# COLLECTION AND USE OF INFORMATION BY COUNTER-INTELLIGENCE IN THE CONTEXT OF HUMAN RIGHTS PROTECTION: CASE OF UKRAINE

**ANTONINA DIMICH**[1]
**VALENTYN PETROV**[2]
**IVAN SLIUSARCHUK**[1]
**NATALIIA MISHCHYSHYN**[1]
**VALENTYNA FORNOLYAK**[1]

**Abstract:** Obtaining complete and reliable information during counter-intelligence activities is critical. The information extraction, analytical processing, and use of information regarding signs and facts of intelligence, terroristic, and other activities of special services of foreign states, as well as organisations, individual groups, and individuals to the detriment of the state security of Ukraine is legally established as its main task. One of the main tasks of intelligence and counter-intelligence is to collect information in the interests of national security on the facts and signs of activities that threaten the sovereignty, territorial integrity, and constitutional order of the state, that is, its main system-forming component, using all possible sources. The purpose of such information collection is to assist the executive branch of government in developing internal and external policy, as well as to develop strategic and tactical decisions in the implementation of national policy. The purpose of this study is to identify the problems of collecting and using information by counter-intelligence, to develop a strategy to overcome such problems, and to investigate the legal principles of protecting human rights in the process of this activity. The results of the study will contribute to the development of the theory of national security. The obtained definition of the legal regime for collecting and using information about an individual or legal entity regarding which counter-intelligence actions are performed will assist intelligence and counter-intelligence units in ensuring the protection of human rights.

**Keywords:** Counter-intelligence activities, human rights, freedoms, national security, Ukraine.



## 1. Introduction

The current stage of development of Ukrainian society is described by a difficult political and economic situation, which is also negatively affected by Russian aggression in the east of Ukraine. In the context of the emergence of fundamentally new threats to the national security of Ukraine, affecting the nature and specific features of the security environment, it is necessary to develop new relations between individual citizens, society, and the state. With this in mind, human rights and freedoms are given increased attention

[1] National Academy of the Security Service of Ukraine, Ukraine (a-dimich@uohk.com.cn; sliusarchuk@toronto-uni.com; nat-mishchyshyn@lund-univer.eu; v-fornolyak@lund-univer.eu).
[2] Support Service, Main Situation Center of the Office of the Rada of National Security and Defense Council of Ukraine, Ukraine (vpetrov@toronto-uni.com).

by rule-making, law enforcement, and other practices due to the need to coordinate the law-guaranteeing functions of state institutions with constitutional functions, as well as international standards in human rights protection. The problems of guaranteeing human rights in those areas that are conventionally at the intersection of public order and national security, on the one hand, and individual human rights and freedoms, on the other hand, are becoming increasingly urgent.

Counter-intelligence in this context constitutes a special type of activity of authorised state bodies and divisions in state security, contributing to the stable and progressive development of society, deterring external and internal threats to the security of Ukraine, stopping intelligence, terroristic, and other illegal actions of foreign special services, individual organisations, groups and individuals regarding the system-forming essence of the state, namely sovereignty, territorial integrity, constitutional order, etc. (Law of Ukraine…, 2003a; Prunckun, 2019; Albul et al., 2020). Considering the specific features of the purpose and objectives of counter-intelligence operations, the provisions of the current internal legislation of Ukraine make provision for the right of authorised units, solely for prevention, timely detection and suppression of intelligence, terroristic, and other attacks on the national security of Ukraine, procurement of information in the interests of counter-intelligence, to carry out appropriate measures authorised by supervisory authorities, including using secret methods of obtaining information (Law of Ukraine No. 12…, 2003a), which temporarily restrict human rights and freedoms guaranteed by the Constitution of Ukraine.

Thus, there is a need for a thorough analysis of the legal basis for restricting the human right to privacy during counter-intelligence operations (Stouder and Gallagher, 2013; Ronn, 2016; Shaffer, 2017). The study of these issues is not only of scientific significance, contributing to the development and elaboration of the theory of national security, but also of practical one, which lies in the need to develop a unified procedure for covert procurement of information on individuals and legal entities by counter-intelligence units of authorised state bodies.

The concept and content of human rights, the grounds and procedure for their restriction by authorised state bodies have been the subject of scientific research by many scientists and practitioners, namely Tertishnik (2002), Shapirko (2015), Albul, Andrusenko, Mukoida and Nozdrin (2020), Tkachuk (2018), Ukhanova (2018), Dzyoban and Zhdanenko (2020), and others. Despite the thoroughness of research, the modern research area does not contain unanimity of opinions on important issues of understanding the theoretical and legal nature of interference in private life in the interests of counter-intelligence, including the justification for the need to gather, store, and use information during counter-intelligence operations, the establishment of a special procedure for obtaining permission to conduct activities that temporarily restrict human rights and freedoms.

The purpose of this study was to investigate the legal basis of interference in human privacy upon gathering and using information by counter-intelligence, to identify current problems in this area and develop proposals for their solution.

