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

Act on Crime Prevention by the Border Guard

(108/2018; amendments up to 1351/2019 included)

By decision of Parliament, the following is enacted:

Chapter 1
General provisions

Section 1 (643/2019)
Scope of application

In addition to what is provided in the Border Guard Act (578/2005), the Act on the Administration of the Border Guard (577/2005) and the Act on the Processing of Personal Data by the Border Guard (639/2019), this Act applies to the duties of the Border Guard to prevent, detect and investigate offences and to refer them for consideration of charges.

Unless otherwise provided in this Act, the provisions on criminal investigation and coercive measures of the Criminal Investigation Act (805/2011) and the Coercive Measures Act (806/2011) and elsewhere in the law apply to the criminal investigation of an offence conducted by the Border Guard.

Section 2
Definitions

In this Act,

1) *crime prevention* means the prevention, detection and investigation of an offence;

2) *preventing an offence* means action aimed at preventing an offence, attempted offence or preparation of an offence when, due to observations of or information otherwise obtained on a

person's actions, there are reasonable grounds to assume that he or she would commit an offence, or action aimed at interrupting the commission of an offence already in progress or at limiting the injury, damage or danger directly caused by it;

3) *detecting an offence* means action aimed at establishing whether the grounds referred to in chapter 3, section 3, subsection 1 of the Criminal Investigation Act for starting a criminal investigation are met when, due to observations of or information otherwise obtained on a person's actions, it can be assumed that an offence has been committed;

4) *investigating an offence* means criminal investigation of an offence;

5) *border guard* means the Border Guard official referred to in section 15 of the Act on the Administration of the Border Guard who has the special powers of border guards provided in this Act or elsewhere in the law;

6) *official with the power of arrest* means the official of the Border Guard referred to in chapter 2, section 9, subsection 1 of the Coercive Measures Act;

7) *administrative unit* means a unit of the Border Guard referred to in section 3, subsection 1 of the Act on the Administration of the Border Guard.

Chapter 2
Duties and powers of the Border Guard in crime prevention

Section 3
Duties of the Border Guard in crime prevention

The Border Guard performs actions to prevent, detect and investigate offences, and to refer them for consideration of charges, independently or in cooperation with other authorities, in compliance with the provisions given in this Act or elsewhere by law. The Border Guard is a criminal investigation authority referred to in the Criminal Investigation Act. Provisions on the general principles to be complied with in the crime prevention by the Border Guard, especially respect for fundamental and human rights, the principle of proportionality and the principle of minimum intervention, are laid down in chapter 2 of the Border Guard Act.

Provisions on the cooperation between authorities in crime prevention matters are laid down in the Act on Cooperation between the Police, Customs and the Border Guard (687/2009).

Section 4
Offences investigated by the Border Guard

It is the duty of the Border Guard to prevent, detect and investigate the following offences:

1) a state border offence referred to in chapter 17, sections 7 and 7a of the Criminal Code (39/1889);

2) facilitation of illegal entry referred to in chapter 17, sections 8 and 8a of the Criminal Code;

3) facilitation of illegal entry and related trafficking in human beings referred to in chapter 25, sections 3 and 3a of the Criminal Code, or other offences against personal liberty referred to in chapter 25 of the Criminal Code;

4) forgery offences referred to in chapter 33, sections 1–4 of the Criminal Code concerning documents checked by the Border Guard;

5) a territorial violation referred to in chapter 17, section 7b of the Criminal Code, or other violations of Finland's territorial integrity;

6) a hunting offence referred to in chapter 48a, section 1 of the Criminal Code, an aggravated hunting offence referred to in section 1a, concealing a poached game referred to in section 4 and aggravated concealing of poached game referred to in section 4a;

7) failure to comply with a provision laid down to be overseen by the Border Guard;

8) acts punishable under chapter 20 of the Maritime Act (674/1994) and under Waterway Traffic Act (463/1996) and causing a traffic hazard in waterway traffic referred to in chapter 23, section 1 of the Criminal Code, causing a serious traffic hazard referred to in section 2, waterway traffic intoxication referred to in section 5, relinquishing a vehicle to an intoxicated person referred to in section 8, operation of a vehicle without a licence referred to in section 10 and interfering in traffic referred to in section 11a;

9) offences against border guard authorities or against border signs or border equipment maintained by the Border Guard;

10) a border zone violation referred to in section 72 of the Border Guard Act;

11) in connection with border checks, receiving offences or receiving violations referred to in chapter 32, sections 1–5 of the Criminal Code;

12) suspected commission of an offence to be tried as a military court case as referred to in section 2 of the Military Court Procedure Act (326/1983) by a person subject to the military discipline procedure referred to in section 30 or 31 of the Act on the Administration of the Border Guard, unless otherwise provided on the powers concerning criminal investigation by the Defence Forces or the police;

13) suspected commission of an offence in office referred to in section 40 of the Criminal Code by a person serving at the Border Guard, unless otherwise provided on the powers concerning criminal investigation by the Defence Forces or the police.

Section 5
Other criminal investigation by the Border Guard

At the request of other criminal investigation authorities, the Border Guard may also carry out criminal investigation involving an offence other than one referred to in section 4 if it is connected with a criminal investigation started by the Border Guard, and the related charge could be tried together with the charge for the offence investigated by the Border Guard.

Section 6 (643/2019)
Duties and powers of a border guard in crime prevention

In addition to the provisions of this Act, provisions on the duties, powers, rights and obligations of a border guard are laid down in the Border Guard Act, the Act on the Administration of the Border Guard, the Act on the Processing of Personal Data by the Border Guard and elsewhere in the law.

