Translation from Finnish
Legally binding only in Finnish and Swedish
Ministry of Defence, Finland

Act on Military Intelligence
(590/2019)

By decision of Parliament, the following is enacted:

Chapter 1
General provisions

Section 1
Scope of application

This Act lays down provisions on the purpose of intelligence collection activities by the Defence Forces (*military intelligence*), on the duties and powers of authorities, on decision-making as well as on the guidance and oversight of military intelligence in the defence administration. The Act also lays down provisions on the technical implementation of network traffic intelligence on behalf of the Finnish Security and Intelligence Service.

Section 2
Relationship with other legislation

Provisions on civilian intelligence are laid down in chapter 5a of the Police Act (872/2011) and in the Act on the Use of Network Traffic Intelligence in Civilian Intelligence (582/2019).

Provisions on crime prevention in the Defence Forces are laid down in the Act on Military Discipline and Combating Crime in the Defence Forces (255/2014).

Provisions on the oversight of intelligence activities are laid down in the Act on the Oversight of Intelligence Activities (121/2019) and in Parliament's Rules of Procedure (40/2000). Provisions on the processing of personal data are laid down in the Act on the Processing of Personal Data by the Defence Forces (332/2019).

Section 3
Purpose of military intelligence

The purpose of military intelligence is to collect and process information on military activities against Finland or relevant to Finland's security environment or on activities referred to in section 4, subsection 2 in order to support the decision-making of the highest state leadership and carry out the following tasks of the Defence Forces:

1) undertaking surveillance of Finland's land and sea areas and airspace, and securing territorial integrity;

2) securing the livelihoods and fundamental rights of the Finnish people and the freedom of action of the government, and defending the lawful social order;

3) participating in the provision of aid and assistance based on Article 222 of the Treaty on the Functioning of the European Union or Article 42(7) of the Treaty on European Union, and participating in territorial surveillance cooperation or the provision of other international assistance and in other types of international activities;

4) participating in international military crisis management and in military tasks in other international crisis management.

Section 4
Targets of military intelligence

Military intelligence is targeted at the following activities if they are of a military nature:

1) activities by a foreign country's armed forces and organised troops comparable to them, and preparing such activities;

2) intelligence activities targeting Finland's national defence;

3) design, manufacture, distribution and use of weapons of mass destruction;

4) development and distribution of military supplies of a foreign country;

5) a crisis that poses a serious threat to international peace and security;

6) activities that pose a serious threat to the security of international crisis management operations;

7) activities that pose a serious threat to safety when Finland provides international assistance or is involved in other international activities.

In addition, military intelligence is targeted at activities by a foreign country or other activities that pose a serious threat to Finland's national defence or endanger functions vital to society.

Section 5
Respecting fundamental and human rights

The military intelligence authorities shall respect fundamental and human rights and, in exercising their powers, choose from all reasonable options the course of action that best serves to uphold these rights.

Section 6
Principle of proportionality

Military intelligence actions shall be justifiable in proportion to the importance of the information obtained through intelligence collection, the urgency of the intelligence task, the intended goal of military intelligence, the target of military intelligence, the limitation of the rights of others because of the use of the intelligence action and other factors affecting the matter. In addition, the action shall have adequate actual possibilities of achieving acceptable goals of military intelligence.

Section 7
Principle of minimum intervention

The exercise of military intelligence powers shall not infringe anyone's rights or cause anyone more harm or inconvenience than is necessary for the duty to be carried out. Intelligence collection may not interfere with the secrecy of confidential communications, except for only as narrowly and precisely as possible.

Section 8
Principle of intended purpose

Military intelligence powers may only be exercised for the purposes laid down in this Act.

Section 9
Prohibition of discriminatory intelligence collection

The targeting of military intelligence actions shall not, without an acceptable reason, be based on a person's age, gender, origin, nationality, place of residence, language, religion, conviction, opinion, political activity, trade union activity, family relationships, state of health, disability, sexual orientation, or other reason related to that person.

Section 10
Definitions

In this Act,

1) *search criterion* means information on the basis of which network traffic intelligence is used to select as narrowly and precisely as possible the network traffic targeted by network traffic intelligence from a part of a communications network, and the interference with the secrecy of confidential communications is limited to the extent necessary for the purpose of intelligence;

2) *search criteria category* means related search criteria that describe the same subject matter;

3) *party setting up a connection* means a network and infrastructure service provider referred to in section 6 of the Act on the Operation of the Government Security Network (10/2015) or a subsidiary wholly owned by it;

4) *group of persons* means a structured group of at least three persons established for a certain period which operates in concert or to achieve a common goal;

5) *location data* means location data referred to in section 3, paragraph 18 of the Information Society Code (917/2014);

6) *telecommunications operator* means a telecommunications operator referred to in section 3, paragraph 27 of the Information Society Code;

7) *party transferring data* means a party that owns or manages a part of a communications network that crosses the Finnish border;

8) *intelligence collection method* means the powers of the military intelligence authorities as laid down in chapter 4;

9) *intelligence task* means an assignment given by the Chief of Intelligence of the Defence Command to a military intelligence authority to collect intelligence on a target of military intelligence referred to in section 4 on the basis of priorities

preliminarily prepared in a joint meeting of the Ministerial Committee on Foreign and Security Policy and the President of the Republic or on the basis of an information request referred to in section 14;

10) *network traffic intelligence* means technical data collection targeted at network traffic in a communications network crossing the Finnish border based on automated screening of the network traffic and the processing of the obtained data for the purpose of performing an intelligence task;

11) *technical data on network traffic* means network traffic data other than that included in the message content;

12) *identification data* means information related to a message that can be associated with a user referred to in section 3, paragraph 7 of the Information Society Code or with a subscriber referred to in paragraph 30 of the said section;

13) *state actor* means an identified authority of a foreign state or a comparable actor and a party employed by such an actor or acting under its orders and guidance;

14) *communications network* means a system consisting of interconnected cables and devices that is intended for transmitting or distributing messages by wire, radio waves, optically or by other electromagnetic means;

15) *corporate or association subscriber* means a corporate or association subscriber referred to in section 3, paragraph 41 of the Information Society Code.

Section 11
Military intelligence authorities

The military intelligence authorities are the Defence Command and the Finnish Defence Intelligence Agency, which may obtain information to perform intelligence tasks as laid down in this Act.

Provisions on military intelligence activities in the Army, Navy and Air Force are laid down in section 60. When carrying out military intelligence activities, the Army, Navy and Air Force operate under the military intelligence authorities.

In the Defence Command, military intelligence tasks are performed and the related powers exercised by the public officials in the Defence Command assigned to military intelligence.

Section 12
General preconditions for the use of intelligence collection methods

The general precondition for the use of an intelligence collection method is that its use is essential and it can reasonably be assumed to provide important information for an intelligence task. If an intelligence collection method is targeted at a state actor, the general precondition for its use is that obtaining information is necessary for an intelligence task.

The intelligence collection methods laid down in this Act may be used without the knowledge of their targets.

An intelligence collection method may not be targeted at premises used for permanent residence.

The use of an intelligence collection method shall be discontinued before the time limit specified in the decision or authorisation as soon as the purpose of its use has been achieved or the preconditions for its use no longer exist.

Further provisions on organising the use of intelligence collection methods within a military intelligence authority, on public officials responsible for the use of intelligence collection methods and on public officials using intelligence collection methods may be issued by government decree.

Chapter 2

Guidance and monitoring of military intelligence

Section 13
Guidance and management of military intelligence

A joint meeting of the Ministerial Committee on Foreign and Security Policy and the President of the Republic preliminarily prepares priorities concerning military intelligence targets.

The Ministry of Defence is responsible for the administrative guidance of military intelligence and submits the preliminarily prepared priorities referred to in subsection 1 to the Defence Forces.

The Defence Command directs military intelligence activities, in compliance with the priorities of military intelligence.

Section 14
Request for information

Requests for information on military intelligence targets in accordance with the priorities referred to in section 13, subsection 1 may be made to the Defence Command by the President of the Republic, the Prime Minister's Office, the Ministry for Foreign Affairs and the Ministry of Defence.

Section 15
Coordination of intelligence collection activities

Military and civilian intelligence activities are coordinated between the President of the Republic, the Prime Minister's Office, the Ministry for Foreign Affairs, the Ministry of Defence and the Ministry of the Interior and, if necessary, between other ministries and authorities.

If military intelligence activities are assessed to have impact on foreign and security policy, the matter has to be prepared preliminarily between the authorities referred to in subsection 1.

Further provisions on organising the coordination of intelligence collection activities may be issued by government decree.

Section 16
Monitoring of military intelligence

The Ministry of Defence submits a report on the priorities referred to in section 13, subsection 1 to the joint meeting of the Ministerial Committee on Foreign and Security Policy and the President of the Republic at least once a year or at the request of the joint meeting of the Ministerial Committee on Foreign and Security Policy and the President of the Republic or on its own initiative.

The Defence Command annually submits a report on military intelligence activities, their quality and scope and on their targeting to the Ministry of Defence. In addition, a report shall be provided without delay at the request of the Ministry of Defence.

Chapter 3
Cooperation with other authorities and international cooperation

Section 17
Cooperation with the Finnish Security and Intelligence Service

The military intelligence authorities shall cooperate with the Finnish Security and Intelligence Service to ensure appropriate performance of the tasks of the intelligence authorities and provide the information needed for this purpose to the Finnish Security and Intelligence Service, notwithstanding provisions on the non-disclosure obligation.

Further provisions on organising the cooperation between the military intelligence authorities and the Finnish Security and Intelligence Service may be issued by government decree.

Section 18
Cooperation with other authorities and with businesses and other corporate entities

Where necessary, the military intelligence authorities shall cooperate with other authorities to ensure appropriate performance of military intelligence. Notwithstanding secrecy provisions, the military intelligence authorities may, in order to carry out their task, disclose information other than personal data to other authorities if the disclosure of information is necessary for national defence or to protect national security. Provisions on the disclosure of personal data are laid down in the Act on the Processing of Personal Data by the Defence Forces.

Notwithstanding secrecy provisions, the military intelligence authorities may, in order to carry out their task, disclose identification data related to malware to businesses and other corporate entities for the purpose of developing intelligence methods and systems or disclose information other than personal data if the disclosure of information is essential to protect the functioning of the Defence Forces or national security.

