

Appendix I

On the use of the investigatory power of selection by the AIVD and the MIVD

CTIVD no 64

(adopted on 4 September 2019)



Review Committee
on the Intelligence and
Security Services

1. Introduction

'Selection' is the exercise of an investigatory power by which data is retrieved from the intercepted data stream using investigation-related interception. This might be, for example, the analysis of a telephone conversation or a sent email message. Selection is carried out with a view to learning the content of the selected data acquired through investigation-related interception. When the selected data has been made available to the relevant team, they determine whether the information is relevant to their own investigation or other investigations.

This appendix explains the assessment framework of the investigatory power of selection under Section 50(1)(a) of the Intelligence and Security Services Act 2017 (ISS Act 2017). The assessment framework in this report consists of the obligations ensuing from the power of selection under the ISS Act 2017, the Policy Rules of the ISS Act 2017, commitments undertaken by the Minister of the Interior and Kingdom Relations and the Minister of Defence, the standards ensuing from the European Convention on Human Rights and the case law of the European Court of Human Rights. These sources result in requirements for the use of selection as an investigatory power.

The assessment framework is structured as follows. Section 2 explains the three-stage model of investigation-related interception and the position of the investigatory power of selection. Section 3 lists the authorization requirements to use the investigatory power as well as some special requirements for processing data on selection. Section 4 addresses the requirement 'as targeted as possible' and Section 5 discusses the legal framework of data reduction in the context of selection. Section 6 deals with the duty of care. This is followed in Section 7 by an overview of the legal requirements against which the CTIVD reviews the use of selection as an investigatory power.

2. The three-stage model of investigation-related interception

This section explains the system of investigation-related interception based on the three stages defined in the explanatory memorandum of the ISS Act 2017.¹ The explanatory memorandum contains a great deal of information on the conditions for the use and scope of the investigatory powers regarding investigation-related interception. Clarifying the legal framework not only benefits the legal certainty of those involved but also provides the oversight body with guidelines.

The rationale for distinguishing three stages is essentially a legal one because in practice the stages take place continuously and influence each other constantly.² This is also evident from the submitted applications to use the relevant special investigatory powers as referred to in Sections 48-50 of the ISS Act 2017. In practice the services file an application that combines interception and optimization of interception (Section 48 in conjunction with Section 49(1) of the ISS Act 2017) while another application combines selection and optimization (Section 49(2) in conjunction with Section 50(1)(a) of the ISS Act 2017).

To sum up, the three stages are (1) interception of communication, (2) the optimization of the interception process and (3) the analysis of the content of communication and metadata (information about the communication).

2.1 Interception

The investigatory power termed ‘investigation-related interception of communication’ forges an unmistakable connection with the Integrated Intelligence Security Services Order (hereinafter: Integrated Order). The Integrated Security and Intelligence Order contains specific investigation assignments for the AIVD and the MIVD and is adopted by the Prime Minister, the Minister of General Affairs, the Minister of the Interior and Kingdom Relations and the Minister of Defence. In addition, there may be urgent investigation assignments that are also approved at ministerial level.³ After the Integrated Order has been adopted, the services draw up investigation assignments based on the applicable legal tasks in which the purpose and necessity of the investigation is recorded. Examples of an investigation assignment given in the explanatory memorandum include the acquisition of telecommunication in a mission area and the acquisition of the metadata of communication between regions under the control of terrorists and the Netherlands.⁴ Investigation assignments only relate to the implementation of tasks of the AIVD and the MIVD. The investigatory power of investigation-related interception may only be implemented in the context of intelligence and security tasks.⁵

In the first stage of the system of investigation-related interception, communication is intercepted in order to carry out the investigation assignments.⁶ The investigatory power of interception itself is laid down in Section 48 of the ISS Act 2017. The investigatory power also entails decrypting

¹ Parliamentary Documents II 2016/17, 34588, no. 3, pp. 96-109.

² See *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 96.

³ *Parliamentary Documents II* 2016/17, 34588, no. 3, pp. 90.

⁴ *Parliamentary Documents II* 2016/17, 34588, no. 3, pp. 95.

⁵ More specifically relating to the implementation of Section 8(2)(a) and (d) and Section 10(a), (c) and (e) of the ISS Act 2017 (see Section 28(1) of the ISS Act 2017).