Unless otherwise provided in this or any other act, a border guard, in a criminal investigation conducted by the Border Guard, has the same right to take investigation measures under the Criminal Investigation Act and use coercive measures under the Coercive Measures Act as a police officer in a criminal investigation conducted by the police.

Section 7
Obligation to notify

The Border Guard shall notify the police of starting operations related to the prevention and investigation of an offence and of related use of the secret intelligence gathering methods and covert coercive measures referred to in this Act and in the Coercive Measures Act. Offences covered by the obligation to notify and the practical implementation of the notification are agreed upon in the cooperation between the Border Guard and the police.

Section 8
Transferring the prevention and investigation of an offence to the police or Customs

Unless otherwise provided on the distribution of tasks between the Border Guard, the police and Customs, and where the nature and scope of the matter or related measures so require or if the said authority so demands, the Border Guard transfers the prevention and investigation of a customs office referred to in the Act on Crime Prevention by Customs (623/2015) to Customs and the prevention and investigation of another offence to the police. In matters being transferred, the Border Guard safeguards the prevention and investigation of the offence until the case has been transferred.

The authority to which the prevention and investigation of the offence is transferred provides the Border Guard with an opportunity to participate in the prevention and investigation also after the transfer, if the matter concerns:

1) a state border offence;

2) facilitation of illegal entry and related offences against personal liberty;

3) a forgery offence concerning a document checked by the Border Guard;

4) a violation of Finland's territorial integrity.

If there is reason to suspect that a person serving at the Border Guard has committed an offence to be tried as a military court case or an offence referred to in chapter 40 of the Criminal Code, the Border Guard shall transfer the investigation of the offence to the police if this is required by the seriousness of the offence or trust in the impartiality of the investigation.

Section 9
Head of investigation

In a criminal investigation carried out by the Border Guard, the head of investigation is an official with the power of arrest.

Further provisions on the training required of the person appointed as the head of investigation at the Border Guard are issued by government decree.

Section 10
Cautioning

A border guard may issue a suspect of an offence a verbal or written caution if the criminal investigation is discontinued under chapter 3, section 9 of the Criminal Investigation Act.

Section 11
Claim for a fine, order imposing a fine, order imposing a fixed fine, and claim for a penal order

A border guard issues claims for a fine, orders imposing a fine, orders imposing a fixed fine and claims for a penal order in compliance with the provisions of the Act on Imposing a Fine and a Fixed Fine (754/2010).

Section 12
Enforcing forfeiture and returning seized objects, property or documents

The provisions of section 38 of the Act on the Enforcement of a Fine (672/2002) on police duties in the enforcement of forfeiture and the provisions of chapter 7, section 23, subsections 2–4 of the

Coercive Measures Act on the return of seized objects, property or documents apply also to the Border Guard in its investigation of a criminal matter.

The decision referred to in chapter 7, section 13, subsection 3 of the Coercive Measures Act on the sale of a seized object is made by a head of an administrative unit.

Forfeiture referred to in section 38 of the Act on the Enforcement of a Fine is enforced by administrative units.

Chapter 3
Secret intelligence gathering

General provisions

Section 13
Use of secret methods of gathering intelligence

This chapter lays down provisions on the use of telecommunications interception, obtaining base station data, extended surveillance, covert intelligence gathering, technical surveillance (on-site interception, technical observation, technical tracking and technical surveillance of a device), gathering data for the identification of a network address or a terminal equipment, use of covert human intelligence sources, and controlled deliveries, for preventing or averting the danger of an offence investigated by the Border Guard. These intelligence gathering methods may be used without the knowledge of the objects.

Section 14
Preconditions for the use of secret methods of gathering intelligence

The general precondition for the use of secret methods of gathering intelligence is that this can be assumed to result in gaining information necessary for preventing or averting the danger of an offence investigated by the Border Guard.

In addition to the provisions below on the special preconditions for the use of secret intelligence gathering methods, extended surveillance, on-site interception, technical observation, technical tracking of a person, technical surveillance of a device and controlled deliveries may be used only

if they can be assumed to be of very great significance for the prevention of an offence investigated by the Border Guard.

The use of a secret intelligence gathering method shall be discontinued before the time limit specified in the decision if the purpose of its use has been achieved or if the preconditions for its use no longer exist.

Section 15
Continuing secret intelligence gathering to investigate an offence

If, during the secret intelligence gathering begun for preventing an offence that would be investigated by the Border Guard, it emerges that there is reason to suspect that the offence on which intelligence is being gathered has already been committed, the intelligence gathering for the purpose of investigating the offence may continue for three days, however, not exceeding the period of validity of the authorisation. If it is necessary to use a covert coercive measure referred to in chapter 10 of the Coercive Measures Act for investigating an offence investigated by the Border Guard, the matter shall be brought within the stated period for decision by the authority with the power to decide on the use of the coercive measure in question.

Gathering intelligence from telecommunications networks

Section 16
Traffic data monitoring and the preconditions for it

In this Act, *traffic data monitoring* means obtaining identification data from messages that have been sent from a network address or terminal equipment connected to a public communications network referred to in the Information Society Code (917/2014) or to a communications network linked thereto, or that have been received by such an address or device, or obtaining the location data of a network address or terminal equipment, or temporarily preventing the use of the address or device. *Identification data* means data referred to in section 3, paragraph 40 of the Information Society Code which can be associated with a legal or natural person and which are processed for the purpose of transmitting messages.