Provisions on the disclosure of information for crime prevention are laid down in sections 79 and 80.

Further provisions on organising the cooperation between the military intelligence authorities and other authorities and on the parties participating in the cooperation and their tasks may be issued by government decree.

Section 19
Coordination of secret intelligence collection

The use of intelligence collection methods laid down in this Act shall, if necessary, be coordinated in order to ensure the occupational safety of the public officials of the Finnish Security and Intelligence Service, the military intelligence authorities and the National Bureau of Investigation and to prevent tactical and technical methods and plans used in secret intelligence collection from being revealed.

Further provisions on organising the coordination of secret intelligence collection may be issued by government decree.

Section 20
International cooperation

The military intelligence authorities may, in accordance with Finland's national interests and with regard to their tasks or to protect national security:

1) exchange intelligence other than personal data with foreign intelligence and security services, notwithstanding secrecy provisions, if doing so is necessary; and

2) participate in international cooperation related to collecting and assessing intelligence.

If joint intelligence collection is carried out in cooperation with the state in the area of which intelligence collection methods are to be used, military intelligence authority officials shall comply with the restrictions and conditions imposed on the use of intelligence collection methods by the state concerned.

A competent foreign official has, by the decision of the Chief of Intelligence of the Defence Command, the right to cooperate in the territory of Finland with a military intelligence authority official in order to carry out the tasks of the military intelligence authority and to use, under the official's guidance and supervision, intelligence collection methods referred to in sections 22, 24, 43, 47, 51 and 66. Foreign officials

are obliged to comply with the orders, restrictions and instructions issued to them by the military intelligence authority.

The decision on the participation in international cooperation and on the use of intelligence collection methods is made by the Chief of Intelligence of the Defence Command.

International cooperation is prohibited where there are reasonable grounds to suspect that the cooperation or disclosure of information could result in a risk that a person would face the death penalty, torture, other degrading treatment, persecution, arbitrary deprivation of liberty or unfair trial.

In addition, the separate provisions on the disclosure and reception of information laid down in international treaties binding on Finland or in the Act on International Information Security Obligations (588/2004) shall be observed in the disclosure and reception of information referred to in this section. Provisions on the disclosure of personal data are laid down in the Act on the Processing of Personal Data by the Defence Forces.

Section 21
Liability for acts in office of foreign officials

Chapter 16, section 20, subsection 4; chapter 21, section 18; and chapter 40, section 12, subsection 4 of the Criminal Code (39/1889) lay down provisions on the application of the said chapters to an offence committed by or directed at a foreign official operating in the territory of Finland or using an intelligence collection method in the territory of Finland in the manner referred to in section 20, subsection 3 of this Act, unless otherwise provided by any international treaty binding on Finland.

Chapter 4
Intelligence collection methods

Extended surveillance, covert intelligence collection and technical surveillance

Section 22
Surveillance and extended surveillance

Surveillance means making covert observations of a certain person, or if a certain person cannot be specified, of a group of persons for the purpose of collecting intelligence. Notwithstanding chapter 24, section 6 of the Criminal Code, surveillance may involve the use of a camera or other such technical device for making or recording visual observations.

Extended surveillance means other than short-term surveillance of a person or a group of persons who, with reasonable cause, may be assumed to be related to an intelligence task.

The military intelligence authorities may, in order to perform an intelligence task, conduct extended surveillance of a target referred to in subsection 2 if extended surveillance can reasonably be assumed to be of particular importance to obtaining information for an intelligence task.

A technical device may not be used in surveillance or extended surveillance of places covered by the right to domestic privacy as referred to in chapter 24, section 11 of the Criminal Code.

Section 23
Decision on extended surveillance

Decisions on extended surveillance are made by an assigned legal adviser or other public official specialised in the use of intelligence collection methods.

Decisions on extended surveillance may be given for up to six months at a time.

Decisions on extended surveillance shall be made in writing. The decision shall specify:

1) the intelligence task on which the action is based;

2) the person who is the object of the action or, if a certain person cannot be specified, a group of persons that has been specified in sufficient detail;

3) the facts on which the preconditions for and targeting of extended surveillance are based;

4) the validity period of the decision;

5) the public official specialised in the use of intelligence collection methods who will be directing and supervising the extended surveillance;

6) any restrictions on and conditions for the extended surveillance.

Section 24
Covert intelligence collection

Covert intelligence collection means intelligence collection on a certain person or, if a certain person cannot be specified, on a group of persons during brief interaction, in which false, misleading or disguised information is used to conceal the tasks of military intelligence authority officials.

The military intelligence authorities may use covert intelligence collection to perform an intelligence task.

Section 25
Decision on covert intelligence collection

Decisions on covert intelligence collection are made by an assigned legal adviser or other public official specialised in the use of intelligence collection methods.

Decisions on covert intelligence collection shall be made in writing. The decision shall specify:

1) the action and its purpose and the intelligence task on which the action is based;

2) the person who is the object of the action or, if a certain person cannot be specified, a group of persons that has been specified in sufficient detail;

3) the facts on which the preconditions for and targeting of covert intelligence collection are based;

4) the public official specialised in the use of intelligence collection methods who will be directing and supervising the covert intelligence collection;

5) the planned time for carrying out the action;

6) any restrictions on and conditions for the covert intelligence collection.

The decision shall be reviewed where necessary if circumstances change.

If the action cannot be delayed, decisions on covert intelligence collection will not have to be drawn up in writing before taking the action. The decision shall, however, be drawn up in writing without delay after the action.

Section 26
On-site interception

On-site interception means, notwithstanding chapter 24, section 5 of the Criminal Code, audio monitoring, recording and other handling of a conversation or a message of a certain person or, if a certain person cannot be specified, of a group of persons

that is not intended for the knowledge of outsiders and where the listener does not participate in the discussion, using a technical device, process or software for the purpose of investigating the content of the conversation or message, or the activities of the participants.

The military intelligence authorities may engage in on-site interception of a person or a group of persons not inside premises used for permanent residence if the on-site interception can reasonably be assumed to be of particular importance to obtaining information for an intelligence task. Interception can be carried out by arranging it at the premises or other location where the person or group of persons related to the intelligence task can be assumed likely to stay or visit.

Section 27
Decision on on-site interception

Decisions on on-site interception are made by a court at the request of an assigned legal adviser or other public official specialised in the use of intelligence collection methods when the interception is targeted at a person or a group of persons in premises other than those used for permanent residence covered by the right to domestic privacy as referred to in chapter 24, section 11 of the Criminal Code or at a person deprived of their liberty. If the matter cannot be delayed, a legal adviser or other public official specialised in the use of intelligence collection methods may decide on on-site interception until the court has made a decision on the request to grant authorisation. The matter shall be brought for decision by a court as soon as possible, but no later than 24 hours after the use of the method was started.

Decisions on on-site interception other than that referred to in subsection 1 are made by an assigned legal adviser or other public official specialised in the use of intelligence collection methods.

An authorisation may be granted and a decision given for up to six months at a time.

The request and decision concerning on-site interception shall specify:

1) the intelligence task on which the action is based;

2) the person who is the object of the action or, if a certain person cannot be specified, a group of persons that has been specified in sufficient detail, or the premises or other location;

3) the facts on which the preconditions for and targeting of on-site interception are based;

4) the validity period of the authorisation, including the precise time;

5) the public official specialised in the use of intelligence collection methods who will be directing and supervising the on-site interception;

6) any restrictions on and conditions for the on-site interception.

Section 28
Technical observation

Technical observation means, notwithstanding chapter 24, section 6 of the Criminal Code, surveillance or recording of a particular person or, if a certain person cannot be specified, of a group of persons or premises or other location using a camera or other technical device, process or software located at the place.

The military intelligence authorities may engage in technical observation of a person or a group of persons not inside the premises used for permanent residence if the technical observation can reasonably be assumed to be of particular importance to obtaining information for an intelligence task. Observation may be conducted by targeting it at the premises or other location where the targeted person or group of persons can be assumed likely to stay or visit.

Section 29

Decision on technical observation

Decisions on technical observation are made by a court at the request of an assigned legal adviser or other public official specialised in the use of intelligence collection methods when the observation targets premises other than those used for permanent residence covered by the right to domestic privacy as referred to in chapter 24, section 11 of the Criminal Code or a person deprived of their liberty. If the matter cannot be delayed, a legal adviser or other public official specialised in the use of intelligence collection methods may decide on technical observation until the court has made a decision on the request to grant authorisation. The matter shall be brought for decision by a court as soon as possible, but no later than 24 hours after the use of the method was started.

Decisions on technical observation other than that referred to in subsection 1 are made by an assigned legal adviser or other public official specialised in the use of intelligence collection methods.

An authorisation may be granted and a decision given for up to six months at a time.

The request and decision concerning technical observation shall specify:

1) the intelligence task on which the action is based;

2) the person who is the object of the action or, if a certain person cannot be specified, a group of persons that has been specified in sufficient detail, or the premises or other location;

3) the facts on which the preconditions for and targeting of technical observation are based;

4) the validity period of the authorisation, including the precise time;

5) the public official specialised in the use of intelligence collection methods who will be directing and supervising the technical observation;

6) any restrictions on and conditions for the technical observation.

Section 30
Technical tracking

Technical tracking means tracking of the movements of an object, substance or item of property using a radio transmitter separately placed inside it or already inside it, or using other such technical device, process or software.

The military intelligence authorities may arrange technical tracking of an object, substance or item of property or of an object, substance or item of property presumably in the possession of a person related to an intelligence task for the purpose of performing an intelligence task.

If the purpose of technical tracking is to track the movements of persons by placing a tracking device in the clothes they are wearing or in an object they are carrying (*technical tracking of a person*), the action may be performed only if it can reasonably be assumed to be of particular importance to obtaining information for an intelligence task.

Section 31
Decision on technical tracking

Decisions on technical tracking of a person are made by a court at the request of an assigned legal adviser or other public official specialised in the use of intelligence collection methods. If the matter cannot be delayed, a legal adviser or other public official specialised in the use of intelligence collection methods who has been assigned to the task by the military intelligence authorities may decide on technical tracking of a person until the court has made a decision on the request to grant authorisation. The matter shall be brought for decision by a court as soon as

possible, but no later than 24 hours after the use of the intelligence collection method was started.

Decisions on technical tracking other than that referred to in subsection 1 are made by a legal adviser or other public official specialised in the use of intelligence collection methods who has been assigned to the task by the military intelligence authorities.