## 2. Materials and Methods

Threats to human rights and freedoms that arise during the collection of information by intelligence agencies in the interests of national security have been thoroughly investigated by Marina Caparini (2008). This researcher claimed that there is a certain paradox in the desire for transparency in the activities of an internally closed body, which is the intelligence and special services of any state. T. Christakis and K. Bouslimani (2021) point out the necessity to keep a balance between restrictive measures in case of threats to national security and violating human rights and fundamental freedoms. However, the preservation of democratic values, especially in transition countries such as Ukraine, requires specially authorised bodies to be accountable and monitored by both the legislative and judicial branches of government, as well as by civil society and the media.

The study by Hans Born and Aidan Wills notes that the means used by intelligence agencies to collect information must correspond to the priorities and values of the society they serve. In democratic countries, intelligence agencies must respect human rights and freedoms, recognise the rule of law and adhere to the principles of democratic governance, including in terms of responsibility and accountability, transparency and collegiality in decision-making. Intelligence activities at all its stages, from problem setting to information dissemination, should be performed within these parameters (Born and Wills, 2016). In this regard, Ronnie Kasrils, in her report on the investigation of abuses by security officials in South Africa, notes that "restrictions on rights can be justified if there is a threat to national security. Such a restriction must meet the proportionality test, which corresponds, among other things, to such categories as the nature of a particular right and the importance of the purpose for which this right is restricted. As such, the possibilities of obtaining intelligence information must be balanced by guarantees of protecting the human rights of citizens and supporting an open democratic society" (Kasrils, 2008).

Therewith, the storage of information (including personal information) on actions and measures against individuals is fully justified, on the one hand, by the involvement of these individuals in illegal actions in the sphere of national security, economic well-being and the protection of human rights. On the other hand, to verify the trustworthiness of persons applying for any of the official positions and in other cases stipulated by law (LAW OF UKRAINE…, 1994; LAW OF UKRAINE…, 2003b; LAW OF UKRAINE…, 2010). Hans Born and Ian Leigh (2005) determine that the danger of procuring, storing, and using a dossier (information about a person) is that during a counter-intelligence operation there is:

a) the possibility of collecting redundant information – the data is collected without a specific purpose, in case of possible benefit in the future;
b) the possibility of obtaining false information: faulty, unjustified, or misleading;
c) the possibility of disclosure without appropriate permission: to third parties or without a reasonable purpose;
d) the opportunities and careers of individuals can be put at serious risk with no chance of preventing it.

According to the Law of Ukraine "On Counter-Intelligence Operations" (Law of Ukraine..., 2003a) the grounds for counter-intelligence activities are as follows:

1. Availability of sufficient information that needs to be verified using special forms, methods, and means on the following:

- intelligence activities against Ukraine, engaged in by special services of foreign states, as well as organisations, individual groups, and individuals;
- encroachment on the state sovereignty, constitutional order, and territorial integrity of Ukraine;
- terroristic attacks or terrorist activities, criminal offences against the peace, security of humankind and the international legal order.

2. Performance of tasks defined by law regarding the following:

- counter-intelligence support of economic, information, technological potential, military-industrial and transport complexes and their facilities, the National Communication System, the Armed Forces of Ukraine, and other military formations created in accordance with the laws of Ukraine, military-technical cooperation, compliance with international non-proliferation regimes;
- counter-intelligence support of foreign diplomatic institutions of Ukraine, the security of employees of these institutions and their family members in the host state, citizens of Ukraine sent abroad who are aware of information constituting a state secret, as well as the protection of state secrets in these institutions;
- counter-intelligence protection of state authorities, law enforcement and intelligence agencies, protection of state secrets;
- protection of embassies and representative offices of foreign states in Ukraine and their employees from terrorist attacks;
- study and verification of persons who are registered for access to state secrets, to work with nuclear materials and at nuclear installations, or involved in confidential cooperation;
- ensuring own security, including employees of bodies and divisions engaged in counter-intelligence activities, their family members and persons who facilitate and assist in the implementation of counter-intelligence activities;
- information and analytical support of state authorities (regarding threats to the state security of Ukraine).

3. The need to utilise technical means to identify and stop the operation of radio-electronic and other devices, the operation of which poses threats to the state security of Ukraine or prerequisites for the leakage of information with restricted access, as well as radio emissions of radio-electronic means used for illegal purposes.