To prevent an offence investigated by the Border Guard, the Border Guard may be authorised to conduct traffic data monitoring of a network address or terminal equipment in possession of a

person or presumed to be otherwise used by the person if, on the basis of the person's statements or behaviour or otherwise, there are reasonable grounds to assume that he or she would commit the following:

1) aggravated facilitation of illegal entry;

2) aggravated facilitation of illegal entry and related trafficking in human beings; or

3) an aggravated hunting offence.

Section 17
Traffic data monitoring with the consent of the owner of the network address or terminal equipment

To prevent an offence investigated by the Border Guard, the Border Guard may, with the consent of a person, conduct traffic data monitoring of the network address or terminal equipment controlled by him or her if there are reasonable grounds to assume that someone, on the basis of his or her statements or other behaviour, would commit an offence investigated by the Border Guard for which the most severe punishment by law is at least two years' imprisonment, or an offence investigated by the Border Guard committed using a network address or terminal equipment.

Section 18
Decision on traffic data monitoring

The decision on traffic data monitoring referred to in section 16, subsection 2 and in section 17 is made by a court at the request of an official with the power of arrest.

If a matter concerning traffic data monitoring referred to in subsection 1 cannot be delayed, the decision on traffic data monitoring may be made by an official with the power of arrest until such time as the court has made a decision on the request for an authorisation. The matter shall be brought for decision by a court as soon as possible, however, no later than 24 hours after the use of traffic data monitoring was started.

The authorisation may be granted for up to one month at a time, and it may also refer to a fixed period prior to granting the authorisation, which may be longer than one month.

The request and decision concerning traffic data monitoring shall specify:

1) the offence on which the action is based and its assumed time of commission;

2) the person who, with reasonable cause, may be assumed to commit an offence referred to in paragraph 1;

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

4) consent, if this is a precondition for the use of traffic data monitoring;

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

6) the network address or terminal equipment targeted by the action;

7) the official with the power of arrest who will be directing and supervising the traffic data monitoring;

8) any restrictions and conditions on the traffic data monitoring.

Section 19
Obtaining base station data and the preconditions for it

Obtaining base station data means acquisition 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 Border Guard may be authorised to obtain relevant base station data to prevent an offence investigated by it if there are reasonable grounds to assume that the person, on the basis of his or her statements, threats or behaviour or otherwise, would commit an offence for which the most severe punishment provided by law is at least four years' imprisonment.

Section 20
Decision on obtaining base station data

The decision on obtaining base station data is made by a court at the request of an official with the power of arrest. If the matter cannot be delayed, the decision on obtaining base station data may be made by an official with the power of arrest until such time as the court has made a decision on the request for an authorisation. The matter shall be brought for decision by a court as soon as possible, however, at the latest within 24 hours after the action was started.

The authorisation is granted for a certain time period.

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

1) the offence on which the action is based and its assumed time of commission;

2) the facts on which the preconditions for obtaining base station data are based;

3) the time period covered by the authorisation;

4) the base station covered by the authorisation;

5) the official with the power of arrest who will be directing and supervising the obtaining of the base station data;

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

Extended surveillance, covert intelligence gathering and technical surveillance

Section 21
Extended surveillance and the preconditions for it

Surveillance means making covert observations of a particular person for the purpose of gathering 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 visual observations.

Extended surveillance means other than short-term surveillance of a person who, with reasonable cause, may be assumed to commit an offence investigated by the Border Guard.

To prevent an offence investigated by the Border Guard, the Border Guard may conduct extended surveillance of a person referred to in subsection 2 if there are reasonable grounds to assume that he or she would commit an offence for which the most severe punishment by law is at least two years' imprisonment, or a receiving offence.

Surveillance referred to in this section of premises that are used for permanent residence is not permitted. A technical device may not be used in surveillance or extended surveillance of domestic premises referred to in chapter 24, section 11 of the Criminal Code.

Section 22
Decision on extended surveillance

The decision on extended surveillance is made by an official with the power of arrest.

A decision on extended surveillance may be made for up to six months at a time.

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

1) the offence on which the action is based and its assumed time of commission;

2) the person who, with reasonable cause, may be assumed to commit an offence referred to in paragraph 1;

3) the facts on which the suspicion of the person and the extended surveillance are based;

4) the validity period of the authorisation;

5) the official with the power of arrest who will be directing and supervising the extended surveillance;

6) any restrictions and conditions on the extended surveillance.

Section 23
Covert intelligence gathering and the preconditions for it

Covert intelligence gathering means intelligence gathering on a particular person during brief interaction, in which false, misleading or disguised information is used to conceal the border guard's task.

To prevent an offence investigated by the Border Guard, the Border Guard may use covert intelligence gathering if, on the basis of a person's statements or other behaviour, there are reasonable grounds to assume that he or she would commit the following:

1) aggravated facilitation of illegal entry; or

2) aggravated facilitation of illegal entry and related trafficking in human beings.

Covert intelligence gathering is not permitted in a place of residence even with the cooperation of the occupier.

Section 24
Decision on covert intelligence gathering

The decision on covert intelligence gathering is made by the Chief or Deputy Chief of the Legal Division of the Border Guard Headquarters to prevent an offence investigated by the Border Guard.