An authorisation may be granted and a decision given for up to six months at a time.

The request and decision concerning technical tracking shall specify:

1) the intelligence task on which the action is based;

2) the person or object, substance or item of property targeted by the action;

3) the facts on which the preconditions for and targeting of technical tracking are based;

4) the validity period of the authorisation, including the precise time;

5) the public official specialised in the use of intelligence collection methods who will be directing and supervising the technical tracking;

6) any restrictions on and conditions for the technical tracking.

Section 32
Technical surveillance of a device

Technical surveillance of a device means other than purely sensory surveillance, recording or other handling of information or of identification data which is contained in a computer, other similar technical device or in software, or of their operation, for the purpose of investigating a matter necessary for an intelligence task.

Technical surveillance of a device may not be used for collecting information on a message referred to in section 34 that is being transmitted nor on its identification data.

The military intelligence authorities may be authorised to engage in technical surveillance of a device of a state actor for the purpose of performing an intelligence task.

The military intelligence authorities may be authorised to engage in technical surveillance of a device of a non-state actor if such surveillance can reasonably be assumed to be of particular importance to obtaining information for an intelligence task. The military intelligence authorities may engage in technical surveillance of a computer or other similar technical device, or of the operation of its software, that is likely to be used by a person related to an intelligence task.

Section 33
Decision on technical surveillance of a device

Decisions on technical surveillance of a device are made by a court at the request of an assigned legal adviser or other public official specialised in the use of intelligence collection methods. If the matter cannot be delayed, an assigned legal adviser or other public official specialised in the use of intelligence collection methods may decide on technical surveillance of a device until the court has made a decision on the request to grant authorisation. The matter shall be brought for decision by a court as soon as possible, but no later than 24 hours after the use of the intelligence collection method was started.

An authorisation may be granted for up to six months at a time.

The request and decision concerning technical surveillance of a device shall specify:

1) the intelligence task on which the action is based;

2) the technical device or software targeted by the action;

3) the facts on which the preconditions for and targeting of technical surveillance of a device are based;

4) the validity period of the authorisation, including the precise time;

5) the public official specialised in the use of intelligence collection methods who will be directing and supervising the technical surveillance of a device;

6) any restrictions on and conditions for the technical surveillance of a device.

Intelligence collection in telecommunications networks

Section 34
Telecommunications interception

Telecommunications interception means the audio monitoring, recording or other handling of messages received by or sent from a network address or terminal equipment via a public communications network referred to in section 3, paragraph 43 of the Information Society Code or a communications network connected to it or via other communications connection, for the purpose of establishing the content of the message and the related identification data. Telecommunications interception may only target messages from or intended for a person who can reasonably be assumed to be related to an intelligence task.

The military intelligence authorities may be authorised to carry out telecommunications interception of a state actor for the purpose of performing an intelligence task.

The military intelligence authorities may be authorised to carry out telecommunications interception of a non-state actor if such interception can

reasonably be assumed to be of particular importance to obtaining information for an intelligence task.

Section 35
Collecting data other than through telecommunications interception

If it is likely that a message referred to in section 34 and the related identification data can no longer be collected through telecommunications interception, the military intelligence authorities may be authorised to collect data held by a telecommunications operator or a corporate or association subscriber subject to the preconditions laid down in section 34.

If, to establish the content of a message, the collecting of data is targeted at a personal technical device suitable for sending and receiving a message that is in direct connection with terminal equipment or at the connection between this personal technical device and terminal equipment, the military intelligence authorities may be authorised to collect data other than through telecommunications interception, provided that the preconditions laid down in section 34 are met.

Section 36
Decision on telecommunications interception and other similar intelligence collection

Decisions on telecommunications interception and on collecting data other than through telecommunications interception are made by a court at the request of an assigned legal adviser or other public official specialised in the use of intelligence collection methods.

An authorisation for telecommunications interception or for collecting data other than through telecommunications interception may be granted for up to six months at a time. When the action is targeted at a person, the authorisation may be granted for up to three months at a time.

The request and decision concerning telecommunications interception and collecting data other than through telecommunications interception shall specify:

1) the intelligence task on which the action is based;

2) the person, network address or terminal equipment targeted by the action;

3) the facts on which the preconditions for and targeting of telecommunications interception or collecting data other than through telecommunications interception are based;

4) the validity period of the authorisation concerning telecommunications interception or collecting data other than through telecommunications interception, including the precise time;

5) the public official specialised in the use of intelligence collection methods who will be directing and supervising the telecommunications interception or collecting data other than through telecommunications interception;

6) any restrictions on and conditions for the telecommunications interception or collecting data other than through telecommunications interception.

Section 37
Data traffic monitoring

Data traffic monitoring means collecting identification data from messages that have been sent from a network address or terminal equipment connected to a communications network or received by such an address or equipment, or collecting the location data of a network address or terminal equipment.

The military intelligence authorities may be authorised to conduct data traffic monitoring of a network address or terminal equipment in the possession of or otherwise used by a state actor for the purpose of performing an intelligence task.

The military intelligence authorities may be authorised to conduct data traffic monitoring of a network address or terminal equipment in the possession of or otherwise used by a non-state actor if such monitoring can reasonably be assumed to be of particular importance to obtaining information for an intelligence task.

Section 38
Decision on data traffic monitoring

Decisions on data traffic monitoring are made by a court at the request of an assigned legal adviser or other public official specialised in the use of intelligence collection methods. If a matter concerning data traffic monitoring cannot be delayed, an assigned legal adviser or other public official specialised in the use of intelligence collection methods may decide on data traffic monitoring until the court has made a decision on the request to grant authorisation. The matter shall be brought for decision by a court as soon as possible, but no later than 24 hours after the use of the method was started.

The military intelligence authorities may, with the consent of the person concerned, conduct data traffic monitoring of a network address or terminal equipment in the possession of the person for the purpose of performing an intelligence task.

Decisions on data traffic monitoring referred to in subsection 2 are made by the Chief of Intelligence of the Defence Command or an assigned legal adviser or other public official specialised in the use of intelligence collection methods.

An authorisation may be granted and a decision made for up to six months at a time, and the authorisation or decision may also refer to a fixed period prior to granting the authorisation or making the decision, which may be longer than six months.

The request and decision concerning data traffic monitoring shall specify:

1) the intelligence task on which the action is based and the purpose of the action;

2) the person, network address or terminal equipment targeted by the action;

3) the facts on which the preconditions for and targeting of data traffic monitoring are based;

4) the validity period of the authorisation, including the precise time;

5) the public official specialised in the use of intelligence collection methods who will be directing and supervising the data traffic monitoring;

6) any restrictions on and conditions for the data traffic monitoring.

Section 39
Collecting base station data

Collecting base station data means collection of data on terminal equipment and network addresses that are or are to be logged in the telecommunications system via a particular base station.

The military intelligence authorities may be authorised to collect base station data significant to an intelligence task.

Section 40
Decision on collecting base station data

Decisions on collecting base station data are made by a court at the request of an assigned legal adviser or other public official specialised in the use of intelligence collection methods. If the matter cannot be delayed, an assigned legal adviser or other public official specialised in the use of intelligence collection methods may decide on collecting base station data until the court has made a decision on the request to grant authorisation. The matter shall be brought for decision by a court as

soon as possible, but no later than 24 hours after the use of the intelligence collection method was started.

An authorisation may be granted and a decision made for up to six months at a time. If the authorisation or decision concerns a fixed period prior to granting the authorisation or making the decision, its validity may exceed six months.

The request and decision concerning collecting base station data shall specify:

1) the intelligence task on which the action is based and the purpose of the action;

2) the base station covered by the authorisation;

3) the facts on which the preconditions for and targeting of collecting base station data are based;

4) the time period covered by the authorisation;

5) the public official specialised in the use of intelligence collection methods who will be directing and supervising the collecting of base station data;

6) any restrictions on and conditions for the collecting of base station data.

Section 41
Collecting data identifying a network address or terminal equipment

The military intelligence authorities may, in order to perform an intelligence task, use a technical device to collect the data identifying a network address or terminal equipment.

The Finnish Transport and Communications Agency inspects that the technical device, due to its properties, does not cause any harmful interference with the devices or services of a public communications network. Decisions on collecting data

identifying a network address or terminal equipment are made by an assigned legal adviser or other public official specialised in the use of intelligence collection methods.

Section 42
Installation and removal of a device, process or software

A public official serving a military intelligence authority has the right to install a device, process or software used for telecommunications interception, collecting data other than through telecommunications interception, data traffic monitoring, on-site interception, technical observation, technical tracking or technical surveillance of a device in the object, substance, item of property, premises or other location or in the information system targeted by the action if the use of the said intelligence collection method necessitates this. To install, start using or remove a device, process or piece of software, a military intelligence authority official has in this case the right to secretly go to the said targets or information system and to circumvent, dismantle or in some other similar way temporarily bypass the protection of the target or information system or to impede it. The installation or removal of a device, process or piece of software may not be performed at premises used for permanent residence.

Undercover activities and pseudo purchases

Section 43
Undercover activities

Undercover activities means extended intelligence collection on certain persons or their activities or, if a certain person cannot be specified, on a group of persons or its actions by means of infiltration in which false, misleading or disguised information or register entries are used or false documents are produced or used to gain trust required for intelligence collection or to avoid revealing the intelligence collection.

The military intelligence authorities may engage in undercover activities directed at a person or a group of persons if the activities targeted by an intelligence task are

planned, organised or professional, or the activities are anticipated to be continuous or recurring.

The military intelligence authorities have the right to engage in undercover activities directed at a person or a group of persons in an information network if the activities can reasonably be assumed to be of particular importance to obtaining information for an intelligence task.

Section 44
Proposal and plan for undercover activities

A proposal for undercover activities shall specify:

1) who is proposing the action;

2) the person who is the object of the intelligence collection or, if a person cannot be specified, a group of persons that has been specified in sufficient detail;

3) the intelligence task on which the action is based;

4) the purpose of the undercover activities;

5) the necessity of the undercover activities;

6) other information needed for assessing the preconditions for the undercover activities.

A written plan shall be drawn up on how the undercover activities are to be carried out, and this shall include essential and sufficiently detailed information for decision-making on the undercover activities and for performing the undercover activities. The plan shall be reviewed where necessary if circumstances change.

