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

Act on the Use of Network Traffic Intelligence in Civilian Intelligence

(582/2019; amendments up to 1363/2019 included)

By decision of Parliament, the following is enacted:

Section 1
Scope of application and relationship with other legislation

This Act lays down provisions on the use of network traffic intelligence in civilian intelligence referred to in chapter 5a of the Police Act (872/2011).

The provisions laid down in chapter 1 of the Police Act concerning the requirement for respect for fundamental and human rights, the principle of proportionality, the principle of minimum intervention and the principle of intended purpose shall be complied with in the use of network traffic intelligence.

The targeting of network traffic 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.

Network traffic intelligence shall not take the form of general and indiscriminate monitoring of network traffic.

Provisions on the use of network traffic intelligence in military intelligence and the technical implementation of network traffic intelligence are laid down in the Act on Military Intelligence (590/2019). Provisions on telecommunications interception, collecting data other than through telecommunications interception and traffic data monitoring in civilian intelligence are laid down in chapter 5a of the Police Act.

Insofar as provisions on the processing of data obtained through network traffic intelligence are not laid down in this Act, provisions on the processing of data are laid down in the Act on the Processing of Personal Data by the Police (761/2003).

Section 2
Definitions

In this Act:

1) *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;

2) *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;

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

4) *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;

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

6) *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.

Section 3
Activities targeted by network traffic intelligence

Network traffic intelligence is targeted at:

1) terrorism;

2) foreign intelligence activities;

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

4) design, manufacture, distribution and use of dual-use goods referred to in section 2 of the Act on the Control of Exports of Dual-Use Goods (562/1996);

5) activities that pose a serious threat to the law and order of a democratic society;

6) activities that pose a threat to the life or health of a large number of people or functions vital to society;

7) activities of a foreign state that could damage Finland's international relations or economic or other vital interests;

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

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

10) activities that pose a serious threat to safety when Finland provides international assistance or is involved in other international activities; and

11) international organised crime that poses a threat to the law and order of a democratic society.

Section 4
Preconditions for the use of network traffic intelligence

The general precondition for the use of network traffic intelligence is that its use is essential for obtaining important information on such activities targeted by network traffic intelligence that seriously threaten national security, and that the information cannot be obtained through other intelligence collection methods.

If the use of search criteria for network traffic intelligence concerns only network traffic of a state actor or a comparable actor, the use of network traffic intelligence shall be necessary for obtaining information on such activities targeted by network traffic intelligence that seriously threaten national security.

Section 5
Targeting of network traffic intelligence

The targeting of network traffic intelligence is done by means of automated screening of network traffic. Automated screening is based on the use of search criteria approved in a procedure under section 7 or 9.

A search criterion describing the content of a message can only be used if:

1) the search criterion is used only for network traffic of a foreign state or comparable actor; or

2) the search criterion describes the content of harmful computer programs or commands.

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 6
Further processing of data collected by means of automated screening

Network traffic that has been screened by automated means in the manner referred to in section 5 may be processed by both automated and manual means. In the processing, the content of a message and other confidential information may be determined.

Section 7
Court authorisation for network traffic intelligence

Decisions on network traffic intelligence are made by a court at the written request of the Director of the Finnish Security and Intelligence Service.

The request and decision concerning network traffic intelligence shall specify:

1) the activities referred to in section 3 that are targeted by network traffic intelligence;

2) the facts concerning the activities referred to in paragraph 1;

3) the facts on which the preconditions for and effectiveness of the use of network traffic intelligence are based;

4) the search criteria or search criteria categories to be used in network traffic intelligence and the justification for their use;

5) the part of the communications network that crosses the border and where the search criteria are applied to the network traffic, and the justification for selecting that part of the communications network;

6) the validity period of the authorisation concerning network traffic intelligence, including the precise time;

7) the assigned commanding police officer of the Finnish Security and Intelligence Service specialised in the use of intelligence collection methods who will be directing and supervising the network traffic intelligence;

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

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

The use of network traffic intelligence shall be discontinued before the time limit specified in the authorisation if the purpose of its use has been achieved or if the preconditions for its use no longer exist.