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

1) the action and its purpose in sufficient detail;

2) the administrative unit carrying out the covert intelligence gathering and the border guard responsible for it;

3) the offence on which the action is based;

4) the person who is the object of the covert intelligence gathering;

5) the facts on which the suspicion of the person is based;

6) the planned time for carrying out the action;

7) any restrictions and conditions on the covert intelligence gathering.

The decision shall be reviewed where necessary if circumstances change.

Section 25
On-site interception and the preconditions for it

On-site interception means, notwithstanding chapter 24, section 5 of the Criminal Code, audio monitoring, recording and other handling of a particular person's conversation or message not intended for the knowledge of outsiders and where the listener does not participate in the conversation, using a technical device, process or piece of software for the purpose of investigating the content of or participants in the conversation or message, or the activities of a person referred to in subsection 4.

On-site interception of premises used for permanent residence is not permitted.

To prevent an offence investigated by the Border Guard, the Border Guard has the right to engage in on-site interception of a person not inside premises used for permanent residence. The Border Guard may also be given authorisation to engage in on-site interception of a person who has been deprived of his or her liberty as a result of an offence and who is in the premises of a public authority. Interception can be carried out by arranging it at the premises or other location where the person on whom the intelligence is gathered can be assumed likely to stay or visit.

A further precondition for on-site interception is that, on the basis of the person's statements, threats or behaviour or otherwise, there are reasonable grounds to assume that he or she would commit an offence investigated by the Border Guard for which the most severe punishment by law is at least four years' imprisonment.

Notwithstanding subsection 2, the Border Guard always has the right to engage in short-term on-site interception if this is essential to carry out a Border Guard crime prevention measure safely and to avert an imminent danger to the life or health of the person carrying out the measure, the person to be apprehended or the person to be protected.

Section 26
Decision on on-site interception

The decision on on-site interception of a person who has been deprived of his or her liberty is made by a court at the request of an official with the power of arrest.

The decision on on-site interception referred to in section 25, subsection 5 and on-site interception other than that referred to in subsection 1 is made by an official with the power of arrest.

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

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

1) the offence on which the action is based and its assumed time of commission, or the danger on which the action is based;

2) the person who, with reasonable cause, may be assumed to commit an offence referred to in paragraph 1;

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

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

5) the premises or other location at which the on-site interception is arranged;

6) the official with the power of arrest who will be directing and supervising the on-site interception;

7) any restrictions and conditions on the on-site interception.

Section 27

Technical observation and the preconditions for it

Technical observation means, notwithstanding chapter 24, section 6 of the Criminal Code, surveillance or recording of a particular person or premises or other location using a camera or other technical device, process or piece of software located at the place.

Technical observation of premises used for permanent residence is not permitted.

To prevent an offence investigated by the Border Guard, the Border Guard has the right to engage in technical observation of a person not inside premises used for permanent residence. The Border Guard may also be given authorisation to engage in technical observation of a person who has been deprived of his or her liberty as a result of an offence and who is in the premises of a public authority. Observation can be carried out by arranging it at the premises or other location where the person on whom the intelligence is gathered can be assumed likely to stay or visit.

A precondition for the technical observation of domestic premises or other location referred to in chapter 24, section 11 of the Criminal Code and of a person who has been deprived of his or her liberty as a result of an offence is that there are reasonable grounds to assume, on the basis of the person's statements, threats or behaviour or otherwise, that he or she would commit an offence investigated by the Border Guard and referred to in section 25, subsection 4. The precondition for other technical observation is that it can, with reasonable cause, be assumed that the person would commit an offence investigated by the Border Guard for which the most severe punishment by law is at least one year's imprisonment.

Notwithstanding subsection 2, the Border Guard always has the right to engage in technical observation if this is essential to carry out a Border Guard crime prevention measure safely and to avert an imminent danger to the life or health of the person carrying out the measure, the person to be apprehended or the person to be protected.

Section 28

Decision on technical observation

The decision on technical observation is made by a court at the request of an official with the power of arrest when the observation targets domestic premises or other location referred to in chapter 24, section 11 of the Criminal Code or a person who has been deprived of his or her liberty as a result of an offence.

The decision on technical observation referred to in section 27, subsection 5 and on technical observation other than that referred to in subsection 1 is made by an official with the power of arrest.

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

The request and decision concerning technical observation shall specify:

1) the offence on which the action is based and its assumed time of commission, or the danger on which the action is based;

2) the person who, with reasonable cause, may be assumed to commit an offence referred to in paragraph 1;

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

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

5) the premises or other location at which the observation is arranged;

6) the official with the power of arrest who will be directing and supervising the technical observation;

7) any restrictions and conditions on the technical observation.

Section 29
Technical tracking and the preconditions for it

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 piece of software.

To prevent an offence investigated by it, the Border Guard may arrange technical tracking of an object, substance or item of property that is the object of an offence or assumed to be in the possession or likely to come into the possession of the person who, on the basis of his or her statements, threats or behaviour or otherwise, may, with reasonable cause, be assumed to commit an offence investigated by the Border Guard for which the most severe punishment by law is at least one year's imprisonment.

If the purpose of technical tracking is to track a person's movements by positioning a tracking device in the clothes that he or she is wearing or in an object he or she is carrying (*technical tracking of a person*), this action may be performed only if there are reasonable grounds to assume that he or she would commit an offence referred to in section 16, subsection 2.

The Border Guard also has the right to engage in technical tracking if this is essential to carry out a Border Guard crime prevention measure safely and to avert an imminent danger to the life or health of the person carrying out the duty, the person to be apprehended or the person to be protected.