Section 45

Decision on undercover activities

Decisions on undercover activities are made by the Chief of Intelligence of the Defence Command. Decisions on undercover activities carried out solely in an information network are made by an assigned legal adviser or other public official specialised in the use of intelligence collection methods.

Decisions on undercover activities may be given for up to six months at a time.

Decisions on undercover activities shall be made in writing. The decision shall specify:

1) who is proposing the action;

2) the public official specialised in the use of intelligence collection methods who will be in charge of conducting the undercover activities;

3) identification information on the public officials engaging in the undercover activities;

4) the intelligence task on which the action is based;

5) the person who is the object of intelligence collection or, if a certain person cannot be specified, a group of persons that has been specified in sufficient detail;

6) the facts on which the preconditions for and targeting of the undercover activities are based;

7) the purpose and execution plan for the undercover activities;

8) the validity period of the decision;

9) any restrictions on and conditions for the undercover activities.

The decision shall be reviewed where necessary if circumstances change. Decisions to cease the undercover activities shall be made in writing.

Section 46
Prohibition against committing an offence

Military intelligence authority officials engaged in undercover activities shall not commit an offence or propose that an offence be committed.

If a military intelligence authority official engaged in undercover activities commits a traffic violation, public order violation or other similar offence for which the punishment by law is a fixed fine, they will be exempt from criminal liability if the action was necessary for achieving the purpose of the undercover activities or preventing the intelligence collection from being revealed.

Section 47
Pseudo purchase

Pseudo purchase means a purchase offer for or purchase of an object, substance, item of property or service made by a military intelligence authority with the aim that the military intelligence authority will take possession of or find an object, substance or item of property related to an intelligence task.

The military intelligence authorities may carry out a pseudo purchase.

The person carrying out a pseudo purchase may only conduct intelligence collection that is essential for the purchase. The pseudo purchase shall be carried out in such a way that it does not induce the target person or anyone else to commit an offence that they would not otherwise commit.

Section 48
Decision on a pseudo purchase

Decisions on a pseudo purchase are made by the Chief of Intelligence of the Defence Command. Decisions on a pseudo purchase concerning a sales offer exclusively to the public may also be made by an assigned legal adviser or other public official specialised in the use of intelligence collection methods.

Decisions on a pseudo purchase may be given for up to six months at a time.

Decisions on pseudo purchases shall be made in writing. The decision shall specify:

1) the intelligence task on which the action is based;

2) the person who is the object of the pseudo purchase;

3) the facts on which the preconditions for and targeting of the pseudo purchase are based;

4) the object, substance, item of property or service targeted by the pseudo purchase;

5) the purpose of the pseudo purchase;

6) the validity period of the decision;

7) the public official specialised in the use of intelligence collection methods who will be directing and supervising the pseudo purchase;

8) any restrictions on and conditions for the pseudo purchase.

Section 49
Plan for carrying out a pseudo purchase

A written plan for carrying out a pseudo purchase shall be drawn up if this is necessary on account of the extent of the operation or for some other similar reason.

The plan for carrying out a pseudo purchase shall be reviewed where necessary if circumstances change.

Section 50
Decision to carry out a pseudo purchase

Decisions to carry out a pseudo purchase shall be made in writing. The decision is made by an assigned public official specialised in the use of intelligence collection methods who will be in charge of carrying out the pseudo purchase.

The decision shall specify:

1) the legal adviser or other public official specialised in the use of intelligence collection methods who has been assigned to the task by a military intelligence authority as well as the date of issue and content of the decision;

2) identification data on the military intelligence authority officials carrying out the pseudo purchase;

3) an account of the steps taken to ensure that the pseudo purchase will not induce the target person or anyone else to commit an offence that they would not otherwise commit;

4) any restrictions on and conditions for the pseudo purchase.

If the action cannot be delayed, the decision will not have to be drawn up in writing before starting to carry out the pseudo purchase. The decision shall, however, be drawn up in writing without delay after the pseudo purchase.

The decision to carry out the pseudo purchase shall be reviewed where necessary if circumstances change.

Use of covert human intelligence sources

Section 51
Use of covert human intelligence sources

Use of covert human intelligence sources means other than occasional, confidential receipt from a person outside the Finnish authorities, of significant information for managing an intelligence task (*covert human intelligence source*).

The military intelligence authorities may request a covert human intelligence source who is approved for the purpose, has suitable personal attributes, is registered and consents to the intelligence collection to gather information referred to in subsection 1 (*controlled use of covert human intelligence sources*), if the controlled use of covert human intelligence sources can reasonably be assumed to be of particular importance to obtaining information for an intelligence task.

In the controlled use of covert human intelligence sources, a request to gather information may not be made if collection would require the use of powers vested in a public authority or endanger the life or health of the covert human intelligence source or another person. Before the controlled use of a covert human intelligence source, the source shall be made aware of their rights and obligations and especially of the activities which are permitted and prohibited for them by law. The safety of covert human intelligence sources shall be ensured as necessary during and after the intelligence collection.

Information on the use of covert human intelligence sources may be entered in a filing system. Provisions on the processing of personal data are laid down in the Act on the Processing of Personal Data by the Defence Forces.

Provisions on protecting covert human intelligence sources are laid down in section 78.

Section 52
Payment of fees to covert human intelligence sources

Registered covert human intelligence sources may be paid a fee. If there are justified grounds, a fee may also be paid to covert human intelligence sources who have not been registered. Separate provisions are issued on the taxability of the fee.

Section 53
Decision on the controlled use of covert human intelligence sources

Decisions on the controlled use of covert human intelligence sources are made by the Chief of Intelligence of the Defence Command.

Decisions on the controlled use of covert human intelligence sources may be given for up to six months at a time.

Decisions on the controlled use of covert human intelligence sources shall be made in writing. The decision shall specify:

1) who is proposing the action;

2) the military intelligence authority official specialised in the use of intelligence collection methods who will be in charge of the intelligence collection;

3) identification information on the covert human intelligence source;

4) the intelligence task on which the action is based;

5) the purpose and execution plan for the intelligence collection;

6) the validity period of the decision;

7) any restrictions on and conditions for the controlled use of covert human intelligence sources.

The decision shall be reviewed where necessary if circumstances change. Decisions to cease the controlled use of covert human intelligence sources shall be made in writing.

Site exploitation and copying

Section 54
Site exploitation

Site exploitation means intelligence collection carried out in order to find an object, item of property, document, piece of information or circumstance at premises used for other than permanent residence or at premises where there is reason to believe that the target of intelligence collection would reveal information in respect of which a person has the obligation or right to refuse to testify under chapter 17, section 11, 13, 14, 16, 20 or 21 or section 22, subsection 2 of the Code of Judicial Procedure.

The military intelligence authorities may be authorised to carry out site exploitation for the purpose of performing an intelligence task.

Section 55
Decision on site exploitation

Decisions on site exploitation are made by a court, at the request of an assigned legal adviser or other public official specialised in the use of intelligence collection methods, when it is targeted at a place other than premises used for permanent residence covered by the right to domestic privacy or at a place with no public access or with limited or hindered public access during the carrying out of site exploitation.

If the matter referred to in subsection 1 cannot be delayed, the decision on site exploitation may be made by the Chief of Intelligence of the Defence Forces or an assigned legal adviser or other public official specialised in the use of intelligence collection methods until the court has made a decision on the request to grant authorisation. The matter shall be brought for decision by a court as soon as possible, but no later than 24 hours after the use of the method was started.

Decisions on site exploitation other than that referred to in subsection 1 are made by the Chief of Intelligence of the Defence Forces or an assigned legal adviser or other public official specialised in the use of intelligence collection methods.

An authorisation may be granted and a decision given for up to one month at a time.

The request or decision concerning site exploitation shall adequately specify:

1) the intelligence task on which the action is based;

2) the place targeted by the site exploitation;

3) the facts on the basis of which the preconditions for site exploitation are considered to exist;

4) if possible, the object being searched for through the site exploitation;

5) any restrictions on the site exploitation.

If required by the urgency of the matter, a decision on site exploitation may be recorded after the site exploitation has been carried out.

Section 56
Copying

The military intelligence authorities have the right to copy a document or an object in order to perform an intelligence task.

When copying is targeted at a message of a non-state actor, the precondition is that the copying can reasonably be assumed to be of particular importance to obtaining information for an intelligence task.

Section 57
Copying of a delivery

The military intelligence authorities have the right to copy a letter or other delivery before it reaches the recipient.

When copying of a delivery is targeted at a message of a non-state actor, the precondition is that the copying can reasonably be assumed to be of particular importance to obtaining information for an intelligence task.

Section 58
Interruption of a delivery for copying

If there is reason to believe that a letter or other delivery that may be copied is arriving or has already arrived at a post office, at a rail traffic point or its part or at the office of a party which transports deliveries on a professional basis in connection with transport or otherwise, an assigned legal adviser or other public official specialised in the use of intelligence collection methods may order that the delivery be kept at the said office until the copying has been carried out.

The order may be given for a period not exceeding one month, the period beginning when the office's manager has been informed of the delivery. The delivery may not, without the permission of the public official referred to in subsection 1, be given to anyone else than the said official or a person designated by the official.

The office's manager shall immediately inform the person who has issued the order of the arrival of the delivery. The said person shall decide on copying without undue delay.

Section 59
Decision on copying and copying of a delivery

Decisions on the copying referred to in section 56 are made by an assigned legal adviser or other public official specialised in the use of intelligence collection methods. The decision shall be made in writing.

If the matter cannot be delayed, a military intelligence authority official other than the public official referred to in subsection 1 may, in an individual case, decide on copying until the public official referred to in subsection 1 has decided the matter. The matter shall be brought for decision by the public official referred to in subsection 1 as soon as possible, but no later than 24 hours after the use of the intelligence collection method was started.

Decisions on the copying of a delivery referred to in section 57 are made by a court at the request of an assigned legal adviser or other public official specialised in the use of intelligence collection methods.

If the matter referred to in subsection 3 cannot be delayed, the decision on the copying of a delivery may be made by the Chief of Intelligence of the Defence Command or an assigned legal adviser or other public official specialised in the use of intelligence collection methods until the court has made a decision on the request to grant authorisation. The matter shall be brought for decision by a court as soon as possible, but no later than 24 hours after the use of the method was started. If required by the urgency of the matter, a decision on the copying of a delivery may be recorded after the copying of a delivery has been carried out.