Section 8
Procedure in court

The provisions of chapter 5a, section 35 of the Police Act on the consideration of authorisations concerning intelligence collection methods shall be observed in a court's consideration of and decisions on matters of authorisation concerning network traffic intelligence.

Section 9
Decision-making in urgent situations

If the matter concerning network traffic intelligence cannot be delayed, the Director of the Finnish Security and Intelligence Service may decide on network traffic intelligence until the court has made a decision on the request to grant authorisation. The decision shall be made in writing. The matter shall be referred to a court for decision as soon as possible, but no later than 24 hours after the network traffic intelligence was started.

If a court considers that the preconditions under section 4 for network traffic intelligence were not met, the use of network traffic intelligence shall be discontinued immediately, and the material obtained by the intelligence and the notes on the information obtained shall be destroyed immediately. If a court considers that the decision referred to in subsection 1 was erroneous in some other respects, the use of network traffic intelligence shall be discontinued immediately to the extent required by the decision of the court, and, to this same extent, the material obtained by network traffic intelligence and the notes on the information obtained shall be destroyed immediately. The information may, however, be retained and stored in a register referred to in the Act on the Processing of Personal Data by the Police subject to the conditions laid down in chapter 5a, section 46, subsection 1 of the Police Act.

Section 10
Technical implementation of network traffic intelligence and other cooperation with military intelligence authorities

The Finnish Defence Intelligence Agency is responsible for the technical implementation of network traffic intelligence.

The Finnish Security and Intelligence Service may assign the Finnish Defence Intelligence Agency to process technical data as specified in section 66 of the Act on Military Intelligence. The Finnish Defence Intelligence Agency applies, on behalf of the Finnish Security and Intelligence Service, for an authorisation under section 67 of the Act on Military Intelligence to process technical data and

submits the results of statistical analysis referred to in section 66, subsection 2 of that Act to the Finnish Security and Intelligence Service, after the Agency has been granted the authorisation to process the technical data and has carried out the actions in accordance with the authorisation.

The Finnish Security and Intelligence Service delivers the decision referred to in section 7 or 9 to the Finnish Defence Intelligence Agency, which will carry out the action specified in section 5 on behalf of the Finnish Security and Intelligence Service. The Finnish Defence Intelligence Agency submits the data it has separated from the network traffic according to the assigned task to the Finnish Security and Intelligence Service.

The provisions of chapter 5a, section 54 of the Police Act apply to other cooperation of the Finnish Security and Intelligence Service with the military intelligence authorities.

Section 11
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 12
Prohibition of intelligence collection

Network traffic intelligence shall not be targeted at a message where the sender and recipient are in Finland, nor at information in respect of which the sender, recipient or the party who stored the information has an obligation or right to refuse to testify under chapter 17, section 13, 14, 16 or 20 or section 22, subsection 2 of the Code of Judicial Procedure.

Section 13
Inspection of recordings and documents

The recordings and documents collected during the use of network traffic intelligence shall be inspected without undue delay by a commanding police officer of the Finnish Security and Intelligence Service referred to in chapter 5, section 7 of the Police Act or a public official designated by the officer.

Section 14
Examination of recordings

Recordings collected during the use of network traffic intelligence may be examined only by a court or a commanding police officer of the Finnish Security and Intelligence Service, or by the Intelligence Ombudsman or a public official designated by the Ombudsman. By order of a commanding police officer of the Finnish Security and Intelligence Service or in accordance with the instructions of the court, recordings may also be examined by another police officer, 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 Act.

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 a police officer of the Finnish Security and Intelligence Service. The expert or other person shall also have the necessary knowledge, skills and experience to carry out the assignment.

Section 15
Destruction of information

Information obtained by 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;

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 in the manner referred to in section 12;

3) the information is not needed to protect national security.

The information referred to in subsection 1, paragraph 3 may, however, be disclosed for the purpose of combating crime subject to the conditions laid down in chapter 5a, section 44 of the Police Act, and retained and stored in a register referred to in the Act on the Processing of Personal Data by the Police subject to the conditions laid down in chapter 5a, section 45, subsection 1 of the Police Act.