## 3. Results

The conducted formal and legal analysis of international regulations has shown that human rights and freedoms to privacy, including protection from unjustified gathering

and dissemination of personal data, are defined as basic human rights. Being consolidated at the general and regional levels, they underlie the basic principles of the rule of law. Thus, Article 12 of the Universal Declaration of Human Rights (1948) states that no one may be subjected to unjustified interference in their personal and family life, groundless encroachment on the integrity of their home, the secrecy of correspondence, or honour and dignity. Everyone has the right to be protected by the law from such interference or encroachment (Universal Declaration of Human Rights, 1948). Subsequently, these provisions were developed in such international documents as the European Convention for the Protection of Human Rights and Fundamental Freedoms (1950), International Covenant on Civil and Political Rights (1966), American Convention on Human Rights (1969), Charter of Fundamental Rights of the European Union (2000), etc. The fundamental human rights law thus provides the basis for protecting privacy, including the collection and dissemination of information about a person, against the illegal storage of such data. Therewith, the Convention for the Protection of Human Rights and Fundamental Freedoms, ratified by the Verkhovna Rada of Ukraine (1997), defines the possibility of interference with a person's private life solely in accordance with the procedure established by law, in cases necessary for a democratic society, in the interests of national and public security or the economic well-being of the country, for preventing disorder and crime; for the protection of health or morals, or for the protection of the rights and freedoms of others (Law of Ukraine..., 1997).

In Ukrainian legislation, guarantees of human rights and freedoms are declared in Section II of the Constitution of Ukraine. The human right to privacy is ensured by Articles 29-32 of this document. Article 32 states that the collection, storage, use, and dissemination of confidential information about a person is not allowed without their consent. However, an exception is made to this right in cases defined by law and only in the interests of national security, economic well-being, and respect for human rights. Thus, the legislation emphasises that ensuring national security is a sufficient reason for restricting human rights and freedoms (Constitution of Ukraine, 1996).

Collecting information about threats to national security can directly relate to fundamental human rights. Ministerial Commission for the supervision of the intelligence services of South Africa was responsible for investigating the official crimes of employees of the National Intelligence Agency. According to a 2008 report by the Ministerial Commission, "intrusive (covert, non-public, secret) investigative measures can play a crucial role in uncovering criminal activities and uprisings, but they can be used to undermine democratic processes, obstruct legitimate political and public activities, and artificially create more favourable conditions for individual politicians and political parties" (Kasrils, 2008). In this aspect, it should be established what meaning the legislation attaches to the term "national security". Thus, according to the Law of Ukraine "On National Security", national security of Ukraine is the protection of state sovereignty, territorial integrity, democratic constitutional order, and other national interests of Ukraine from real and potential threats. At the same time, the national interests of Ukraine are interpreted as the vital interests of a person, society, and the state, the implementation of which ensures the state sovereignty of Ukraine, its progressive democratic development, as well as safe living conditions and the well-being of its citizens (Law of Ukraine..., 2003b).

Given the above, there is a risk of unjustified expansion of the powers of special services and intelligence agencies to gather, store, use, and disseminate information about an individual or legal entity, as noted by a number of scientists (Rizak, 2011). After all, the concepts of "national security" and "national interests" include a fairly wide range of issues. Mr Ronnie Kasrils identifies the following threats during secret information gathering activities in his report:

- the object of intelligence activity may never know that intrusive measures were taken against it and, accordingly, will be incapable of challenging their legality and expediency in court;
- intrusive measures are applied in an environment of strict secrecy, which does not allow supervisory authorities to effectively monitor their use and identify cases of arbitrariness and abuse of power;
- the means of collecting information may violate a person's privacy rights to a greater extent than the specific circumstances of the investigation require;
- intelligence agencies accumulate and store confidential information about the object of investigation and persons in contact with it after the investigation period has come to an end, and sometimes use this information for other purposes;
- secret means of collecting information generally violate not only the rights of the person under investigation, but also their associates, even if these persons are not the objects of the investigation.

These risks and threats have led to the establishment of international standards for the storage of personal information, such as the Council of Europe Convention "On Protection of Individuals with Regard to Automatic Processing of Personal Data". This regulation is aimed at "ensuring respect for the rights and fundamental freedoms of each person, in particular, the right to maintain confidentiality in connection with the automatic processing of personal information relevant to this person (Convention for the Protection of Individuals..., 1981).

The implementation of the Global Principles on National Security and the Right to Information at the level of national legislation (The Global Principles on National Security and the Right to Information (the Tshwane principles), 2013) allows striking a balance between the need to keep confidential the activities of certain institutions, including special services, and the right of the public to know about such activities. Among these principles, the main ones are as follows:

- information should be kept confidential only if its disclosure entails real and certain risks of substantial damaging the legitimate interests of national security (Principle 3);
- information about serious violations of international human rights and humanitarian law should be disclosed in all cases (Principle 10A);
- the public should have access to information about surveillance programmes (Principle 10E); no official should be categorically exempt from disclosure requirements (Principle 5);

- public officials acting in the public interest by exposing government abuses should be protected from retaliation (Principle 40) (2013).