⁶ In more legal wording, it concerns the investigatory power to use a technical tool to conduct investigation-related interception, reception, recording and listening to any form of telecommunication or data transfer using a computerized device or system irrespective of where these matters take place.

telecommunication or data transfer and conducting a technical analysis of the information in so far as this is aimed at optimizing the use of the investigatory power of interception. During the technical analysis, the contents of the communication may only be checked for correct rendition of reception (i.e. a quality control), for example whether or not the communication consists of noise.⁷

Once the services are convinced of the purpose and necessity, proportionality and subsidiarity of the use, the Minister of the Interior and Kingdom Relations and/or the Minister of Defence will be asked to authorize the requested form of investigation-related interception for the period of a maximum of one year. With the introduction of Article 5 of the Policy Rules of the ISS Act 2017, the application for authorization must expressly specify how the use of the investigatory powers will be as targeted as possible (see Section 4 for further details).

The application for interception must contain a characterization of the telecommunication or data transfer using a computerized device or system against which the investigatory power is to be exercised. The application must also show what type of interception is being referred to: interception of satellite and radio communications or cable traffic. Furthermore, where possible, the nature of the traffic must be specified, such as GSM, radio or internet traffic, combined with a geographical demarcation. In addition, the AIVD and the MIVD must include in their application which types of traffic are relevant, such as speech, (digital) chat or document exchange. Where it concerns interception of cable traffic, the application must indicate the part of the cable infrastructure and type of traffic to be intercepted.⁸ The services may request information from communication service providers to help them select the section of the infrastructure to conduct interception in. These providers have a duty to assist in providing information and allowing interception.⁹ The services select those data streams which are reasonably expected to be relevant to answering ongoing investigations assignments by the services.¹⁰

Based on Section 48(3) of the ISS Act 2017, additional substantiation is required if the interception of metadata only does not suffice. Only specially authorized staff may consult the data to decrypt the information and conduct the technical analysis to check the correct reception (including the contents of the communication).

After obtaining the authorization from the relevant minister, the application to use the special investigatory power is submitted to the Review Board for the Use of Powers (TIB). If the TIB is of the opinion that the authorization is lawful, the interception may commence.

2.2 Optimization of the interception process

The second stage in the system of investigation-related interception aims to optimize the results of the interception (*search aimed at interception*, regulated in Section 49(1) of the ISS Act 2017) and to optimize the subsequent selection process (*search aimed at selection*, Section 49(2) of the ISS Act 2017).¹¹ At this stage it is not so much about consulting the data but about collecting the information with which the interception process in particular can be optimized in a broader sense.

⁷ See *Parliamentary Documents II* 2016/17, 34588, no. 3, pp. 97-103 (under the heading 'stage 1').

⁸ *Parliamentary Documents II* 2016/17, 34588, no. 3, pp. 99.

⁹ Section 53 ff. of the ISS Act 2017.

¹⁰ *Parliamentary Documents II* 2016/17, 34588, no. 3, pp. 110.

¹¹ *Parliamentary Documents II* 2016/17, 34588, no. 3, pp. 95.

Search aimed at interception

Search aimed at interception is about exploring telecommunication. The investigatory power in Section 49(1) of the ISS Act 2017 intends to explore the use of telecommunication networks by establishing the characteristics and nature of the telecommunication, as well as the identity of the person or organization connected to that telecommunication. This search form is primarily aimed at optimizing interception, mainly looking at the nature of the traffic. That includes identifying the language of the communication. In many cases this process is conducted by automated processes. Search aimed at interception pertains to the technical characteristics and nature of the communication, such as protocols, frequencies, language and the quality of the interception.¹²

Under Section 49(4) of the ISS Act 2017, the use of the investigatory power requires the authorization of the minister responsible for the relevant service. This authorization may be granted for the period of one year, with the option to extend for a further year. As noted in the introduction to this section, in practice this concerns an order combining Sections 48 and 49(1) of the ISS Act 2017.