Section 30
Decision on technical tracking

The decision on the technical tracking of a person is made by a court at the request of an official with the power of arrest. If the matter cannot be delayed, the decision on tracking may be made by an official with the power of arrest until such time as the court has made a decision on the request for an authorisation. The matter shall be brought for decision by a court as soon as possible, however, at the latest within 24 hours after the action was started.

The decision on technical tracking referred to in section 29, subsection 4 and on technical tracking other than that referred to in subsection 1 is made by an official with the power of arrest.

The authorisation may be granted and the decision made for up to six months at a time.

The request and decision concerning technical tracking shall specify:

1) the offence on which the action is based and its assumed time of commission, or the danger on which the action is based;

2) the person who, with reasonable cause, may be assumed to commit an offence referred to in paragraph 1;

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

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

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

6) the official with the power of arrest who will be directing and supervising the technical tracking;

7) any restrictions and conditions on the technical tracking.

Section 31
Technical surveillance of a device and the preconditions for it

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 that is important for preventing an offence.

Technical surveillance of a device may not be used to obtain information on the content of a message nor identification data.

To prevent an offence investigated by the Border Guard, the Border Guard may be given authorisation to engage in technical surveillance of a device if, on the basis of the person's statements, threats or behaviour or otherwise, there are reasonable grounds to assume that he or she would commit an offence referred to in section 25, subsection 4. The Border Guard may target

technical surveillance of a device at a computer or other similar technical device, or the operation of its software, that is likely to be used by the person in question.

Section 32
Decision on technical surveillance of a device

The decision on technical surveillance of a device is made by a court at the request of an official with the power of arrest. If the matter cannot be delayed, the decision on technical surveillance of a device may be made by an official with the power of arrest until such time as the court has made a decision on the request for an authorisation. The matter shall be brought for decision by a court as soon as possible, however, no later than 24 hours after the intelligence gathering method was started.

The authorisation may be granted for up to one month at a time.

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

1) the offence on which the action is based and its assumed time of commission;

2) the person who, with reasonable cause, may be assumed to commit an offence referred to in paragraph 1;

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

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

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

6) the official with the power of arrest who will be directing and supervising the technical surveillance of a device;

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

Section 33

Gathering data identifying a network address or terminal equipment

To prevent an offence investigated by it, the Border Guard may use a technical device to gather data identifying a network address or terminal equipment if the most severe punishment by law for the offence to be prevented is at least one year's imprisonment.

To obtain the data referred to in subsection 1, the Border Guard may only use technical devices which can be deployed solely for identifying a network address and terminal equipment. The Finnish Transport and Communications Agency inspects the technical device to ensure that it meets the requirements provided in this subsection and that the device, due to its properties, does not cause any harmful interference with the equipment or services of a public communications network.

The decision on gathering data identifying a network address or terminal equipment is made by an official with the power of arrest.

Section 34
Installation and removal of a device, process or piece of software

A border guard has the right to position a device, process or piece of software used for technical surveillance in the object, substance, item of property, premises or other location, or information system, targeted by the action if this is required for the surveillance to be carried out. To install, start using or remove a device, process or piece of software, a border guard has the right to secretly go to the above mentioned 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. Separate provisions are issued on searches of a domicile.

A device, process or piece of software to be used for technical surveillance may be installed in premises used for permanent residence only if a court has given authorisation for this based on the request of an official with the power of arrest or if the installation is essential in cases referred to in section 25, subsection 5; section 27, subsection 5; and section 29, subsection 4.

Section 35
Protecting border guards in covert intelligence gathering for the prevention of an offence

An official with the power of arrest may decide that the border guard performing covert intelligence gathering be equipped with a technical device that enables audio and visual monitoring, if this is justified to ensure his or her 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 border guard. 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. The recordings shall be destroyed when the case is final or is discontinued.

Use of covert human intelligence sources, and controlled deliveries

Section 36
Use of covert human intelligence sources

Use of covert human intelligence sources means other than occasional, confidential receipt from a person outside the border guard authorities and outside other criminal investigation authorities, of significant information for managing tasks relating to the prevention and investigation of offences prescribed by law for investigation by the Border Guard (*covert human intelligence source*).

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

Section 37
Controlled delivery and the preconditions for it

The Border Guard may refrain from intervening in the transport or other delivery of an object, substance or item of property or delay such intervention, if this is necessary to identify persons involved in the commission of an offence in progress or to prevent a more serious or larger offence (*controlled delivery*).

The Border Guard may use a controlled delivery to prevent an offence investigated by the Border Guard for which the most severe punishment by law is at least four years' imprisonment. It is

further required that the controlled delivery can be monitored and intervention used if necessary. Furthermore, the action may not pose a significant danger to anyone's life, health or liberty, or a significant danger of substantial damage to the environment or property, or of a substantial financial loss. Separate provisions are issued on the cooperation between public authorities in carrying out a controlled delivery.

Separate provisions are issued on international controlled deliveries under international agreements or other international obligations binding on Finland.

Section 38
Decision on a controlled delivery

The decision on a controlled delivery performed by the Border Guard is made by the Chief or Deputy Chief of the Legal Division of the Border Guard Headquarters.

A decision may be made for up to one month at a time.

The decision shall specify:

1) the offence on which the action is based and its time of commission;

2) the person who, with reasonable cause, may be assumed to commit an offence referred to in paragraph 1;

3) the facts on which the suspicion of the person is based;

4) the purpose and execution plan for the intelligence gathering;

5) the transport or other delivery targeted by the action;

6) the validity period of the decision;

7) any restrictions and conditions on the controlled delivery.