In their recommendations on the implementation of international human rights standards in the legal field of Ukraine (Born and Wills, 2016), (Born and Leigh, 2005), the researchers warn against excessive expansion of the powers of intelligence services. Thus, they suggest the following steps in this area:

- any special powers of security and intelligence agencies should be clearly stipulated in the country's legislation;
- the law on special powers should be clear and comprehensive, so that the special services are not tempted to resort to those measures that are under-regulated at the legislative level;
- inclusion of the principle of expediency of using such special powers in the legislation;
- the actions of security and intelligence agencies should be properly supervised and monitored;
- all actions of special services should be based on respect for human rights and respect for the rule of law (Born and Leigh, 2005).

At present, these researchers, based on the case law of the European Court of Human Rights, have identified the following markers that can be used to verify "compliance with the law" of special powers of intelligence and counter-intelligence agencies:

1. Laws are understood as common law legislation and sub-legislation. For the provision to be qualified as a law, it must be adequately formulated to enable citizens to regulate their behaviour.
2. A law providing for the use of unlimited discretion in an individual case cannot be considered foreseeable, and such a provision cannot be considered a law. The scope of authority should be clearly defined.
3. It is necessary to establish all possible guarantees to avoid abuse of powers by the special services regarding fundamental human rights and freedoms. The legislation must define the guarantees for preventing abuse of authority established.
4. If the relevant safeguards are not prescribed in the relevant law, it should at least contain conditions and procedures for oversight by other institutions (Born and Leigh, 2005).

The conducted comparative analysis of Ukrainian and international regulations demonstrated that most of the provisions of international law are implemented in Ukrainian legislation, and the main guarantees of human rights and freedoms in the collection and storage of personal data (dossiers) during counter-intelligence operations are declared in legislative acts. Thus, to protect personal data, the Law of Ukraine "On Personal Data Protection" (2010) was adopted on 01.06.2010, which establishes the basic methods of personal data protection and contains the terminological aspect of special terms for regulating the range of public relations in this area of law. Article 1 of this

document states that it is aimed at protecting fundamental human and civil rights and freedoms, in particular the right to non-interference in personal life, in connection with the processing of personal data. This law also applies to the processing of personal data, which is performed in whole or in part with the use of automated means, as well as to the processing of personal data contained in the file cabinet or intended to be entered in the file cabinet, using non-automated means. The same regulation also declares that:

- personal data is processed for specific and legitimate purposes determined with the consent of the personal data subject, or in cases prescribed by the laws of Ukraine, in accordance with the procedure established by law;
- processing data about an individual, which is confidential information, is prohibited without prior individual's consent, except in cases prescribed by law, and only in the interests of national security, economic well-being, and human rights;
- personal data is processed in a form that allows identifying the individual whom it concerns for no longer than is necessary for the legitimate purposes for the collection or further processing (Law of Ukraine No. 34 "On Personal Data Protection", 2010).

At present, it is quite obvious that this law follows the Council of Europe Convention of 1981 and introduces the provisions of international law into the Ukrainian legal field. That is, there are sufficient grounds for collecting and storing data on a person (dossier) during counter-intelligence activities in Ukraine, and the basic provisions of international law on the protection of human rights and freedoms during such activities are recognised.

Formal legal analysis and comparative legal method of research allowed establishing that Ukrainian legislation defines the main task of counter-intelligence and intelligence activities as the extraction, analytical processing, and use of information containing signs or facts of intelligence, terroristic, and other activities of special services of foreign states, as well as organisations, individual groups and persons to the detriment of the national security of Ukraine. Information on the grounds for counter-intelligence operations may be contained in the following:

- statements and messages of citizens, persons involved in confidential cooperation, officers and officials, public organisations, media;
- the materials of pre-trial investigation and court bodies;
- requests, information and materials of special services and law enforcement agencies of foreign states, international institutions and organisations;
- materials of law enforcement agencies and other state authorities of Ukraine regarding threats to the state security of Ukraine, materials of the Security Service of Ukraine regarding the organisation, implementation, forms, and methods of terroristic, intelligence, and other activities to the detriment of the state security of Ukraine;
- requests of authorised state bodies, institutions, and organisations defined by the Cabinet of Ministers of Ukraine regarding access to state secrets and work with nuclear materials and on nuclear installations.

Therewith, according to Article 7 of this Law, specially authorised units are granted the right to public and covert identification, recording, and documenting intelligence, terroristic, and other encroachments on the state security of Ukraine, to maintain the corresponding criminal records, and the Law of Ukraine "On the Security Service of Ukraine" (Law of Ukraine..., 1992b) grants state security bodies the right to create information systems and maintain criminal records in the interests of counter-intelligence and intelligence activities within the scope and in accordance to the procedure determined by the tasks assigned to the Security Service of Ukraine pursuant to legislation.

Having analysed the legislation of Ukraine, the authors of this study concluded that despite the rather widespread use of the term "criminal records" in the Laws of Ukraine "On the Security Service of Ukraine" (Law of Ukraine..., 1992b), "On Counter-Intelligence Operations" (Law of Ukraine..., 2003a), there is no regulatory consolidation of this term. The authors of this study believe that "criminal records" in counter-intelligence should be interpreted as "the process of identifying, registering, accumulating, summarising, storing, and transmitting information concerning the facts and signs of intelligence and subversive activities of foreign special services, encroachments by individual organisations, groups, and individuals to the detriment of state sovereignty, constitutional order, territorial integrity, economic, scientific, technical, and defence potential of Ukraine, the legitimate interests of the state and the rights of citizens, as well as to ensure the protection of state secrets".