Search aimed at selection

Search aimed at selection is concerned with optimizing selection in the system of investigation-related interception. This investigatory power is regulated in Section 49(2) of the ISS Act 2017. The first step in exercising this investigatory power is establishing and verifying the selection criteria in relation to the persons, organizations and topics that are being investigated by the services. The resulting intercepted telecommunication can then be examined for selection criteria that could yield relevant data for the services' investigation into persons or organizations. In addition, potential selection criteria can be verified on their usefulness, by examining the results of the intercepted telecommunication to see if these yield any relevant data for the investigation.¹³

The investigatory power in Section 49(2) of the ISS Act 2017 also enables - in connection with ongoing investigations - the identification of persons or organizations who qualify for investigation by the AIVD or the MIVD.¹⁴ In other words, the investigatory power makes it possible to identify or pinpoint potential targets as well.¹⁵ Using the results from the newly intercepted telecommunication and based on the data from ongoing investigations, checks can be conducted to see whether any connections can be made to people or organizations that possibly qualify for investigation by the AIVD or the MIVD. If the search of the telecommunication yields new targets or organizations that qualify for investigation by the AIVD or the MIVD, authorization must be sought to use the content of that communication, as referred to in Section 50(2) of the ISS Act 2017.¹⁶

Under Section 49 of the ISS Act 2017 the use of the special investigatory power requires the authorization of the minister responsible for the relevant service. The granted authorization is valid for a period of three months. Based on Section 49(5) of the ISS Act 2017, only specifically designated officials may consult the stored content from investigation-related interception. Section 49(3) of the ISS Act 2017 states that records may be kept of the results of the investigation as referred to in Section 49 of the ISS Act 2017, if the services need to do so to properly perform their tasks.

¹² *Parliamentary Documents II* 2016/17, 34588, no. 3, pp. 104.

¹³ *Parliamentary Documents II* 2016/17, 34588, no. 3, pp. 106. See CTIVD report no. 28 (2011), p. 43.

¹⁴ *Parliamentary Documents II* 2016/17, 34588, no. 3, pp. 107.

¹⁵ *Parliamentary Documents II* 2016/17, 34588, no. 3, pp. 106. See CTIVD report no. 28 (2011), p. 44.

¹⁶ *Parliamentary Documents II* 2016/17, 34588, no. 3, pp. 107.

2.3 Analysis of data

The third stage of the system of investigation-related interception is the selection of communication with a view to learning the content of the selected data.¹⁷ The investigatory power to apply selection to the intercepted data is laid down in Section 50(1)(a) of the ISS Act 2017.

Also during this third stage of investigation-related interception, metadata analysis takes place, which can be focused on identifying persons or organizations. At this stage only the metadata of the information is looked at, not the content. This investigation activity is regulated by the investigatory power of automated data analysis in Section 50(1)(b) of the ISS Act 2017 where it concerns metadata obtained through investigation-related interception and the analysis is aimed at identifying persons or organizations.

¹⁷ *Parliamentary Documents II* 2016/17, 34588, no. 3, pp. 107.

3. Requirements when implementing the power of selection

Due to the severe privacy infringement inherent to both the acquisition and further processing of the intercepted data, further safeguards have been put in place for the use of the investigatory power of selection.¹⁸

The following section contains a brief description of the general requirements that apply as a safeguard when using the investigatory power of selection.

3.1 Authorization requirements

The team of the AIVD or the MIVD drafts an application to use the investigatory power of selection as referred to in Section 50(1)(a) of the ISS Act 2017. That legislation states that the Minister of the Interior and Kingdom Relations or the Minister of Defence must grant authorization to use the investigatory power. The TIB then conducts its lawfulness assessment. In practice this involves several intermediary links.¹⁹ Before the head of the service forwards the application to the minister, others, including lawyers of the AIVD and the MIVD, examine the application. The head of the service signs the application to use the investigatory power of selection. The explanatory memorandum²⁰ illustrates the authorization procedure as part of the review system in the ISS Act 2017 as follows:

