data collection and analysis from open sources, which is used in the interests of criminal justice by law enforcement officers.

OSINT is positioned as an exploration among available sources covering any information. The data about person, business entity can be obtained on legal grounds from free public sources. Generally, it is information from the Internet, but can also include data contained in open libraries, newspaper articles, press releases, and stored on various types of media. Based on the form of fixation, the search objects can be texts, film, photo, video recordings, materials located on websites about webinars, public events, conferences (Softlist, 2022).

The main sources of information, which help to create a profile of the object, are social networks, blogs, video hosting, forums, magazines, newspapers, television, radio, public materials of state structures, publicly available observations, reports, articles, reports, conferences, and information with limited access (regarding banking transactions, telephone connections, travel routes, real estate owned or used by a person, or people of his (her) circle and connections).

On the basis of the profile, pre-trial investigation bodies can establish the whereabouts, hidden assets, possible accomplices who facilitated or directly participated in the commission of corrupt acts, as well as receive other information that is not directly related to the subject matter of pre-trial investigation, but is related to private life and is sensitive for the person.

At the same time, according to the legislation of Ukraine, just the access to information on telephone connections and removal of information from electronic information systems and their parts, the access to which is restricted by logical protection system without the knowledge of the owner or user, requires the permission of the investigating judge; the implementation of other means does not need such authorization. The rest of the information from the databases can be obtained either at the request of the investigator, the prosecutor, directly through an electronic office, or by examining mobile devices, including using portable hardware and software complexes for forensic research, which allows to extract, decode and analyse evidence.

Therefore, acquisition and recording significant amount of electronic information for the benefit of criminal justice in Ukraine is outside the scope of judicial control, and the development of technologies for collecting electronic evidence is substantially ahead of the regulation of such activities by criminal procedural legislation.

It should be noted that the ECHR has repeatedly emphasized the need for a balanced approach to the interference in private life and defining its limits.

In the case of Szabó and Vissy v. Hungary (2016), which concerned Hungarian legislation regulating secret anti-terrorist surveillance for national security purposes (in particular, “section 7 / E (3) Surveillance”), the applicants complained that they could be subjected to unreasonable and to offensive measures; the introduced regulations do not rule out abuse in the absence of judicial control.

The court, recognizing the violation of Article 8 of the Convention, stated that under current conditions, the fight against terrorism requires the government to resort to advanced technologies, including those enabling mass surveillance of citizens’ telecommunications to prevent crimes. Such wiretapping, given new technologies that allow the government to easily intercept masses of data, even on individuals outside the primary range of operations, could be applied to any Hungarian citizen. Besides, the Court drew attention to the fact that the permission to carry out the mentioned measures took place within the scope of the executive power, without assessing whether the interception of communications is strictly necessary in the absence of a judicial. Accordingly, in the opinion of the Court, Hungarian legislation did not provide safeguards to prevent abuse.

Notably, the Court also stated that there had been no violation of Article 13 (right of an effective remedy) of the Convention along with Article 8, reiterating that Article 13 could not be interpreted as requiring a remedy against the state of domestic law.

In terms of determining the procedure for access to biological samples, in addition to the generally recognized objects (blood, saliva, nails, hair, sperm, suturing agent, bucal epithelium etc.), it also refers to fingerprints, handwriting, speech and voice of a person, traces of a person’s scent and others.

This view is primarily due to the fact that the purposeful search and collection of information about a person and his (her) life as an intervention in the most sensitive sphere, requires a balanced approach.

There are a number of other cases related to complaints about the collection and processing of personal data by law enforcement authorities brought before the ECtHR: Centrum för rättvisa v. Sweden (2021): a non-profit public interest law firm complains about Swedish state law concerning the secret surveillance of citizens;

Tretter and others v. Austria (2010). The case concerns amendments to the Law on State Authorities in Police Affairs, which entered into force in January 2008 and expanded the powers of law enforcement agencies to collect and process citizens' personal data;

Ringler v. Austria (2010) deals with the violation of the right to respect for private life and correspondence, the right to an effective remedy in similar matters.