Radio signals intelligence, foreign computer network exploitation and intelligence collection abroad

Section 60
Radio signals intelligence

Radio signals intelligence means intelligence collection targeted at radio-frequency electromagnetic waves (*radio waves*).

The Finnish Defence Intelligence Agency or the Army, Navy or Air Force may target radio signals intelligence at radio waves originating from or arriving at a device outside the territory of Finland.

Radio signals intelligence may not be used for collecting information on the content of messages of non-state actors.

Section 61
Decision on radio signals intelligence

Decisions on radio signals intelligence are made by the Chief of Intelligence of the Defence Command. The decision shall be made in writing.

Section 62
Foreign computer network exploitation

Foreign computer network exploitation means collecting data on an information system located outside Finland using information technology methods.

The Finnish Defence Intelligence Agency may target foreign computer network exploitation at an information system if such exploitation can be expected to be of particular importance to obtaining information for an intelligence task.

A written plan shall be drafted on foreign computer network exploitation, which shall include relevant and adequately detailed information for the decision-making on and performance of foreign computer network exploitation. The plan shall be reviewed as necessary if circumstances change.

Section 63
Decision on foreign computer network exploitation

Decisions on foreign computer network exploitation are made by the Chief of Intelligence of the Defence Command. The decision shall be made in writing.

The decision on foreign computer network exploitation shall specify:

1) the intelligence task on which the action is based;

2) the target of the action;

3) the purpose and execution plan for the foreign computer network exploitation;

4) the public official specialised in the use of intelligence collection methods who will be directing and supervising the foreign computer network exploitation;

5) any restrictions on and conditions for the foreign computer network exploitation.

The military intelligence authorities shall keep the Ministry of Defence informed of ongoing foreign computer network exploitation.

Section 64
Military intelligence abroad

The provisions of section 12, subsection 3; section 60, subsection 3; and section 85, subsection 2 of this Act may in individual cases be waived in military intelligence activities engaged in and intelligence collection methods employed abroad if this is essential. Sections 79, 80 and 89 of the Act do not apply to military intelligence activities engaged in and intelligence collection methods employed abroad.

Decisions on the military intelligence activities and use of intelligence collection methods carried out outside Finland are made by the Chief of Intelligence of the Defence Command. Participation of a military intelligence authority official in the military intelligence activities abroad referred to in this section requires the consent of the public official concerned.

The provisions of this Act on the proposal, plan, requirement or decision shall be observed with respect to the content of a decision, proposal and plan concerning the use of an intelligence collection method.

Intelligence collection on network traffic

Section 65
Prohibition of general and indiscriminate monitoring of network traffic

Intelligence collection on network traffic shall not take the form of general and indiscriminate monitoring of network traffic.

Section 66
Processing of technical data

The Finnish Defence Intelligence Agency may, in order to target network traffic intelligence, momentarily collect and store technical data on network traffic from network traffic in a communications network and process it by means of automatic data processing for statistical analysis purposes.

The results of statistical analysis may not contain data allowing identification of an individual natural person.

The Finnish Defence Intelligence Agency shall destroy all collected and stored technical data on network traffic immediately after the results of the statistical analysis are complete.

Section 67

Decision on processing of technical data

Decisions on the processing of technical data are made by a court at the request of an assigned legal adviser or other public official of the Finnish Defence Intelligence Agency specialised in the use of intelligence collection methods.

An authorisation may be granted for up to three months at a time.

The request and decision concerning the processing of technical data shall specify:

1) the geographical area or network area where the incoming or outgoing network traffic is targeted by the processing of technical data;

2) the parts of a communications network where the data is searched for;

3) the public official of the Finnish Defence Intelligence Agency specialised in the use of intelligence collection methods who will be directing and supervising the processing of technical data;

4) a plan for the execution of the processing of technical data.

Section 68

Intelligence collection on the network traffic of state actors

The Finnish Defence Intelligence Agency may collect data on the network traffic of a state actor relevant for an intelligence task from the network traffic in a communications network crossing the Finnish border by means of automatic data processing and process the state actor's communications. Collecting data from network traffic is based on the use of search criteria.

The Finnish Defence Intelligence Agency may process data collected from network traffic by both automated and manual means.

Data that identifies the terminal equipment or network address in the possession of a person staying in Finland or otherwise presumably used by that person may not be used as a search criterion.

Section 69
Decision on intelligence collection on the network traffic of state actors

Decisions on intelligence collection on the network traffic of state actors are made by a court at the request of the Chief of Intelligence of the Defence Command. If the matter cannot be delayed, the Chief of Intelligence of the Defence Command may decide on intelligence collection on the network traffic of state actors until the court has made a decision on the request to grant authorisation. The decision shall be made in writing. The matter shall be brought for decision by a court as soon as possible, but no later than 24 hours after the network traffic intelligence was started.

An authorisation may be granted for up to six months at a time.

The request and decision concerning intelligence collection on the network traffic of state actors shall specify:

1) the intelligence task for which network traffic is gathered;

2) the search criteria or search criteria categories to be used in intelligence collection and the justification for their use;

3) the part of the communications network targeted by intelligence collection and the justification for the targeting;

4) the validity period of the authorisation, including the precise time;

5) the public official of the Finnish Defence Intelligence Agency specialised in the use of intelligence collection methods who will be directing and supervising the intelligence collection on the network traffic of state actors;

6) any restrictions on and conditions for the intelligence collection on the network traffic of state actors.

Section 70
Intelligence collection on the network traffic of non-state actors

The Finnish Defence Intelligence Agency may collect data on the network traffic of a non-state actor relevant for an intelligence task from the network traffic in a communications network crossing the Finnish border by means of automatic data processing if the data cannot be obtained through other intelligence collection methods. Collecting data from network traffic is based on the use of search criteria.

Data that identifies the terminal equipment or network address in the possession of a person staying in Finland or otherwise presumably used by that person may not be used as a search criterion.

Intelligence collection on the network traffic of non-state actors may not be based on the content of a message unless information describing the content of malware is used in the targeting.

The Finnish Defence Intelligence Agency may process data obtained from network traffic by both automated and manual means.

Section 71
Decision on intelligence collection on the network traffic of non-state actors

Decisions on intelligence collection on the network traffic of non-state actors are made by a court at the request of the Chief of Intelligence of the Defence Command. If the matter cannot be delayed, the decision on intelligence collection on the network traffic of non-state actors may be made by the Chief of Intelligence of the Defence Command until the court has made a decision on the request to grant authorisation. The decision shall be made in writing. The matter shall be brought for decision by a court as soon as possible, but no later than 24 hours after the network traffic intelligence was started.

An authorisation may be granted for up to six months at a time.

The request and decision concerning intelligence collection on the network traffic of non-state actors shall specify:

1) the intelligence task for which network traffic is gathered;

2) the facts concerning the target of intelligence collection;

3) the facts on which the effectiveness and necessity of network traffic intelligence are based;

4) the facts on which the other preconditions for the use of network traffic intelligence are based;

5) the search criteria or search criteria categories to be used in intelligence collection and the justification for their use;

6) the part of the communications network targeted by intelligence collection and the justification for the targeting;

7) the validity period of the authorisation, including the precise time;

8) the public official of the Finnish Defence Intelligence Agency who will be directing and supervising the collection and storing of communications;

9) any restrictions on and conditions for the network traffic intelligence.

Section 72
Setting up a connection required by the processing of technical data and network traffic intelligence

The party setting up a connection executes the authorisations referred to in sections 67, 69 and 71 and routes the network traffic in the part of the communications network specified in the authorisation to the Finnish Defence Intelligence Agency.

The party setting up a connection discloses the network traffic in the communications network part of the interface referred to in the authorisation to the Finnish Defence Intelligence Agency.

Section 73
Technical implementation of network traffic intelligence on behalf of the Finnish Security and Intelligence Service

Technical implementation of network traffic intelligence on behalf of the Finnish Security and Intelligence Service means:

1) statistical analysis of technical data on the basis of an assignment that the Finnish Security and Intelligence Service has given to the Finnish Defence Intelligence Agency and submission of the analysis to the Finnish Security and Intelligence Service; and

2) obtaining network traffic transmitted through a part of a communications network crossing the Finnish border in accordance with an authorisation granted by a court to

the Finnish Security and Intelligence Service by means of automatic data processing and disclosing the data to the Finnish Security and Intelligence Service.

Provisions on the technical implementation of network traffic intelligence for the Finnish Security and Intelligence Service are laid down in section 10 of the Act on the Use of Network Traffic Intelligence in Civilian Intelligence.

The Finnish Defence Intelligence Agency may not determine the content of a message in the technical implementation of network traffic intelligence on behalf of the Finnish Security and Intelligence Service.

Section 74
Disclosure of information on harmful computer programs to businesses and corporate entities

Notwithstanding secrecy provisions, the military intelligence authorities may disclose information on harmful computer programs and their functioning obtained by means of network traffic intelligence to a business, corporate entity or authority if the disclosure of the information is necessary for military national defence, to protect national security or to safeguard the interests of the business or corporate entity.

Chapter 5
Protecting military intelligence, public officials and covert human intelligence sources

Section 75
Protecting military intelligence

The military intelligence authorities may use false, misleading or disguised information, make and use false, misleading or disguised register entries as well as produce and use false documents when this is essential for preventing military intelligence from being revealed.

The register entries referred to in subsection 1 shall be corrected after the preconditions referred to in the subsection no longer exist.

Further provisions on organising the protection of military intelligence, on the public officials in charge of protecting military intelligence and on cooperation with registrars may be issued by government decree.

Section 76
Decision on protecting military intelligence

Decision on making register entries and producing documents referred to in section 75 are made by the Chief of Intelligence of the Defence Command.

Decisions on protection other than that referred to in subsection 1 are made by an assigned legal adviser or other public official specialised in the use of intelligence collection methods.

The Chief of Intelligence of the Defence Command shall keep a record of entries and documents, oversee their use and ensure that entries are corrected.

Section 77
Protecting public officials using intelligence collection methods

An assigned legal adviser or other public official specialised in the use of intelligence collection methods may decide that the public official carrying out covert intelligence collection, undercover activities or a pseudo purchase and preparing or engaging in the use of covert human intelligence sources will be equipped with a technical device that enables audio and visual monitoring if this is justified to ensure the official's safety.