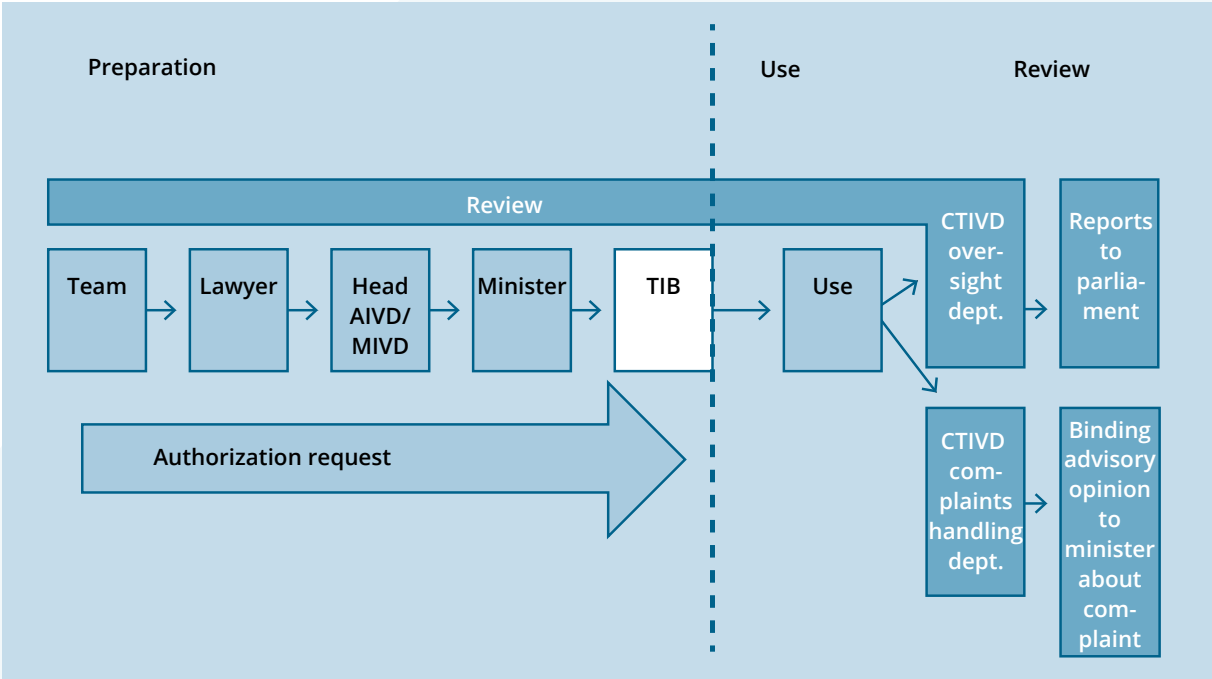


Figure 1: review regime ISS Act 2017.

The current review regime with safeguards for the use of investigatory powers appears to comply with the requirements set by the European Court of Human Rights (ECHR). The ECHR sets strict requirements to national legislation for the use of ‘bulk interception’ by the intelligence and security

¹⁸ *Parliamentary Documents II* 2016/17, 34588, no. 3, pp. 96.
¹⁹ The minister may also appeal to the legal affairs department of the ministry involved to assess the application.
²⁰ *Parliamentary Documents II* 2016/17, 34588, no. 3, pp. 52.

services.²¹ In the Big Brother Watch case, the ECHR ruled that the United Kingdom's review of the use of selectors and search terms for automated searches of data intercepted in bulk and its subsequent analysis of the stored material was insufficient. According to the ECHR, a strict demarcation and check of substantive data from bulk interception is important in the selection and analysis of the intercepted communication.²² Briefly put, in the Big Brother Watch case the system in the United Kingdom was found to be inadequate due to the lack of effective review by a judicial body or independent review body.²³

In the Netherlands, Section 50 of the ISS Act 2017 introduces an independent assessment by the TIB for (among other things) the use of the investigatory power of selection. The assessment by the TIB also applies to the investigatory power used for metadata analysis of data from investigation-related interception, in so far as this is aimed at the identification of persons and organizations. In addition, an independent check is made by the CTIVD during and after the use of the investigatory power. It is our expectation, therefore, that the Netherlands has sufficient safeguards in place for the application of the investigatory power of selection.

Selection criteria are applied to the use of the investigatory power of selection. Selection criteria are for example telephone numbers or email addresses connected with a target. They could also be keywords related to a specified topic and connected with a certain investigation assignment.²⁴ Section 50(3) of the ISS Act 2017 stipulates that the selection criteria are established by either the minister concerned or by the head of service on his behalf. This authorization power may, also based on Section 50(3) of the ISS Act 2017, be submandated to subordinate officials. According to the law, establishing selection criteria does not require any advance assessment by the TIB.²⁵

3.2 Approach to professionals entitled to privilege

The ISS Act 2017 contains specific rules regarding the use of investigatory powers against journalists and lawyers.