Provisions on the notification of the decision referred to in this section to the PCB criminal intelligence unit referred to in section 5 of the Act on Cooperation between the Police, Customs and the Border Guard are laid down by government decree.

Common provisions

Section 39
Procedure in court

The provisions of chapter 3, sections 1, 3, 8 and 10 of the Coercive Measures Act on a remand hearing shall be complied with in a court's consideration of and decisions on matters of authorisation concerning secret intelligence gathering.

A request to use a secret intelligence gathering method shall be considered by a court without delay in the presence of the border guard who made the request or a border guard designated by him or her who is familiar with the matter. The matter shall be decided urgently. The court hearing can also be conducted using video conferencing or another suitable technical data transmission method where the participants are connected in such a way that they can hear and see each other.

If a court has granted an authorisation for traffic data monitoring, it may examine and decide a matter concerning the granting of an authorisation for another network address or terminal equipment in the absence of the border guard who made the request or of a border guard designated by him or her, if less than one month has elapsed since the oral hearing of the matter concerning granting an authorisation for the same offence to be prevented. The matter may also be considered in the absence of the said border guard if the use of the intelligence gathering method has already been discontinued.

The matter may be decided without hearing the person who, with reasonable cause, may be assumed to commit or to have committed an offence investigated by the Border Guard, or the holder of the network address or terminal equipment or the occupier of the premises where the audio or visual monitoring is taking place. When considering a matter referred to in section 17, the holder of the network address or terminal equipment shall, however, be provided with an opportunity to be heard, unless this is precluded for reasons connected with the prevention of an offence. In considering a matter concerning on-site interception and technical observation of a

person who has been deprived of his or her liberty, a representative of the establishment where the person is being held shall be provided with an opportunity to be heard, unless this in unnecessary in view of his or her previous hearing.

No appeal may be made against decisions issued on matters concerning authorisations. A complaint may be filed against the decision, with no time limit. The complaint shall be considered urgently.

Section 40
Protection of secret intelligence gathering

When using a secret intelligence gathering method, the Border Guard has the right to delay intervention in an offence if this delay does not pose a significant danger to anyone's life, health or liberty, or a significant danger of substantial damage to the environment or property, or of a substantial financial loss. It is further required that delaying is necessary to avoid revealing the intelligence gathering or to secure the purpose of the operation.

The Border Guard may use false, misleading or disguised information, make and use false, misleading or disguised register entries, and produce and use false documents when this is necessary to protect the use of a secret intelligence gathering method that has already been completed, is ongoing or is to be used in the future.

The register entries referred to in subsection 2 shall be corrected after the preconditions referred to in the subsection no longer exist.

Section 41
Decision on protection

The decision to make register entries and produce documents referred to in section 40, subsection 2 is made by the Chief or Deputy Chief of the Legal Division of the Border Guard Headquarters.

The decision on the protection of intelligence gathering other than that referred to in subsection 1 is made by a border guard with the power of arrest who is separately appointed to the task and specially trained in secret intelligence gathering.

The Chief or Deputy Chief of the Legal Division of the Border Guard Headquarters shall keep a record of the entries made and documents produced by the Border Guard, oversee their use and see to the correction of the entries.

Section 42
Disclosure prohibition concerning secret intelligence gathering

For an important reason connected with the prevention of an offence, an official with the power of arrest may prohibit third parties from disclosing any details they may have of the use of a secret intelligence gathering method. It is further required that the third party, due to his or her task or position, has assisted or was requested to assist in carrying out the secret intelligence gathering 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.

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.

Section 43
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 chapter.

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

Section 44
Prohibitions concerning audio and visual monitoring

The provisions of chapter 10, section 52 of the Coercive Measures Act apply to prohibitions on on-site interception and technical observation.

Section 45
Inspecting recordings and documents

The recordings and documents accumulated during the use of a secret intelligence gathering method shall be inspected without undue delay by an official with the power of arrest or a public official designated by him or her.

Section 46
Examining recordings

Recordings accumulated during the use of a secret intelligence gathering method may be examined only by a court or an official with the power of arrest. By order of an official with the power of arrest or in accordance with the instruction of the court, a recording may also be examined by another border guard, an expert or other person assisting in carrying out the intelligence gathering.

Section 47
Surplus information

Surplus information means information obtained by traffic data monitoring, obtaining base station data and technical surveillance that is not related to an offence or averting a danger, or that concerns an offence other than the one for the prevention of which the authorisation has been granted or the decision made.

Section 48
Use of surplus information

The Border Guard may use surplus information in the investigation of an offence investigated by the Border Guard if the information concerns an offence investigated by the Border Guard for the prevention of which it would have been possible to use the intelligence gathering method under this chapter with which the information has been obtained.

The Border Guard may also use surplus information if its use can be assumed to be of very great importance for the investigation of an offence investigated by the Border Guard and the most severe punishment by law for the offence is at least three years' imprisonment.

The use of surplus information as evidence is decided by a court in connection with the hearing of the main matter. Provisions on noting the use of surplus information in criminal investigation records are laid down in chapter 9, section 6, subsection 2 of the Criminal Investigation Act, and provisions on notifying its use in an application for a summons are laid down in chapter 5, section 3, subsection 1, paragraph 8 of the Criminal Procedure Act (689/1997).

In addition, surplus information may always be used to prevent an offence investigated by the Border Guard, to direct the crime prevention operations of the Border Guard and as evidence in support of innocence.