The audio and visual monitoring may be recorded. The recordings shall be destroyed as soon as they are no longer needed to protect the public official. If, however, there

is a need to keep them for reasons connected with the legal protection of a party involved in the case, the recordings may be stored and used for this purpose. In this case, the recordings shall be destroyed when the case is final or discontinued.

Section 78
Protecting covert human intelligence sources

The military intelligence authorities may, with the consent of covert human intelligence sources, monitor their residence or other premises used as their residence and their immediate surroundings by a camera or another technical device, process or software located at the place if this is necessary to avert a danger to the life or health of the covert human intelligence source. It is not necessary to inform third parties of the protection of covert human intelligence sources.

The monitoring shall be discontinued without delay if it is no longer necessary to avert a danger to the life or health of the covert human intelligence source.

The recordings collected in the monitoring referred to in subsection 1 shall be destroyed as soon as they are no longer needed for protecting the covert human intelligence source. If, however, there is a need to keep them for reasons related to the legal protection of a party involved in the case, the recordings may be stored and used for this purpose. In this case, the recordings shall be destroyed when the case is final or discontinued.

An assigned legal adviser or other public official specialised in the use of intelligence collection methods may decide that the covert human intelligence source will, with the source's consent, be equipped with a technical device enabling audio and visual monitoring if this is essential in an individual case to ensure the source's safety. The audio and visual monitoring may be recorded. The recordings shall be destroyed as soon as they are no longer needed to protect the covert human intelligence source.

The Chief of Intelligence of the Defence Command may decide that false, misleading or disguised information or register entries will be made available to the covert human intelligence source or false documents will be produced for the source's use in an individual case if this is essential to protect the source's life and health. The register entries shall be corrected after the preconditions referred to in this subsection no longer exist.

Chapter 6
Disclosure of intelligence in certain cases

Section 79
Reporting a suspected offence

The military intelligence authorities shall, without undue delay, notify the National Bureau of Investigation if it becomes evident during the use of an intelligence collection method that there is reason to believe that an offence has been committed for which the most severe punishment provided by law is at least six years' imprisonment. Notification may be postponed by the decision of the Chief of Intelligence of the Defence Command by up to one year at a time if this is essential for national defence or to protect national security or a person's life and health.

The military intelligence authorities may notify the National Bureau of Investigation of an offence committed if the notification can be believed to be of particular importance to investigating an offence for which the most severe punishment provided by law is at least three years' imprisonment.

When considering postponing the notification referred to in subsection 1 or making the notification referred to in subsection 2, the assessment shall, in addition to the significance to national defence and protecting national security, consider the significance of investigating the offence to public and private interest.

The information obtained through the use of an intelligence collection method may always be disclosed as evidence in support of innocence and to prevent significant

danger to life, health and liberty or significant damage to the environment, property or assets.

A court will decide on the use of information disclosed under this section as evidence in connection with the consideration of the principal matter. Provisions on recording the use of information in criminal investigation records are laid down in chapter 9, section 6, subsection 2 of the Criminal Investigation Act (805/2011), and provisions on notifying the use of information in an application for a summons are laid down in chapter 5, section 3, subsection 1, paragraph 9 of the Criminal Procedure Act (689/1997).

Decision on making the notification referred to in this section are made by the Chief of Intelligence of the Defence Command.

Further provisions on the notification procedure may be issued by government decree.

Section 80
Notification and disclosing information in certain cases

The military intelligence authorities shall without delay notify a competent authority if it becomes evident during the use of an intelligence collection method that an offence is being prepared for which the most severe punishment provided by law is at least six years' imprisonment and the offence is still preventable.

The information obtained through the use of an intelligence collection method may be disclosed to a competent authority in order to prevent an offence for which the most severe punishment provided by law is at least two years' imprisonment.

When considering making the notification referred to in subsection 1, the assessment shall, in addition to the significance to national defence and protecting national

security, consider the significance of preventing the offence to public and private interest.

The information obtained through the use of an intelligence collection method may always be disclosed as evidence in support of innocence and to prevent significant danger to life, health and liberty or significant damage to the environment, property or assets.

A court will decide on the use of information disclosed under this section as evidence in connection with the consideration of the principal matter. Provisions on recording the use of information in criminal investigation records are laid down in chapter 9, section 6, subsection 2 of the Criminal Investigation Act, and provisions on notifying the use of information in an application for a summons are laid down in chapter 5, section 3, subsection 1, paragraph 9 of the Criminal Procedure Act.

Decisions on making the notification referred to in this section and on the disclosure of information are made by the Chief of Intelligence of the Defence Command.

Further provisions on the notification procedure may be issued by government decree.

Section 81
Notification of initiating criminal investigation or crime prevention

If, on the basis of a notification or disclosure of information referred to in this chapter, a criminal investigation authority initiates criminal investigation or undertakes a criminal investigation action or a crime prevention authority undertakes a measure to prevent an offence, the criminal investigation authority or the crime prevention authority shall, before initiating the criminal investigation or undertaking the criminal investigation action or the measure to prevent an offence, notify the military intelligence authorities thereof.

Chapter 7
Prohibitions of intelligence collection, destruction of intelligence and notification of the use of an intelligence collection method

Section 82
Prohibition of intelligence collection

Telecommunications interception, collecting data other than through telecommunications interception, on-site interception, technical observation, radio signals intelligence or network traffic intelligence shall not be targeted at communications or information in respect of which a party may not testify or has the right to refuse to testify under chapter 17, section 13, 14, 16, 20 or section 22, subsection 2 of the Code of Judicial Procedure.

If it becomes evident during telecommunications interception, collecting data other than through telecommunications interception, on-site interception, technical observation, radio signals intelligence or network traffic intelligence or otherwise that the message concerned is one in respect of which audio and visual monitoring are prohibited, the action shall be interrupted and the recordings obtained through the action and the notes on the information obtained accordingly shall be destroyed immediately.

Network traffic intelligence shall not be targeted at communications where the sender and recipient are in Finland.

The prohibitions of intelligence collection referred to in this section do not, however, apply to cases where the person referred to in subsection 1 participates in the activities targeted by military intelligence and a decision on telecommunications interception, collecting data other than through telecommunications interception, on-site interception, technical observation or network traffic intelligence has also been made in respect of the said person.

Section 83

Prohibition of copying

A document or other object referred to in section 54 may not be copied if it contains information in respect of which a party has the obligation or right to refuse to testify under chapter 17, section 11, 13, 14, 16, 20 or 21 of the Code of Judicial Procedure.

If the non-disclosure obligation or the obligation or right to remain silent is based on chapter 17, section 11, subsection 2 or 3 or section 13, 14, 16 or 20 of the Code of Judicial Procedure, the precondition for the prohibition is, in addition to the provisions of subsection 1, that the object is in the possession of the person referred to in the said legal provision or of a person related to the first-mentioned person as referred to in section 22, subsection 2 of the said chapter or in the possession of a party for whose benefit the non-disclosure obligation or right has been provided.

However, the prohibition of copying does not apply if:

1) the person referred to in chapter 17, section 11, subsection 2 or 3; section 13, subsection 1 or 3; section 14, subsection 1; or section 16, subsection 1 of the Code of Judicial Procedure for whose benefit the non-disclosure obligation has been provided consents to copying; or

2) the person referred to in chapter 17, section 20, subsection 1 of the Code of Judicial Procedure consents to copying.

A document or data in the possession of a telecommunications operator or a corporate or association subscriber containing information related to a message referred to in section 34, subsection 1 or identification data referred to in section 36, subsection 1 or base station data referred to in section 39, subsection 1 may not be copied.

Section 84
Destruction of intelligence

Information obtained by an intelligence collection method shall be destroyed without delay after it has become evident that the information is no longer needed, the information may not be used for carrying out military intelligence tasks or the information is not needed for national defence or to protect national security.

The base station data referred to in section 39 shall be destroyed after it has become evident that the data is no longer needed, the data may not be used for carrying out military intelligence tasks or the data is not needed for national defence or to protect national security.

A copy referred to in section 56 or 57 shall be destroyed without delay if it becomes evident that the copying has been targeted at material covered by a prohibition of copying or the information is not needed for national defence or to protect national security.

Information other than that referred to in section 82, subsection 1 may, however, be retained and stored if the information is necessary in cases referred to in section 79 or 80.

Section 85
Interruption of telecommunications interception, on-site interception, radio signals intelligence, technical surveillance of a device and site exploitation

If it becomes evident that telecommunications interception is directed at messages from or to a person other than the person referred to in the authorisation or that the person who is the object of on-site interception is not staying at the premises or other location where the interception is being conducted, the use of the intelligence collection method shall be interrupted in respect of this as soon as possible, and the recordings obtained by audio monitoring and the notes on the information obtained accordingly shall be destroyed immediately.

The obligation to interrupt the measure and to destroy recordings and notes applies to radio signals intelligence if it becomes evident that the radio signals intelligence is targeted at the content of a message of a non-state actor.

The obligation to interrupt the measure and to destroy recordings and notes applies to technical surveillance of a device if it becomes evident that the device targeted by the surveillance is not used by the person referred to in section 32, subsection 4.

If it becomes evident during site exploitation that intelligence collection has been targeted at information in respect of which a party has the obligation or right to refuse to testify under chapter 17, section 11, 13, 14, 16, 20, 21 or section 22, subsection 2 of the Code of Criminal Procedure, intelligence collection shall be interrupted immediately in respect of this and the notes on and copies of the information shall be destroyed immediately.

Information other than that referred to in subsection 4 may, however, be retained and stored if the information is necessary in cases referred to in section 79 or 80.

Section 86
Destruction of information obtained through network traffic intelligence

In addition to the provisions of section 82, subsection 2, the information obtained through network traffic intelligence shall be destroyed without delay after it has become evident that:

1) both parties to the communications were in Finland when the communications were exchanged; or

2) the sender or the recipient or the party who stored the information has an obligation or right to refuse to testify in respect of this information under the provisions of section 82, subsection 1.

The military intelligence authorities are responsible for the destruction. If the Finnish Defence Intelligence Agency has submitted the information to the Finnish Security and Intelligence Service in connection with the technical implementation of network traffic intelligence on behalf of the Finnish Security and Intelligence Service, the Finnish Security and Intelligence Service is responsible for the destruction.