In the case "Azer Ahmadov v. Azerbaijan" (2021), the Court drew attention to the fact that conduct of secret measures for obtaining information must contain personal data of the person in respect of whom they are conducted. Otherwise, it violates his (her) right to privacy guaranteed by the Convention.

In the case "Big Brother Watch and Others v. the United Kingdom" (2021), the applicants – 3 non-governmental organizations, a researcher, working internationally in the field of privacy and freedom of expression, and investigative journalists, alleged that they were likely subjects of surveillance by the UK intelligence services. Their fears sparked media interest after Edward Snowden's revelation, who is the former system administrator for the US National Security Agency (NSA).

During the consideration of the case, the Court examined three aspects of monitoring:

1) large-scale interception (monitoring) of telecommunications;
2) exchange of received intelligence information between the countries;
3) receiving communication data (billing information) from telecommunications operators and providers.

In the Decision, the Court stated that in accordance with the national legislation of the Great Britain, there were certain stages of the monitoring process, which included: interception of messages transmitted by telecommunications channels; real-time application of filters to determine the significance of intercepted information; analysis of selected and stored material by an analyst.

The ECtHR previously found no abuses on the part of the United Kingdom's intelligence services; however, it identified insufficient independent oversight of the selection and retrieval processes, in particular information filtering criteria for subsequent selection and verification of intercepted data.

Following this, the court concluded that the national legislation did not meet the requirement of the "quality of law" and the criterion of "necessity in a democratic society".

As for the receipt of billing information from telecommunications operators, the ECtHR drew attention to the fact that the legislation of the European Union requires such procedure to be limited to the purpose of combating serious crime, and access to such data had to be previously authorized by a court or other independent administrative body.

And in this matter, the domestic legislation of Great Britain turned out to be inappropriate, since it did not contain such guarantees, and the ECtHR did not find any violations in the existing procedure for exchanging intelligence information.

Non-governmental organizations have also repeatedly criticized experiments with the use of algorithms in criminal proceedings for the purpose of characterizing the person, on which the reservation in the European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment on the use of such algorithms with special restrictions is based.

Therefore, it is necessary to highlight two key issues in the context of research on the regulation of electronic search, collection and use of information on the person in criminal proceedings: 1) ensuring the balance between the interests of criminal proceedings and the guarantees of human rights and freedoms; 2) the limits of the possible use of algorithms, artificial intelligence for obtaining conclusions, individual profiles of a person, the influence of such information on making legal decisions in criminal proceedings.

To some extent, the issue of the balance of interests in the criminal procedural legislation of European countries has found its solution. Thus, in the Federal Republic of Germany (FRG), the search measures of law enforcement agencies have been formally defined as some form of tacit measures of obtaining information under the name “electronic search”.

Chapter VIII “Seizure, control of telecommunications, computer search for possible offenders based on common indicators, application of technical means, use of undercover investigators and searches” of the German Criminal Code (Federal Ministry of Justice, 1998) of the Federal Republic of Germany defines system of secret measures of information, which includes: 1) seizure (the objects of which among others include computer files, electronic messages); 2) automatic comparison and transfer of personal data; 3) comparison of information for the investigation of the criminal act; 4) seizure of postal and telegraphic dispatches; 5) control of telecommunications; 6) measures applied without knowledge of the person to whom they apply (recording of conversations in publicly inaccessible places); 7) statements made in private outside housing; 8) receiving information about communication within the framework of telecommunications; 9) other measures applied without the knowledge of the person to whom they relate (monitoring); 10) measures applicable to mobile phones.

At the same time, such a measure as an online search using special software is not an element of the criminal procedure; it is regulated by other federal laws.

Automatic comparison and transfer of personal data, which involves the collection and analysis of information on the person from various databases, can be applied in cases where there are grounds to believe that a criminal act of a significant degree of danger has been committed.