It was established that upon collecting and accumulating information, special services and intelligence agencies form dossiers on individuals and legal entities that can be processed in automated systems (Law of Ukraine..., 1992b). Under the automated system, the Law of Ukraine "On Information Protection in Information and Telecommunications Systems" (Law of Ukraine..., 1994) defines that an information (automated) system is an organisational and technical system where information processing technology is implemented through technical and software tools.

In international law, the Council of Europe Convention "On Protection of Individuals with Regard to Automatic Processing of Personal Data" (1981) provides that personal data subjected to automated processing must be:

- received and processed in good faith and legally;
- stored for specific and legitimate purposes and not used in a way that is incompatible with these purposes;
- adequate, appropriate, and non-excessive relating to the purposes for which they are stored;
- accurate and updated if necessary;
- stored in a form that allows identifying the data subjects for no longer than is necessary for storing such data (Article 5).

According to Article 7 of the same document, for the protection of personal data, appropriate security measures are taken to prevent accidental or unauthorised destruction or accidental loss, as well as to prevent unauthorised access, modification, or distribution.

Article 8 of this Convention makes provision for the right to grant any person the opportunity to:

- inquire about the existence of a personal data file for automated processing, its main purposes, as well as the identity and permanent place of residence or the main place of work of the file controller;
- receive, after reasonable periods and without excessive delay or cost, confirmation or refutation of the fact of storing personal data concerning this person in a data file for automated processing, as well as receive such data in an accessible form;
- require, where appropriate, the correction or destruction of such data if it was processed contrary to the provisions of internal legislation that enact fundamental principles of respect for human rights;
- use remedies in case of failure to comply with the request for confirmation or, where appropriate, to provide, correct, or destroy personal data.

The convention also provides that the restriction of human rights and freedoms in a democratic society is a necessary measure in the following cases: protection of state and public security, financial interests of the state or the fight against criminal offences; and protection of the data subject or the rights and freedoms of others.

It is quite evident that Ukrainian legislation makes provision for a somewhat wider scope of issues allowing for restrictions on human rights and freedoms upon of processing their personal data in the interests of national security. Furthermore, the Law "On Counter-Intelligence Operations" (Law of Ukraine..., 2003a) does not make provision for sufficient conditions for entering and storing personal data in criminal records, and the Law of Ukraine "On the Security Service of Ukraine" (Law of Ukraine..., 1992b) and Criminal Procedural Code of Ukraine (Law of Ukraine..., 2013) do not provide for such conditions. In addition, Ukrainian legislation does not set time-limits for storing information regarding an individual or legal entity in information systems or criminal records of special services. Only the Criminal Procedural Code of Ukraine makes provision that materials of criminal proceedings obtained as a result of covert intelligence operations which the prosecutor does not consider necessary for further pre-trial investigation should be immediately destroyed based on this prosecutor's decision. Furthermore, there is a ban on the use of such materials for purposes not related to criminal proceedings (Criminal Procedural Code of Ukraine, 2013).

And, while Chapter 21 of the Criminal Procedural Code of Ukraine requires to notify the object of covert intelligence operations to conduct such activities, there is no provision for the notice of a person regarding the collection and accumulation of personal data by special services and intelligence agencies. The academia has come across a new task, to strike a balance between the requirements of a democratic society for the protection of fundamental human rights and freedoms and ensuring national security.

## 4. Discussion

The issue of the legality of collecting and accumulating information about individuals and legal entities by special services and intelligence agencies is debatable. Thus, M. Rizak (2011) highlights in his developments the following legitimate conditions for restricting human rights upon processing information regarding a person in question in databases:

1. Restrictions are imposed based on the law.
2. Restrictions are necessary in a democratic society.
3. Restrictions must pursue one of the following goals:

- ensuring national security, including ensuring defence capability and public order in the state;
- ensuring economic security, if it is required by an important economic or financial interest of the state (including in the field of monetary, budgetary, and tax policy);
- ensuring the protection of the data subject or the rights and freedoms of others, including for detection, prevention, and investigation of crimes;
- implementation of scientific research or creation of statistics, provided that there is clearly no risk of violation of the privacy of data subjects and restriction of access to this data for a period of time not exceeding the period necessary for the implementation of such a goal, ensuring the right of the data subject to establish the existence of such a personal data file for automated processing, to learn about its main purposes, as well as to know about the person and permanent place of residence or the main place of work of the file controller (Rizak, 2011). The authors of this study agree with the opinion of this researcher that the legislation of Ukraine should make provision for a clearer definition of sufficient conditions for restricting human rights and freedoms upon processing information about a person in question in information systems, including special and intelligence agencies.