Section 30(2) of the Act stipulates that if an investigatory power, such as investigation-related interception, is specifically aimed at a journalist and this could lead to the 'acquisition of data relating to the journalist's source', the court of The Hague must grant authorization following a request by the minister. Section 30(3) of the ISS Act 2017 subsequently stipulates that if an investigatory power is used against a lawyer and this use could 'lead to the acquisition of data relating to the confidential communication between a lawyer and his client', the court of The Hague must also grant authorization.²⁶ The ECHR previously defined this prior independent assessment as a requirement in its case law.²⁷

²¹ In particular see: ECHR 19 June 2018, no. 35242/08, ECLI:CE:ECHR:2018:0619JUD003525208 (Centrum för Rättvisa vs. Sweden) and ECHR 13 September 2018, nos. 58170/13, 62322/14 and 24960/15, ECLI:CE:ECHR:2018:0913JUD005817013 (Big Brother Watch and others vs. The United Kingdom). The Big Brother Watch case is now being handled by the Grand Chamber of the European Court of Human Rights and there is a possibility that the judgment of the ECHR will be amended.

²² Section 329 (*Big Brother Watch vs. the United Kingdom*).

²³ Section 344-345 (*Big Brother Watch vs. the United Kingdom*).

²⁴ *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 10.

²⁵ Moreover, this is not a requirement of the ECHR in the *Big Brother Watch* case either (Section 340).

²⁶ In the investigation into the use of filters in investigation-related interception, the assessment framework explains that the inclusion in a positive filter of any characteristics of lawyers and journalists or other selection criteria that inevitably lead to the acquisition of their communication is prohibited unless there is authorization from the court of The Hague. The legal provision in Section 30 of the ISS Act 2017 does not go as far as to exclude any additional acquisition by a negative filter.

²⁷ *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 48. In particular see European Court of Human Rights 22 November 2012, no. 39315/06 (*Telegraaf c.s. vs. State of the Netherlands*) and more recently in the *Big Brother Watch* case in Section 499. In national context, see also Court of the Hague 1 July 2015, ECLI:NL:RBDHA:2015:7436 and Court of Appeal of The Hague 27 October 2015, ECLI:NL:2015:2881.

If it emerges that a phone conversation being listened to contains confidential communication as referred to in Section 30 of the ISS Act 2017, an authorization request must still be made to listen to the conversation.²⁸

3.3 Handling sensitive information

Section 19(3) of the ISS Act 2017 stipulates that the processing of data relating to someone's religious or personal beliefs, race, trade union membership, health and sexuality is not permitted. However, this is countered in the fourth subsection of this section which states that this type of data may only be processed in addition to the processing of other data and only in so far as this is unavoidable for the purpose of data processing.

The use of the word 'unavoidable' indicates that the assessment here is more stringent than the general assessment of necessity of Section 18(1) of the ISS Act 2017.²⁹ Legislative history cites the example that 'the religious or philosophical beliefs of persons are registered in cases where anti-democratic, subversive or anti-militaristic activities are being conducted in which these persons use their religious or philosophical beliefs as an argument for their activities'.³⁰

3.4 Division of positions and roles

Sections 48(4) and 49(5) of the ISS Act 2017 prescribe the division of positions and roles where it concerns investigation-related interception. Article 2 of the AIVD Mandate Decision on Division of Positions and the Defence Mandate Regulation states that the ministers grant the heads of service the mandate and authorization to appoint subordinate officials who may - to the exclusion of others - access data obtained (including substantive data) through the powers described in Sections 48 and 49 of the ISS Act 2017.

As regards the use of the power of selection, the above provisions are only relevant where 'search aimed at selection' is concerned. The ISS Act 2017 does not impose the division of positions when using the power of selection in Section 50(1)(a) of the ISS Act 2017. However, the power of selection is an investigatory power that provides for accessing substantive data from investigation-related interception. This data requires special protection, particularly in connection with the right to confidential correspondence that can be derived from Article 8 of the European Convention on Human Rights.³¹ A separate investigatory power applies to the processing and analysis of metadata aimed at persons and organizations, as the analysis of metadata may entail a serious infringement of the right to privacy.³²

The above implies that a distinction is made between substantive data and metadata, but the legislative history of the ISS Act 2017 does not define the terms 'substantive data' and 'metadata' in more detail. Therefore further implementation in the AIVD and MIVD's policy is required. In specific cases, the actual distinction is made by technical systems.