Surplus information may also be used to prevent a significant danger to life, health or liberty, or substantial damage to the environment or property, or a substantial financial loss. If the prevention of the danger or damage referred to above does not fall within the powers of the Border Guard, the matter is transferred to a competent authority without delay.

Provisions on the use of surplus information obtained under the Coercive Measures Act to prevent an offence investigated by the Border Guard are laid down in chapter 10, section 56 of the Coercive Measures Act.

Section 49 (643/2019)
Destroying information

Information obtained through a secret intelligence gathering method shall be destroyed without delay once it has become evident that the information is not needed to prevent or investigate an offence or to avert a danger.

Surplus information may, however, be held and stored in accordance with the Act on the Processing of Personal Data by the Border Guard if the information concerns an offence referred to in section 48, subsection 1 or 2 of this Act or if the information is necessary to prevent an offence referred to in chapter 15, section 10 of the Criminal Code. Information not stored or incorporated in criminal investigation material shall be destroyed without undue delay once it has become

evident that the information cannot be used or that it is no longer needed to prevent or investigate an offence.

Base station data shall be destroyed once it has become evident that the information is not needed to prevent or investigate an offence or to avert a danger.

Section 50
Interrupting on-site interception and technical surveillance of a device

If it becomes evident 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 gathering method shall be interrupted 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 and to destroy recordings and notes also applies to technical surveillance of a device if it becomes evident that the surveillance is directed at the content of a message or at identification data, or that the device targeted by the surveillance is not used by the person referred to in section 31, subsection 3.

Section 51
Destroying information obtained urgently

If, in urgent situations referred to in section 18, subsection 2; section 20, subsection 1; section 30, subsection 1; or section 32, subsection 1, an official with the power of arrest has decided to begin traffic data monitoring, obtaining base station data, technical tracking of a person or technical surveillance of a device, but a court deems that the preconditions for the action have not been met, it shall cease and the material obtained by the action and the notes on the information obtained shall be destroyed immediately. However, the use of information obtained in this way is permitted under the same conditions that apply to the use of surplus information under section 48.

Section 52
Notification of use of a secret intelligence gathering method

The object of intelligence gathering shall be notified in writing without delay of the traffic data monitoring, extended surveillance, covert intelligence gathering, technical surveillance or controlled delivery once the purpose of the intelligence gathering has been achieved. The use of a

secret intelligence gathering method shall, however, be notified to the object of the intelligence gathering no later than one year after use of the method ceased.

At the request of an official with the power of arrest, a court may decide that the notification referred to in subsection 1 to the target of intelligence gathering may be postponed for up to two years at a time if this is justified to secure ongoing intelligence gathering, to ensure State security or to protect lives or health. By decision of the court, the notification need not be sent at all if this is essential to ensure State security or to protect lives or health.

If the identity of the object of intelligence gathering is not known by the expiry of the time limit or postponement referred to in subsection 1 or 2, the use of the intelligence gathering method shall be notified in writing without undue delay as soon as the identity is established.

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

For extended surveillance and covert intelligence gathering, there is no obligation to notify the object of the intelligence gathering unless a criminal investigation has been started into the matter. If a criminal investigation is started, the provisions of chapter 10, section 60 of the Coercive Measures Act shall be observed.

When considering postponing the notification or not sending it in cases referred to in subsections 2 and 5, the assessment shall also take into account the right of the party to properly secure his or her rights.

The provisions of section 39 apply to the consideration in court of the matter concerning the notification.

Section 53
Record

After discontinuing the use of a secret intelligence gathering method other than surveillance, a record shall be prepared without undue delay.

Further provisions on entry of actions may be issued by decree of the Ministry of the Interior.

Section 54
Restriction on parties' right of access in certain cases

By derogation from section 11 of the Act on the Openness of Government Activities (621/1999), a person whose rights or obligations are affected by the matter has no right of access to information on the use of an intelligence gathering method referred to in this chapter until the notification referred to in section 52 of this Act has been made. Neither does he or she have the right of access of the data subject referred to in the Act on the Processing of Personal Data in Criminal Matters in Connection with Maintaining National Security (1054/2018). (643/2019)

Once a notification referred to in section 52 has been made, a person referred to in subsection 1 has the right of access to information about documents or recordings concerning the use of a secret intelligence gathering method, unless withholding the information is essential to ensure State security or to protect life, health or privacy, or secret tactical and technical methods. When considering withholding a document, a recording or information, the assessment shall also take into account the right of a person referred to in subsection 1 to properly secure his or her rights.

Information on an audio or visual recording may only be given by making it available for listening or viewing at the premises of the Border Guard if, in view of the content of the recording, there is reason to assume that providing the information in any other way could lead to a violation of the protection of privacy of a person appearing in the recording.

Section 55
Telecommunications operators' obligation to assist, and access to certain premises

A telecommunications operator shall, without undue delay, make the telecommunications network connections required by traffic data monitoring. The same also applies to situations where the Border Guard performs the traffic data monitoring using a technical device. A telecommunications operator shall also make available to an official with the power of arrest the information in their possession that is necessary for carrying out technical tracking.

Section 56 (1351/2019)
Compensation to telecommunications operators

Telecommunications operators have the right to receive compensation from state funds for the direct costs incurred in assisting public authorities and disclosing information as referred to in this chapter, in compliance with section 299 of the Act on Electronic Communication Services. The decision on the payment of compensation is made by the administrative unit that carried out the action.