The legitimacy of the conditions of such restriction would ensure respect for human rights and freedoms during counter-intelligence operations. The democratic values based on which Ukraine builds its state system make provision for the proportionality of certain restrictions on human rights and freedoms to the challenges and threats that special authorised bodies counteract. It is to solve this problem that the studies of Ukrainian researchers should be aimed at. Article 9 of the Law of Ukraine "On Counter-Intelligence Operations" (Law of Ukraine..., 2003a) contains a direct prohibition on publishing or providing (disclosing) the collected information, as well as information on conducting or not conducting counter-intelligence activities and measures relating to a certain person until a decision is made on the results of such activities or measures.

In addition, researchers are debating on the definition of what should be considered as information about an individual. According to Article 11 of the Law of Ukraine "On Information", information about an individual is information about an individual who is

identified or can be specifically identified (Law of Ukraine..., 1992c). T.I. Obukhovska defined basic data about a person (personal data) as follows: nationality, education, marital status, religion, health status, as well as address, date, and place of birth. Sources of documented information about a person are documents issued in his or her name, documents signed by them, as well as information about the person collected by state authorities and local self-government bodies within the limits of their powers (Obukhovska, 2014).

M. Rizak (2011) believes that information about a person (personal data) constitutes a type of information that emphasises the individuality of each person, and also contains universal biological and social properties of an individual, and the defining feature of personal data is the ability to use this data to identify a particular person. Thus, the emergence of human rights in the field of processing information about a person in databases is inextricably linked with the moment when a sufficient array of information about an individual is accumulated in a particular database to identify them. The authors of this study believe that a definition more appropriate to international standards is the one provided in the Law of Ukraine "On Personal Data Protection" (2010), personal data information or a set of data about an individual who is identified or can be correctly identified.

As previously noted in this study, respect for fundamental human rights and freedoms is a democratic value that the state protects. Information about a particular person accumulated in information systems and databases is the property of a particular person and all actions relating to such data must be performed exclusively with this person's consent, except in cases stipulated by law. Nevertheless, the legislative discourse continues to discuss the sufficiency of information that is subject to legal protection. Part 2, Article 14 of the Criminal Procedural Code of Ukraine (2013) refers to personal data as "private life of citizens, secrecy of correspondence, telephone conversations, and telegraph messages." And according to Article 9 of the Law of Ukraine "On Law Enforcement Intelligence Operations" (Law of Ukraine..., 1992a), as well as Article 11 of the Law of Ukraine "On Counter-Intelligence Operations" (Law of Ukraine..., 2003a), under the protection of the law fall not just information about the personal life, but also information concerning the person's honour and dignity. But no regulation defines exactly which set of information concerns honour and dignity.

Another controversial issue is the notice of the Commissioner for Human Rights of the Verkhovna Rada of Ukraine on the commencement of processing information about an individual or legal entity. Thus, Article 9 of the Law of Ukraine "On Personal Data Protection" (Law of Ukraine..., 2010) defines the obligation of the owner of personal data to notify the Commissioner on the processing of personal data, which poses a particular risk to the rights and freedoms of personal data subjects, within thirty working days from the date of the commencement of such processing. The Commissioner for Human Rights identifies the types of personal data processing that pose a particular risk to the rights and freedoms of personal data subjects, as well as the categories of subjects to whom the notification requirement applies.

The procedure for notifying the Commissioner for Human Rights of the Verkhovna Rada of Ukraine on the processing of personal data, which poses a particular threat to the rights and freedoms of personal data subjects, on a structural division or responsible

person organising work relating to the protection of personal data during their processing, as well as the disclosure of this information, approved by the Order of the Commissioner No. 1/02-14 of 08.01.2014, defines among such data the personal data regarding the following:

- bringing to administrative or criminal responsibility;
- application of pre-trial investigation measures against a person;
- taking measures against a person stipulated by the legislation of the Law of Ukraine "On Law Enforcement Intelligence Operations";
- location and/or ways of movement of the person.

This information can be accumulated in the information systems of special and intelligence services, but the legislation does not make provision for a mechanism for such notice, and given that information on conducting counter-intelligence operations can be provided only after a decision is made on its results (which may exceed the time limit established by law), in practice compliance with such a provision is problematic. Shapirko investigated the mechanism for obtaining permission to gather personal data about a person upon intelligence operations. The basis for such a gathering is the court's permission to hold such an event, and the prosecutor's office and the court are responsible for overseeing compliance with the rule of law. Quite rightly, the researcher notes that "the results of intelligence operations that, in accordance with the legislation of Ukraine, constitute a state secret, as well as information concerning the personal life, honour, and dignity of a person, are not subject to transfer and disclosure" (Shapirko, 2015). In this case, it is logical to obtain court permission to collect information about a person from open sources, without conducting cover intelligence operations because the Criminal Procedural Code makes provision for obtaining a court order only in case of covert intelligence operations. Both the Law of Ukraine "On Counter-Intelligence Operations" and the Law of Ukraine "On Law Enforcement Intelligence Operations" (Law of Ukraine..., 1992a) do not specify sufficient conditions for collecting and accumulating personal data in information systems and criminal records of authorised bodies of national security. Given that interference in private life is a relatively new concept in the practice of law enforcement agencies and special services of Ukraine, modern Ukrainian academia does not have a unified approach to understanding the proportional scope of such interference, which would be considered adequate to the risks and threats to national security that special and intelligence agencies prevent.