Investigating the grounds for conducting such a measure, one should note a key criterion for recognizing the legality of interference in private life. Thus, the Constitutional Court of the Federal Republic of Germany, on the basis of an analysis of the content of secret forms of obtaining evidence in criminal proceedings, drew attention to the fact that when using the obtained evidence the first line of reference is to determine in which area such interference occurred and distinguished the following spheres: 1) social sphere (business relationships); 2) private sphere (private conversations, actions and communication in the domestic sphere, etc.); 3) intimate sphere (Holovnenko & Spitza, 2012).

Social contacts in the first sphere do not require special protection. In the second area, the interests of criminal proceedings must be weighed against the protection of the private. Interference in the intimate sphere is prohibited.

That is, the principle of proportionality is defined as one of the key criteria in the criminal procedural legislation of the Federal Republic of Germany when clarifying the existence of grounds for conducting special investigative actions.

The collection and accumulation of information in Great Britain for the benefit criminal justice is regulated by the Investigative Powers Act (Legislation, 2016), which gives broad powers to law enforcement agencies to collect, store, and analyse information, including the right to access banking, commercial information, intrusion into telephones, computers, as well as mass accumulation of personal data, including data on visits to certain Internet resources with the approval of the judge. A limited circle of law enforcement officials authorized to carry out such measures is also defined, and criminal liability for the abuse of such powers is established.

Analysis of the activities of law enforcement agencies of several other countries of the world authorized to prevent and combat corruption indicates that they use a wide range of databases and sources of electronic information in their activities.

Thus, the Independent Commission Against Corruption (Hong Kong) has the right to follow up on a court order and detect illegal financial transactions and assets hidden by a corrupt person in any form. These powers include checking bank accounts, conducting searches and seizing documents, as well as the right to require suspects to provide detailed information about their assets, income and expenses.

Special investigators of the Bureau for the Investigation of Corruption (Singapore) following the instructions of the prosecutor, the Director of the Bureau for Special Powers, may obtain access to the bank’s documentation, request any information on property in use or belonging to him or her or close persons, bank transfers or cash withdrawals, collect and analyse information on business activities, etc. (OECD, 2007).

Considering the aspects of searching, collecting and using information on the person on the benefit of criminal justice, an extremely important trend of spreading the use of artificial intelligence during such activities and the consequences of the risks involved should be taken into account. As noted by the Secretary General of the Council of Europe Marija Pejčinović Burić, artificial intelligence is already with us: it changes the information we receive, influences our choices, and in the nearest future it will influence the work of governments and state institutions even more. Artificial intelligence presents both benefits and risks. The role of the Council of Europe is to ensure the protection and development of human rights, democracy and the rule of law in the digital environment (Council of Europe, 2023).

Determining the limits of the possible use of artificial intelligence in criminal justice remains quite problematic; however, the first steps of regulation the development of the basic principles of its use have already been taken at the international level.

Thus, the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Council of Europe, 1981) introduced the basic principles of data protection, including: integrity of data collection and processing; their storage only for specified and lawful purposes; non-use in a manner that is incompatible with these purposes; to be adequate, appropriate and not excessive in relation to the purposes for which they are stored; to be kept in a form allowing the identification of data subjects no longer than is necessary for the purposes of storage. However, there is a reservation that even in the interest of criminal proceedings automated processing of data on racial affiliation, political, religious or other beliefs, as well as data relating to health and sexual life is prohibited, if domestic legislation does not provide appropriate guarantees (Article 6 of the Convention).

As involving AI in the sphere of justice raises a number of ethical issues, an important international act governing them was adopted – the European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment (European Commission for the Efficiency of Justice, 2018). The main purpose of the Charter is to increase the efficiency and quality of the administration of justice by processing the algorithms of court decisions and data while respecting the basic rights and freedoms guaranteed by the ECHR and the Council of Europe Convention on the Protection of Personal Data.

The Charter establishes five principles regarding the use of artificial intelligence in the administration of justice:

- the principle of observing basic human rights when using AI.
- the principle of non-discrimination, namely prevention of any discrimination between individuals or groups of individuals.
- the principle of quality and security, which requires the processing of court decisions and data in a secure technological environment.
- the principle "under the control of the user".
- the principle of transparency, impartiality and fairness.