An administrative review may be requested in respect of the decision on the payment of compensation. 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). The administrative court shall provide the Finnish Transport and Communications Agency with an opportunity to be heard.

Section 57
Effect of mitigated penal latitude

Determining sentences in accordance with a mitigated penal latitude, applying chapter 6, section 8 of the Criminal Code, does not affect the use of intelligence gathering methods referred to in this chapter.

Chapter 4
Covert coercive measures

Section 58
Use of covert coercive measures

Chapter 10 of the Coercive Measures Act applies to the use of covert coercive measures in a criminal investigation conducted by the Border Guard subject to the exceptions provided below.

The Border Guard may not use undercover activities, pseudo purchases and controlled use of covert human intelligence sources.

The Border Guard has the right to use:

1) telecommunications interception, obtaining data other than through telecommunications interception and covert intelligence gathering only when investigating aggravated facilitation of illegal entry or aggravated facilitation of illegal entry and related trafficking in human beings or aggravated trafficking in human beings;

2) traffic data monitoring only when investigating aggravated facilitation of illegal entry, aggravated facilitation of illegal entry and related trafficking in human beings or aggravated trafficking in human beings, an aggravated receiving offence, a professional receiving offence, aggravated forgery, an aggravated hunting offence or aggravated concealing of poached game;

3) technical tracking of a person only when investigating aggravated facilitation of illegal entry or aggravated facilitation of illegal entry and related trafficking in human beings or aggravated trafficking in human beings or an aggravated hunting offence.

When conducting other criminal investigation referred to in section 5, a border guard may not use the following secret coercive measures: telecommunications interception, obtaining data other than through telecommunications interception, traffic data monitoring, covert intelligence gathering, technical tracking of a person, undercover activities, pseudo purchases and controlled use of covert human intelligence sources.

Section 59
Decision on covert intelligence gathering in criminal investigation of an offence

The Chief or Deputy Chief of the Legal Division of the Border Guard Headquarters decides on covert intelligence gathering for the purpose of investigating an offence investigated by the Border Guard.

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

1) the action and its purpose in sufficient detail;

2) the administrative unit carrying out the covert intelligence gathering and the border guard responsible for it;

3) the suspected offence;

4) the person who is the object of the covert intelligence gathering;

5) the facts on which the suspicion of an offence is based;

6) the planned time for carrying out the action;

7) any restrictions and conditions on the covert intelligence gathering.

The decision shall be reviewed where necessary if circumstances change.

Section 60
Protecting a border guard in covert intelligence gathering in criminal investigation of an offence

An official with the power of arrest may decide that the border guard carrying out covert intelligence gathering in criminal investigation of an offence shall be equipped with a technical device that enables audio and visual monitoring if this is justified to ensure his or her 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 border guard. 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 that case, the recordings shall be destroyed when the case is final or discontinued.

Section 61
Decision on a controlled delivery in criminal investigation of an offence

The Chief or Deputy Chief of the Legal Division of the Border Guard Headquarters decides on a controlled delivery for the purpose of investigating an offence investigated by the Border Guard.

A decision on a controlled delivery may be made for up to one month at a time.

The decision concerning a controlled delivery shall specify:

1) the suspected offence and the time of its commission;

2) the person suspected of the offence;

3) the facts on which the criminal suspicion of the person is based;

4) the purpose and execution plan for the intelligence gathering;

5) the transport or other delivery targeted by the action;

6) the validity period of the decision;

7) any restrictions and conditions on the controlled delivery.

Provisions on the notification of the decision referred to in this section to the PCB criminal intelligence unit referred to in section 5 of the Act on Cooperation between the Police, Customs and the Border Guard are laid down by government decree.

Chapter 5
Miscellaneous provisions

Section 62
Oversight of secret intelligence gathering and use of covert coercive measures

The Border Guard Headquarters and the administrative units using secret intelligence gathering methods oversee the intelligence gathering referred to in this Act. Provisions on the oversight of covert coercive measures are laid down in chapter 10, section 65 of the Coercive Measures Act.

The Border Guard provides the Ministry of the Interior each year with an account of the use and oversight of secret intelligence gathering methods and covert coercive methods and their protection.

Provisions on reports to be submitted to the Parliamentary Ombudsman concerning secret intelligence gathering and covert coercive measures are laid down in the Police Act (872/2011) and in the Coercive Measures Act.

Further provisions on the arrangement and oversight of the use of secret intelligence gathering methods referred to in this Act, on the recording of actions and on accounts to be supplied for oversight purposes may be given by government decree.

Section 63
Crime prevention measures extending to the territory of a foreign state

To investigate an offence or to apprehend suspects, the Border Guard has the right to continue in the territory of a foreign state the pursuit, surveillance or technical surveillance of persons that was started in Finland, in accordance with the provisions on continuing these actions in the territory of foreign states laid down in European Union law or any international treaty binding on Finland.

In performing the task referred to in subsection 1, a border guard has the powers specified in European Union law and international treaties binding on Finland that are referred to in this Act. The same provisions that apply to official duties carried out in Finland apply to official duties and rights of a border guard when carrying out the duties referred in subsection 1 outside the territory of Finland.

Section 64
Further provisions

Where necessary, further provisions on prohibitory lines and other signs which, in accordance with the Coercive Measures Act, may be used to mark buildings, rooms or areas closed by the Border Guard to safeguard the investigation of an offence investigated by the Border Guard are issued by decree of the Ministry of the Interior.

Section 65
Entry into force

This Act enters into force on 1 April 2018.