The party carrying out the technical implementation of network traffic intelligence is responsible for the destruction of information, or if the information has already been submitted to the party that assigned the task, that party is responsible for the destruction of information.

Section 16
Disclosure of information on harmful computer programs or commands to authorities, businesses or corporate entities

Notwithstanding non-disclosure provisions, the Finnish Security and Intelligence Service may disclose information on harmful computer programs or commands obtained by means of network traffic intelligence to an authority, business or corporate entity if the disclosure of the information is necessary for protecting national security or for safeguarding the interests of the party receiving the information.

The provisions of section 23, subsection 2 of the Act on the Openness of Government Activities (621/1999) apply to the obligation of persons employed by a business or corporate entity to remain silent.

Section 17
Disclosure of information for the purpose of combating crime

The provisions of chapter 5a, section 44 of the Police Act apply to the disclosure of information obtained by network traffic intelligence for the purpose of combating crime.

Section 18
Restriction on parties' right of access in certain cases

By derogation from section 11 of the Act on the Openness of Government Activities, a person has no right of access to information on the use of network traffic intelligence until such a notification referred to in section 20 has been made.

Provisions on the data subject's right of access to information are laid down in the Act on the Processing of Personal Data by the Police.

Section 19
Record

After discontinuing the use of network traffic intelligence, the Finnish Security and Intelligence Service shall prepare a record without undue delay.

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

Section 20
Notification of the use of network traffic intelligence

If, in the processing referred to in section 6, manual means were used to determine the content of a confidential message of a person who was in Finland during the carrying out of network traffic intelligence, or the content of information saved by such a person, or identification data referred to in chapter 5, section 8 of the Police Act, the person shall be notified of the network traffic intelligence in compliance with the provisions of chapter 5a, section 47 of the Police Act concerning notification of telecommunications interception. However, there is no obligation to give a notification of network traffic intelligence, if the information has been destroyed pursuant to section 9, subsection 2 or section 15.

Section 21
Setting up a connection required for network traffic intelligence

The provisions of section 72 of the Act on Military Intelligence shall be observed in setting up a connection required for network traffic intelligence.

Section 22

Obligation of the party transferring data to disclose information

A party transferring data shall, without undue delay, at the specific request of an assigned commanding police officer of the Finnish Security and Intelligence Service specialised in the use of intelligence collection methods, disclose to the Finnish Security and Intelligence Service 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 the use of network traffic intelligence to the court.

Section 23
Compensation for parties transferring data

A party transferring data has the right to receive compensation from state funds for the direct costs incurred in disclosing information pursuant to section 22. The Finnish Security and Intelligence Service decides on the payment of compensation.

An administrative review may be requested of the decision. Provisions on requesting an administrative review are laid down in the Administrative Procedure Act (434/2003). Provisions on requesting a judicial review by an administrative court are laid down in the Administrative Judicial Procedure Act (808/2019). (1363/2019)

Section 24
Oversight of network traffic intelligence in the Ministry of the Interior's branch of government

Intelligence collection referred to in this Act is overseen by the Director of the Finnish Security and Intelligence Service and the Ministry of the Interior.

Further provisions on organising the oversight in the Ministry of the Interior's branch of government referred to in subsection 1 may be given by decree of the Ministry of the Interior.

Section 25
External oversight of network traffic intelligence

The Ministry of the Interior shall issue an annual report on the use of network traffic intelligence to the Parliamentary Ombudsman, the Intelligence Oversight Committee and the Intelligence Ombudsman.

Provisions on the oversight carried out by the Intelligence Ombudsman are laid down in the Act on the Oversight of Intelligence Activities (121/2019). Further provisions on parliamentary oversight of intelligence activities are laid down in Parliament's Rules of Procedure (40/2000).

Further provisions on the reports to be submitted for the oversight of network traffic intelligence may be issued by government decree.

Section 26
Notifications to the Intelligence Ombudsman

The Finnish Security and Intelligence Service shall inform the Intelligence Ombudsman of requests and decisions made and authorisations granted by a court under this Act as laid down in chapter 5a, section 61 of the Police Act.

Section 27
Entry into force

This Act enters into force on 1 June 2019.