Based on the mentioned Convention, the Committee of Ministers of the Council of Europe issued Recommendation CM / Rec (2020) 1 to Member States regarding the impact of algorithmic systems on human rights, which provides guidelines and the algorithm of necessary actions for effective protection of human rights and personal data. The measures provide for the legislative regulation of issues of access and use of information and the obligation of users and processors of personal data to submit adequate documentation to verify compliance with the law.

In addition, the Recommendation on the Ethics of Artificial Intelligence (UNESCO 2021) proposed the following basic conditions for the use of artificial intelligence, particularly those that may apply to criminal justice: 1) privacy must be respected, protected and encouraged at all stages of the use of artificial intelligence systems. The collection, use, transfer, storage and removal of data in such systems is carried out taking into account the standards of international law, regional and national norms; 2) the framework principles of data protection and their management mechanisms should be developed on the basis of the principles of multi-stakeholder interest, protected by judicial systems, and based on international principles of data protection and standards regarding the collection, use and disclosure of personal data, provided that there are legal purpose and the appropriate legal basis for processing; 3) algorithmic systems require ppproperly assessing the privacy implications, and the actors of artificial intelligence are obliged to ensure accountability in the development and implementation of such systems, protecting personal information throughout the life cycle of such systems; 4) the control of artificial intelligence systems is not just about control by individual persons, but also, in necessary cases, inclusive control by society; 5) delegating the control of artificial intelligence systems can be limited in number and do not deal with crucial issues; 6) the transparency and comprehensibility of such systems is a guarantee of the realization of the right to a fair trial; where there are substantial risks of adverse effects on human rights, the principle of transparency may be the basis for the disclosure of algorithms or databases.

Conclusion

The use of electronic search systems during the investigation of corruption crimes is an effective tool contributing to the performance of criminal justice tasks, which provides quick, objective investigation of the circumstances of the case, establishes the whereabouts of the person, evading pre-trial investigation and trial, identifies assets and ensures execution of punishment through confiscation of property.

Along with this, such activity is related to interference in private life and significantly limits human rights and freedoms. Accordingly, the use of electronic search systems, databases, algorithms and artificial intelligence is subject to detailed regulation in criminal procedural legislation, taking into account such principles as:

1) Balancing the interests of the criminal justice system and human rights and freedoms, thus limiting, collecting and using information as an exceptional measure due to the gravity of the offence;
2) decision on permission to search for, collect and use private information must be considered as a form of tacit receipt of information with the introduction of an appropriate judicial control;
3) application of algorithms, artificial intelligence for searching, collecting and analysing information cannot replace a person, whose sphere of control includes interpretation and conclusions regarding the information obtained;
4) misuse of databases by law enforcement agencies, software complexes allowing interference in the person’s private life, including their application without necessary legal grounds, is subject to criminalization, and results obtained shall not be admissible as evidence of guilt.

Bibliographic References

Anheleniuk, A. (2023). The use of electronic evidence in the criminal procedural law of Ukraine (problematic issues). *Uzhhorod National University Herald Series Law, 2*(79), 214-218. DOI: 10.24144/2307-3322.2023.79.2.32

Azer Ahmadov v. Azerbaijan. (App No. 2309/10). *European Court of Human Rights* (2021, July 22). Retrieved from: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-211101%22]}

Babikov, O., Bozhyk, V., Bugera, O.I., Kyrenko, S.H., & Viunyk, M. (2024). Balancing Interests: Criminal Proceedings & Private Life Interference Under Martial Law in Ukraine. *German Law Journal*, 1-25. Retrieved from: https://acortar.link/KTo4cD

Big Brother Watch and Others v. the United Kingdom (Applications Nos. 58170/13, 62322/14, and 24960/15). *European Court of Human Right*s. (2021, May 25). Retrieved from: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-210077%22]}

Born, H., & Wills, A. (2012). *Overseeing Intelligence Services: A Toolkit.* Geneva: DCAF. Retrieved from: https://acortar.link/hlnusf