Section 87

Discontinuing the use of an intelligence collection method on which a decision was made in an urgent situation and destruction of the information obtained by it

If the Chief of Intelligence of the Defence Command or an assigned legal adviser or other public official specialised in the use of intelligence collection methods has, in an urgent situation referred to in section 27, 29, 31, 33, 38, 40, 55, 59, subsection 4, 69 or 71, decided to start on-site interception, technical observation, technical tracking of a person, technical surveillance of a device, data traffic monitoring, collecting base station data, site exploitation, copying of a delivery, intelligence collection on the network traffic of state actors or intelligence collection on the network traffic of non-state actors, but a court considers that the preconditions for the action were not met, the use of the intelligence collection method shall be discontinued and the material obtained by the method and the notes on the information obtained shall be destroyed immediately.

If a military intelligence authority official has, in an urgent situation referred to in section 59, subsection 2, decided on copying but an assigned legal adviser or other public official specialised in the use of intelligence collection methods considers that the preconditions for the action were not met, the use of the intelligence collection method shall be discontinued and the material obtained by the method and the notes on the information obtained shall be destroyed immediately.

The information referred to in this section, other than that referred to in section 82, subsection 1, may nevertheless be used for reporting an offence referred to in

section 79, subsection 1 or preventing an offence referred to in section 80, subsection 1.

Section 88
Use of information unrelated to an intelligence task

Information obtained through the use of an intelligence collection method which is unrelated to an intelligence task may be used in performing other ongoing or future intelligence tasks if the information could have been obtained by the same intelligence collection method as the information unrelated to an intelligence task. Decisions on the use of information unrelated to an intelligence task are made by a court if it is competent to decide on the intelligence collection method by which the information was obtained, or by the Chief of Intelligence of the Defence Command or an assigned legal adviser or other public official if they are competent to decide on the use of the intelligence collection method.

If the matter referred to in subsection 1 cannot be delayed, an assigned legal adviser or other public official specialised in the use of intelligence collection methods may decide on the use of information unrelated to an intelligence task until the court referred to in subsection 1, the Chief of Intelligence of the Defence Command, an assigned legal adviser or other public official specialised in the use of intelligence collection methods has made a decision on the request to use the information. The matter shall be brought for decision by the court referred to in subsection 1, the Chief of Intelligence of the Defence Command, an assigned legal adviser or other public official specialised in the use of intelligence collection methods as soon as possible but no later than 24 hours after the use of information unrelated to an intelligence task was started.

Information unrelated to an intelligence task, other than that referred to in section 82, subsection 1, may nevertheless be used under the same conditions as information may be used in cases referred to in section 79, subsection 1 or 80, subsection 1.

Section 89

Notification of the use of intelligence collection methods

The person who was the object of intelligence collection shall be notified in writing without delay of telecommunications interception, collecting data other than through telecommunications interception, data traffic monitoring, technical surveillance, copying directed at a message and copying of a delivery directed at a message after the purpose of the use of the intelligence collection method has been achieved.

The person who was the object of intelligence collection shall be notified in writing of intelligence collection on the network traffic of non-state actors after the purpose of the use of the intelligence collection method has been achieved and if, in the processing, manual means were used to determine the identification data or content of a confidential message of a person who was in Finland during the carrying out of network traffic intelligence. However, there is no obligation to give a notification, if the information obtained through network traffic intelligence has been destroyed pursuant to section 86.

The use of an intelligence collection method shall, however, be notified to the object of intelligence collection no later than one year after use of the method was discontinued.

If the identity of the object of intelligence collection is not known by the expiry of the time limit or postponement referred to in subsection 1 to 3, the use of the intelligence collection method shall be notified in writing to the person without undue delay as soon as their identity is established.

The court that granted the authorisation shall simultaneously be informed in writing of notifying the object.

A court may, at the request of the Chief of Intelligence of the Defence Command or an assigned legal adviser or other public official specialised in the use of intelligence collection methods, decide that the notification referred to in subsection 1 and 2 to

the object of the intelligence collection may be postponed for up to two years at a time if this is justified for safeguarding the ongoing use of an intelligence collection method, for national defence or for ensuring national security or protecting life or health. The notification need not be sent at all if this is essential for national defence or to protect national security or to protect life or health.

There is no obligation to notify the object of the intelligence collection of extended surveillance, covert intelligence collection, undercover activities, pseudo purchases, controlled use of covert human intelligence sources, site exploitation, copying directed at something else than a message and copying of a delivery directed at something else than a message unless a criminal investigation has been started into the matter on the basis of a notification referred to in section 79 or 80. If a criminal investigation is initiated, the provisions of chapter 10, section 60, subsections 2 to 7 of the Coercive Measures Act (806/2011) shall be observed.

There is no obligation to notify the object of an intelligence collection method of the use of the intelligence collection method if the target was a state actor.

In the court's consideration of a matter concerning a notification, the provisions of section 116 shall be observed.

Chapter 8
Participation of Defence Forces public officials and conscripts in military intelligence, and international activities

Section 90
Participation of Defence Forces public officials in military intelligence

Public officials of the Defence Forces with adequate training in the use of intelligence collection methods may use intelligence collection methods referred to in chapter 4 under the guidance and supervision of a military intelligence authority for the purpose of obtaining information for an intelligence task. These public officials act under the military intelligence authority that performs the intelligence task.

Section 91

Powers of reservists serving under the Conscription Act

Reservists with adequate training participating in reservist training under the Conscription Act (1438/2007) may assist the military intelligence authorities in radio signals intelligence, foreign computer network exploitation, processing of technical data and targeting of network traffic intelligence.

Reservists with adequate training assigned to reservist training referred to in section 32, subsection 3 of the Conscription Act, in extra service referred to in section 82 of the said Act or called up to service during mobilisation under section 86 may use, in addition to the provisions of subsection 1, extended surveillance, on-site interception, technical observation, technical tracking and technical tracking of a device as well as foreign computer network exploitation for the purpose of performing an intelligence task. The intelligence collection referred to in this subsection may not be used for gathering information on the content of a message.

Reservists participating in reservist training under the Conscription Act who have resigned from the service of a military intelligence authority on the basis of section 47 of the Act on the Defence Forces (551/2007) may use the intelligence collection methods referred to in chapter 4.

Reservists may exercise the powers referred to in this section only under the guidance and supervision of a public official specialised in the use of intelligence collection methods.

Section 92

Participation of the Defence Forces in international activities

In addition to the provisions of this Act concerning decision-making on the use of intelligence collection methods, an assigned legal adviser or other public official specialised in the use of intelligence collection methods or a person specialised in the

use of intelligence collection methods who has resigned from the service of a military intelligence authority under section 47 of the Act on the Defence Forces, who participates in the provision of international assistance and other international activities and who has been appointed to an employment relationship with the Defence Forces or is in an employment relationship under the Act on Military Crisis Management (211/2006) may decide on the use of intelligence collection methods in the provision of international assistance by the Defence Forces and in other international activities as well as in military crisis management operations.

Reservists with adequate training on the use of intelligence collection methods who have been appointed to an employment relationship with the Defence Forces may use intelligence collection methods under the guidance and supervision of a public official or reservist referred to in subsection 1.

The Chief of Intelligence of the Defence Command will decide on the participation of a person referred to in this section in the provision of international assistance and in other international activities and military crisis management as well as on the public officials and reservists referred to in subsection 1 who will decide on the use of intelligence collection methods used in these activities.

Section 93
Liability for acts in office of a person serving under the Conscription Act

Provisions on criminal liability for acts in office apply to a person serving under the Conscription Act who uses an intelligence collection method referred to in section 90 or 91.

Section 94
Liability for damages of a person serving under the Conscription Act

The State shall be liable for damage caused by reservists serving under the Conscription Act when carrying out a task under this Act as laid down in the Tort Liability Act (412/1974).

Provisions on the liability for damages of reservists serving under the Conscription Act are laid down in chapter 4, section 2 of the Tort Liability Act.

Chapter 9
Disclosure prohibition, obligations and rights of telecommunications operators and parties transferring data, and use of and access to information

Section 95
Disclosure prohibition

An assigned legal adviser or other public official specialised in the use of intelligence collection methods may prohibit a third party from disclosing facts about the use of an intelligence collection method that the party has become aware of if this is justified for protecting intelligence collection activities. A further precondition is that the said third party, due to their task or position, has assisted or been asked to assist in the use of the intelligence collection method.

The disclosure prohibition is issued for up to one year at a time. The prohibition shall be served to the recipient in writing and in a verifiable manner. It shall specify the facts that are subject to the prohibition, state the validity period of the prohibition and note the threat of punishment for violating the prohibition.

No judicial review may be requested by way of appeal against a decision on the disclosure prohibition. The party subject to the prohibition may, however, file a complaint to the Helsinki District Court without a time limit. The complaint shall be considered urgently.

The punishment for violating the disclosure prohibition is imposed under chapter 38, section 1 or 2 of the Criminal Code, unless a more severe punishment for the act is provided elsewhere by law.

The party subject to a disclosure prohibition may, notwithstanding subsection 4, notify the Intelligence Ombudsman of the disclosure prohibition.

Section 96
Telecommunications operators' obligation to assist

Telecommunications operators shall, without undue delay, make the telecommunications network connections required for telecommunications interception and data traffic monitoring and make available to the military intelligence authorities the information, equipment and personnel necessary for carrying out telecommunications interception. The same also applies in situations where telecommunications interception or data traffic monitoring is performed by a military intelligence authority using a technical device.

Section 97
Responsibility of the party transferring data to contribute to the constructing and maintaining the access points required by network traffic intelligence

A party transferring data is obligated to contribute to the constructing and maintaining of the access points required by network traffic intelligence by providing the Finnish Defence Intelligence Agency with information necessary for this purpose and access to the premises where the access point is to be constructed. The Finnish Defence Intelligence Agency shall construct the access point in such a way that it causes as little inconvenience to the party transferring data as possible. The party transferring data has the right to participate in the measures for constructing the access point.

If the access point referred to in subsection 1 cannot be constructed with the contribution of the party transferring data, the Finnish Defence Intelligence Agency has the right to construct the access point in the part of a communications network administered by the party transferring data. The party transferring data shall, as far

as possible, be present when the access point required for network traffic intelligence is being constructed.