Hans Born and Ian Leigh (2005), in their recommendations for bringing the practice of intelligence services in line with democratic standards, insist on the following:

- the legislative mandate should limit the purposes and circumstances under which information is collected and dossiers are opened regarding individuals;
- the law should make provision for effective control over the terms of storage of information, its use and rules of access to it, as well as for the compliance of legislation with international standards in this area;
- intelligence agencies should not be deprived of the right to freedom of information and access to the dossier; they should be granted access to information in terms of national security and the competence of such a service;

- courts, in accordance with the law, must determine that exceptions to the restriction of human rights are used reasonably, etc.

## 5. Conclusions

Summarising the above, the authors of this study propose to supplement the Law of Ukraine "On the Security Service of Ukraine" with Article $8^1$ with the following: "1. The head of the body or division of the Security Service of Ukraine must notify everyone who has made a request about the fact of collecting information about the specified person (if so, specify which ones) as soon as possible (no later than three months in advance), except in cases where this is prohibited by law. The specified official can postpone his or her decision for no more than four weeks, and notify the person who made the request before the end of the first term. 2. If the request is granted, the head of the body or department should provide the person who made the request with access to information about him or her. 3. When executing a request, all necessary measures must be taken to ensure that the person making the request is properly identified".

Clause 12) Article 25 of the above Law should be supplemented with Paragraph Two to read as follows: "Criminal records" in counter-intelligence should be interpreted as "the process of identifying, registering, accumulating, summarising, storing, and transmitting information concerning the facts and signs of intelligence and subversive activities of foreign special services, encroachments by individual organisations, groups, and individuals to the detriment of state sovereignty, constitutional order, territorial integrity, economic, scientific, technical, and defence potential of Ukraine, the legitimate interests of the state and the rights of citizens, as well as to ensure the protection of state secrets".

There is also a need to review the procedure for granting permission to gather and process personal data during counter-intelligence operations and bring it in line with international standards. Further scientific research in this area is considered appropriate to resolve the issue of developing clear criteria of sufficiency for the accumulation, processing, and storage of information in information systems and criminal records of special authorised counter-intelligence bodies.

## References

ALBUL, Sergii, ANDRUSENKO, Sergii, MUKOIDA, Ruslan and NOZDRIN, Dmytro (2020). *Basics of Operational and Investigative Activities*. Odesa: Odesa State University of Internal Affairs.

AMERICAN CONVENTION ON HUMAN RIGHTS. (1969). Available at: https://treaties.un.org/doc/publication/unts/volume%201144/volume-1144-i-17955-english.pdf

BORN, Hans and LEIGH, Ian (2005). *Making intelligence accountable: legal standards and best practice for oversight of intelligence agencies*. Available at: https://securitysectorintegrity.com/wp-content/uploads/2017/02/Making-Intelligence-Accountable_ENG.pdf

BORN, Hans and WILLS, Aidan (2016). *Oversight of intelligence services*. Geneva: ADEF.

CAPARINI, Marina (2008). *Controlling and overseeing intelligence services in democratic states*. Available at: https://www.researchgate.net/publication/265221667

CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION. (2000). https://zakon.rada.gov.ua/laws/show/994_524#Text Available at:

CHRISTAKIS, Théodore and BOUSLIMANI, Katia (2021). "National security, surveillance, and human rights", in R. Geiß and N. Melzer (eds.), *The Oxford Handbook of the International Law of Global Security*. Available at: https://www.oxfordhandbooks.com/view/10.1093/law/9780198827276.001.0001/law-9780198827276-chapter-39

CONSTITUTION OF UKRAINE. (1996). Available at: https://zakon.rada.gov.ua/laws/main/254%D0%BA/96-%D0%B2%D1%80

CONVENTION FOR THE PROTECTION OF HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS. (1950). Available at: https://zakon.rada.gov.ua/laws/show/995_004/ed19900101

CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA. (1981). Available at: https://zakon.rada.gov.ua/laws/show/994_326#Text

CRIMINAL PROCEDURE CODE OF UKRAINE. (2013). Available at: https://zakon.rada.gov.ua/laws/show/4651-17#Text

DZYOBAN Oleksandr and ZHDANENKO, Serhii (2020). "Human rights and national security: philosophical and legal aspects of their relationship", *Informatsiia i Pravo*, 2 (33), pp. 9-22. https://doi.org/10.37750/2616-6798.2020.2(33).208030