Cahn, A.F., & Veiszlemlein, J. (2020). *COVID-19 tracking data and surveillance risks are more dangerous than their rewards.* NBC News. Retrieved from: https://acortar.link/3OmeLF

Centrum för rättvisa v. Sweden (App No. 35252/08). *European Court of Human Rights*. (2021, May 25). Retrieved from: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-210078%22]}

Committee of Ministers (2020). *Recommendation CM/Rec (2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, adopted at the 1373rd meeting of the Ministers' Deputies*. Retrieved from: https://rm.coe.int/09000016809e1154

Council of Europe (1981). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Retrieved from: https://rm.coe.int/1680078b37

Council of Europe (2023). *The Council of Europe and artificial intelligence*. Retrieved from: https://acortar.link/P54PqF

Demura, M., Klepka, D., & Krytska, I. (2020). Ensuring of the rights and legal interests of the person in the conditions of “digitalization” of criminal proceedings. *Law*

Review of Kyiv University of Law, (1), 295-301. https://doi.org/10.36695/2219-5521.1.2020.59

European Commission for the Efficiency of Justice (2018). *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment, adopted at the 31st plenary meeting of the CEPEJ, 03 – 04 December 2018*. Retrieved from: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c

Federal Ministry of Justice (1998). *German Criminal Code in the version published on 13 November 1998* (Federal Law Gazette I, p. 3322), as last amended by Article 2 of the Act of 22 November 2021 (Federal Law Gazette I, p. 4906). Retrieved from: https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html

Forklog (2020). *Big brother is watching you or how corporations profit from our data*. Retrieved from: https://acortar.link/LNtrn5

Holovnenko, P., & Spitza, N. (2012). *Code of Criminal Procedure of the Federal Republic of Germany – Strafprozessordnung (StPO): Scientific and practical commentary and translation of the text of the law*. Potsdam. University Press Potsdam. Retrieved from: https://acortar.link/JMuRpY

Legislation (2016). *Investigatory Powers Act 2016*. Retrieved from: https://www.legislation.gov.uk/ukpga/2016/25/contents

Kaplina, V.A., Raimundas, J., & Shumylo, M.Ye. (2019). Informational theory of evidence and the problems of using the electronic means of proving in criminal procedure. *Journal of the National Academy of Legal Sciences of Ukraine, 26*(2), 118-130. 10.31359/1993-0909-2019-26-2-118. Retrieved from: https://acortar.link/JhLOsJ

Kireeva, O.S., Makhlai, O.M., & Basalyk, S.A. (2023). Use of databases in the work of a criminal analyst of an operational search unit. *Scientific innovations and advanced technologies, 13*(27), 221-233. https://doi.org/10.52058/2786-5274-2023-13(27)-221-233.

OECD (2007). *The Anti-Corruption Network for Transition Economies. Specialized anti-corruption institutions: examination of models.* Retrieved from: https://www.oecd.org/corruption/acn/39972270.pdf

Prokhazka, H., & Melnyk, O. (2023). Implementation of AI in international law and administrative law (in the context of human rights protection). *Amazonia Investiga, 12*(67), 66-77. https://doi.org/10.34069/AI/2023.67.07.6

Ringler v. Austria ECHR. (App no. 2309/10) *European Court of Human Rights.* (2010, 12 January). Retrieved from: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-120348%22]}

Skrypnyk, A. V. (2022). *Use of digital information in criminal procedural evidence*: monograph. Kharkiv: Pravo. https://doi.org/10.31359/9789669982940. Retrieved from: https://acortar.link/qn9qmG

Softlist (2022). *OSINT: open source data collection and analysis technology*. Retrieved from: https://acortar.link/ZV0psc

Szabó and Vissy v. Hungary (App No. 37138/14). *European Court of Human Rights.* (2016, January 12). https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-160020%22]}

Tretter and others v. Austria (App No. 3599/10). *European Court of Human Rights*. (2010, January 15). Retrieved from: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-120352%22]}

UNESCO (2021). *Recommendation on the Ethics of Artificial Intelligence*. Retrieved from: https://unesdoc.unesco.org/ark:/48223/pf0000380455