Section 98
Obligation of the party transferring data to disclose information

A party transferring data shall, without undue delay, at the specified request of an assigned legal adviser or other public official of the Finnish Defence Intelligence Agency specialised in the use of intelligence collection methods, disclose technical data in its possession on the structure of a communications network crossing the Finnish border and the routing of network traffic therein that is necessary for identifying the part of the communications network when submitting an authorisation request and an authorisation decision concerning network traffic intelligence to the court.

Section 99
Compensation for telecommunications operators

Telecommunications operators have the right to receive compensation from state funds for the direct costs incurred in assisting a military intelligence authority and disclosing information pursuant to section 96 as laid down in section 299 of the Information Society Code. The military intelligence authority that performed the action decides on the payment of compensation.

Section 100
Compensation for parties transferring data

Parties transferring data have the right to receive compensation from state funds for the direct costs incurred in assisting a military intelligence authority pursuant to section 97 and disclosing information pursuant to section 98. The Finnish Defence Intelligence Agency decides on the payment of compensation.

Section 101
Request for review of a decision on compensation

An administrative review may be requested of a decision on compensation issued to a telecommunications operator or a party transferring data as laid down in the Administrative Procedure Act (434/2003).

A judicial review of a decision made concerning a request for an administrative review may be requested by way of appeal from an administrative court as laid down in the Administrative Judicial Procedure Act (586/1996).

A decision of an administrative court may be appealed against only if the Supreme Administrative Court grants leave to appeal.

The administrative court shall provide the Finnish Transport and Communications Agency with an opportunity to be heard.

Section 102
Payment for setting up a connection

The party setting up a connection may charge the Finnish Defence Intelligence Agency fees for the services it has provided under chapter 4. The amount of the fees may not exceed the amount of total costs incurred by the party setting up a connection in setting up the connection.

Section 103
Use of information retained by telecommunications operators

In addition to the provisions of section 157, subsection 1 of the Information Society Code on the use of information to be retained, the information to be retained may also be used for gathering information on activities referred to in section 4 of this Act which are targeted by military intelligence.

Section 104
Right to obtain information from a private entity

The military intelligence authorities have, at the request of an assigned legal adviser or other public official specialised in the use of intelligence collection methods and notwithstanding the business, banking or insurance secrecy binding on a corporate entity member, auditor, managing director, board member or employee, the right to obtain information from a private entity which may in an individual case be expected to be necessary for investigating the activities referred to in section 4 and which may be expected to be relevant for:

1) identifying or locating a person or a legal person who is the object of military intelligence or for determining their contact information or movements;

2) targeting the use of an intelligence collection method at a certain person; or

3) investigating the financial activities of a person or a legal person.

In individual cases, the military intelligence authorities have the right to obtain from a telecommunications operator and a corporate or association subscriber upon request contact information about a network address that is not listed in a public directory or data identifying a network address or terminal equipment if the information is needed to perform an intelligence task. Similarly, the military intelligence authorities have the right to obtain postal address information from corporate entities engaged in postal services.

Chapter 10
Oversight of military intelligence in the defence administration

Section 105
Internal oversight

Military intelligence is overseen by the Chief of Intelligence of the Defence Command. The Chief Legal Adviser of the Defence Forces is responsible for the internal oversight of legality of military intelligence.

Section 106

Oversight by the Ministry of Defence

Military intelligence activities are overseen by the Ministry of Defence.

The Ministry of Defence has, notwithstanding secrecy provisions, the right to obtain information on issues related to military intelligence which are of social or economic importance or of serious significance.

Further provisions on organising the oversight of military intelligence and on the reports to be submitted in the defence administration may be issued by decree of the Ministry of Defence.

Section 107

External oversight of military intelligence

The Ministry of Defence shall issue an annual report on the use of intelligence collection methods and measures to protect military intelligence as well as on the oversight to Parliament's Intelligence Oversight Committee, the Parliamentary Ombudsman and the Intelligence Ombudsman.

Further provisions on the reports to be submitted for the oversight of military intelligence may be issued by decree of the Ministry of Defence.

Section 108

Notifications to the Intelligence Ombudsman

The military intelligence authorities shall give information to the Intelligence Ombudsman on authorisations and decisions concerning intelligence collection methods issued under this Act as soon as the authorisation was granted or the decision made. The Intelligence Ombudsman shall also be notified of a request concerning an intelligence collection method submitted to a court.

The military intelligence authorities shall notify the Intelligence Ombudsman as soon as possible of a decision concerning:

1) protection of military intelligence;

2) disclosure prohibition;

3) postponement of the notification referred to in section 79, subsection 1.

In the submission of notifications referred to in this section, special attention shall be given to ensuring that the non-disclosure obligation is observed and that the information contained in documents and information systems is protected with the necessary procedures and data security arrangements.

Chapter 11
Miscellaneous provisions

Section 109
Calculation of time limits

The Act on the Calculation of Statutory Time Limits (150/1930) does not apply to the calculation of time limits referred to in this Act.

A period that is specified in months ends on the day of the closing month that corresponds to the starting date in question. If there is no such corresponding date in the closing month, the period will end on the last day of that month.

Section 110
Inspection of recordings and documents

The recordings and documents collected during the use of an intelligence collection method shall be inspected without undue delay by the public official in charge of the

use of the intelligence collection method or the public official designated by the official.

Section 111
Examination of recordings

Recordings collected during the use of intelligence collection methods may be examined only by a court, the Chief of Intelligence of the Defence Command, an assigned legal adviser or other public official specialised in the use of intelligence collection methods or the Intelligence Ombudsman or a public official designated by the Ombudsman. By order of the Chief of Intelligence of the Defence Command or in accordance with the instructions of the court, recordings may also be examined by a party other than the military intelligence authority official referred to above, an expert or other person assisting in carrying out the intelligence collection.

If an expert or other person referred to in subsection 1 is a private party, the provisions on criminal liability for acts in office apply to the expert or other person when they are carrying out the tasks referred to in this chapter.

If an expert or other person referred to in subsection 2 is used, the examining of recordings shall take place under the direct guidance and supervision of the military intelligence authority official referred to in subsection 1. The expert or other person shall also have the necessary knowledge, skills and experience to carry out the assignment.

Section 112
Record

A record shall be prepared on the use of an intelligence collection method without undue delay.

Further provisions on the keeping of records of actions for oversight purposes may be issued by government decree.

Section 113
Obligation to remain silent

The provisions laid down in the Act on the Openness of Government Activities (621/1999), in other acts and below in this chapter apply to the obligation of public officials who are part of the military intelligence authority personnel to remain silent.

Public officials who are part of the military intelligence authority personnel may not disclose information on the identity of a person who has given information confidentially or acted as an undercover officer if the disclosure of information could endanger the safety of the person who gave the information confidentially or acted as an undercover officer, or of their close family members.

The obligation to remain silent is also in force if the disclosure of information on a person's identity would endanger completed, ongoing or future intelligence collection.

The obligation to remain silent referred to in subsections 1 to 3 also applies to a party who performs an intelligence task under the direction and supervision of the military intelligence authorities or in an employment relationship with the Defence Forces.

The obligation to remain silent remains in force after the end of the employment relationship with the military intelligence authorities.

Section 114
Right to remain silent

Members of the military intelligence authority personnel are not obliged to disclose information concerning the identity of persons who provided them with confidential information during their employment relationship or to disclose information on any secret tactical or technical methods.

The right to remain silent also applies to a party who performs an intelligence task under the direction and supervision of the military intelligence authorities or assists a military intelligence authority.

Section 115
Badge

The Defence Command confirms a badge that military intelligence authority officials shall carry with them when performing official duties.

When performing official duties, the military intelligence authority officials shall declare that they are military intelligence authority officials or present their badge upon request if such declaration or presentation is possible without jeopardising the performance of the action.

An identifier other than the one referred to in subsection 1, indicating the status of military intelligence authority officials and to be used when engaged in official duties of the military intelligence authorities, is approved by the Chief of Intelligence of the Defence Command, who will also decide on its use.

The military intelligence authorities shall ensure that the military intelligence authority officials who carried out official duties can be identified if necessary.

Section 116
Procedure in court

Matters concerning granting an authorisation for intelligence collection methods are considered by the Helsinki District Court. The district court has a quorum with only the chairperson present. The composition shall be supplemented with a legally trained member as referred to in chapter 2, section 11 of the Code of Judicial Procedure unless this is manifestly unfounded considering the nature of the matter. The court session may also be held at another time and in another place than those specified in the provisions governing the sessions of a general court of first instance.

A request to use an intelligence collection method shall be made in writing. A request to use an intelligence collection method shall be considered by a court without delay in the presence of the public official who made the request or a public official designated by that official who is familiar with the matter. The court shall give the Intelligence Ombudsman or a public official designated by the Ombudsman an opportunity to be heard in the hearing of a matter concerning granting an authorisation for the use of an intelligence collection method.

The matter shall be decided urgently. The court hearing can also be conducted by using video conferencing or other suitable technical means of communication, provided that the participants are connected in such a way that they can hear and see each other.

Provisions on the content of decisions concerning intelligence collection methods are laid down specifically for each intelligence collection method. The decision shall be given immediately or at the latest when the hearing of matters concerning intelligence collection methods and related to the same entity of intelligence collection activities has been completed.

If a court has granted an authorisation for telecommunications interception or data traffic monitoring, it may examine and decide a matter concerning the granting of an authorisation for another person, network address or terminal equipment in the absence of the public official who made the request or another public official designated by the official who made the request, if less than six months have elapsed since the hearing of the previous matter concerning the granting of an authorisation. The matter can also be considered in the absence of the said public official if the use of the intelligence collection method has been discontinued.

No judicial review may be requested by way of appeal in respect of decisions issued in matters concerning authorisations. A complaint may be filed against the decision to the Helsinki Court of Appeal without a time limit. The complaint shall be considered

urgently. The Intelligence Ombudsman also has the right to file a complaint against a decision given in a matter concerning the granting of an authorisation for the use of an intelligence collection method.

In considering a matter concerning the use of an intelligence collection method, special attention shall be given to ensuring that the non-disclosure obligation is observed and that the information contained in documents and information systems is protected with the necessary procedures and data security arrangements.

Section 117
Restriction on parties' right of access in certain cases

Notwithstanding the provisions of section 11 of the Act on the Openness of Government Activities, a person whose rights or obligation are affected by the matter has no right of access to information on the intelligence collection referred to in this Act until such a notification referred to in section 89 has been made.

Section 118
Entry into force

This Act enters into force on 1 June 2019.