EUROPEAN CONVENTION FOR THE PROTECTION OF HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS. (1950). Available at: https://www.echr.coe.int/documents/convention_eng.pdf

INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS. (1966). Available at: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

KASRILS, Ronnie (2008). *Intelligence in a constitutional democracy*. Available at: *https://assets.publishing.service.gov.uk/media/57a08baae5274a31e0000cc8/ReviewComm.Sept08.pdf*

LAW OF UKRAINE NO. 12 "ON COUNTER-INTELLIGENCE OPERATIONS". (2003a). Available at: Available at: https://zakon.rada.gov.ua/laws/main/374-15

LAW OF UKRAINE NO. 22 "ON LAW ENFORCEMENT INTELLIGENCE OPERATIONS". (1992a). Available at: Available at: https://zakon.rada.gov.ua/laws/show/2135-12/ed20170412

LAW OF UKRAINE NO. 27 "ON THE SECURITY SERVICE OF UKRAINE". (1992B). Available at: https://zakon.rada.gov.ua/laws/show/2229-12#Text

LAW OF UKRAINE NO. 31 "ON INFORMATION PROTECTION IN INFORMATION AND TELECOMMUNICATION SYSTEMS". (1994). Available at: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

LAW OF UKRAINE NO. 34 "ON PERSONAL DATA PROTECTION". (2010). Available at: https://zakon.rada.gov.ua/laws/show/2297-17#Text

LAW OF UKRAINE NO. 39 "ON THE FOUNDATIONS OF NATIONAL SECURITY OF UKRAINE" (2003b). Available at: http://zakon2.rada.gov.ua/laws/show/964-15

LAW OF UKRAINE NO. 40 "ON RATIFICATION OF THE CONVENTION FOR THE PROTECTION OF HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS OF 1950, THE FIRST PROTOCOL AND PROTOCOLS NO. 2, 4, 7 AND 11 TO THE CONVENTION". (1997). Available at: https://zakon.rada.gov.ua/laws/show/475/97-%D0%B2%D1%80

LAW OF UKRAINE NO. 48 "ON INFORMATION". (1992c). Available at: https://zakon.rada.gov.ua/laws/show/2657-12#Text

OBUKHOVSKA, Tetyana (2014). "Protection of personal data in the development of the information society: prerequisites, principles and international law", *Bulletin NAPA*, 1, pp. 95-103.

PRUNCKUN, Hank (2019). *Counterintelligence Theory and Practice (Security and Professional Intelligence Education Series)*, Rowman & Littlefield Publishers, Washington.

RIZAK, Mykhailo (2011). "Human rights and legitimate grounds for their restrictions in the field of processing personal information in databases", *Scientific Bulletin of Uzhhorod University*, 16, pp. 200-204.

RONN, Kira Vrist (2016). "Intelligence ethics: A critical review and future perspectives", *International Journal of Intelligence and CounterIntelligence*, 29 (4), pp. 760-784. https://doi.org/10.1080/08850607.2016.1177399

SHAFFER, Ryan (2017). "Significant distrust and drastic cuts: The Indian government's uneasy relationship with intelligence", I*nternational Journal of Intelligence and CounterIntelligence*, 30 (3), pp. 522-531. https://doi.org/10.1080/08850607.2017.1263529

SHAPIRKO, Petro (2015). "Human rights in operational and investigative activities: theoretical problems", *Juridical Scientific and Electronic Journal*, 2, pp. 248-251.

STOUDER, Michael D. and GALLAGHER, Scott R. (2013). "Crafting operational counterintelligence strategy: A guide for managers", *International Journal of Intelligence and CounterIntelligence*, 26 (3), pp. 583-596. https://doi.org/10.1080/08850607.2013.780560

TERTISHNIK, Volodymyr (2002). *Guarantees of truth and protection of human rights and freedoms in criminal proceedings*. Dnipro: Dnipropetrovsk Law Academy of the Ministry of Internal Affairs of Ukraine.

THE GLOBAL PRINCIPLES ON NATIONAL SECURITY AND THE RIGHT TO INFORMATION (THE TSHWANE PRINCIPLES). (2013). https://www.justiceinitiative.org/uploads/bd50b729-d427-4fbb-8da2-1943ef2a3423/global-principles-national-security-10232013.pdf

TKACHUK, Nataliya (2018). "Information rights and freedoms of human and citizen of Ukraine: definition of terms, correlation of concepts", *Informatsiia i Pravo*, 2 (25), pp. 17-30.

UKHANOVA, Nataliya (2018). "Challenges and threats to human rights and security in the information sphere", *Informatsiia i Pravo*, 4 (27), pp. 33-45.

UNIVERSAL DECLARATION OF HUMAN RIGHTS. (1948). Available at: https://zakon.rada.gov.ua/laws/main/995_015

Received: December, 1st 2021

Accepted: March, 15th 2022