²⁸ See the extensive CTIVD report no. 52 (2017), Appendix II.

²⁹ *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 34.

³⁰ *Parliamentary Documents II* 2016/17, 34588, no. 18, p. 26.

³¹ See ECHR 3 April 2007, no. 62617/00, Sections 41-42 (*Copland vs. The United Kingdom*) and ECHR 12 January 2016, no. 37138/14, Section 53 (*Szabó and Vissy vs. Hungary*).

³² See most recently ECHR 13 September 2018, nos. 58170/33, 62322/14 and 24960/15, Section 355 (*Big Brother Watch and others vs. the United Kingdom*).

4. 'As targeted as possible'

Based on Article 5 of the Policy Rules of the ISS Act 2017, the use of investigatory powers must be as targeted as possible.³³ This requirement was introduced following the advisory referendum as an additional safeguard when applying investigatory powers.³⁴

In addition to the assessments of necessity, proportionality and subsidiarity, the requirement 'as targeted as possible' is therefore the fourth assessment in the exercise of the investigatory powers of the ISS Act 2017.³⁵

This requirement is essential for the protection of fundamental rights, particularly when investigation-related interception is used. The use of this investigatory power is in fact a serious infringement of the fundamental rights of citizens, including people not directly the subject of the services' focus, because communication conduct is collected and analysed.

Implementation of the requirement 'as targeted as possible' in the context of selection

The explanatory memorandum to the ISS Act 2017 lacks any further implementation of this requirement in the context of the power of selection. The explanatory memorandum to the draft amendment of the ISS Act 2017 does now include further implementation this requirement.³⁶ No further explanation is given either in the previously cited Policy Rules or the explanation to it. It is clear that the requirement of choosing the most targeted approach possible needs substance because the power of selection is an investigatory power. The request for authorization to use an investigatory power must clarify how the requirement to exercise the power in the most targeted way possible will be implemented.³⁷

The use of the power of selection is aimed at a person, organization or topic. The 'selection object' must thus be described as specifically as possible. The use in regard to a person is more targeted than the use in regard to an organization. The use against an organization may be more targeted than against a topic, depending on the circumstances of the case. In previous reports, the CTIVD explained that a request to use an investigatory power in regard to an organization must clearly indicate that there is in fact an organization. The CTIVD distinguishes formal and fluid organizations.³⁸

A formal organization is one that has a more or less permanent structure, for example an institution or company. The request to use an investigatory power against a formal organization must indicate precisely at which category of persons within the organization the investigatory power is aimed.³⁹ This could include the department or officers on which the use is focused.

³³ Policy Rules of the ISS Act 2017, *Parliamentary documents I* 2017/2018, 34588, no. I.

³⁴ *Parliamentary documents II* 2017/18, 34588 no. 70 (letter of 6 April 2018) and explanation to Policy Rules of the ISS Act 2017.

³⁵ See the explanation to Article 5 of the Policy Rules of the ISS Act 2017, *Parliamentary documents I* 2017/2018, 34588, no. I.

³⁶ *Parliamentary Documents II* 2018/19, 35242, no. 3, pp. 10-11: "In their authorization request, the services must as far as reasonably possible (and where applicable) include the requirement 'as targeted as possible' by demarcating the data to be obtained: geographically, by time, by data/traffic type, by object/target, by conduct or otherwise. They must also take into account the intelligence context in which the as yet unknown threat is to be examined, including the stage of the investigation, the necessity to falsify, the time element and realistic technical possibilities."

³⁷ Article 5 of the Policy Rules of the ISS Act 2017, *Parliamentary documents I* 2017/2018, 34588, no. I.

³⁸ See for example CTIVD report no. 40 (2014).

³⁹ See CTIVD report no. 46 (2016). 15.

By contrast, fluid organizations are characterized by a more informal structure, for example followers of the same ideological movement who have united.⁴⁰ Particularly in the case of more fluid organizations, the substantiation must argue expressly that the cohesion between the members of the organization is such that it constitutes an organization. The following criteria may be used to do so: 'cooperative partnership', 'permanent nature', 'joint objective' and 'awareness' of that joint objective for the members of the organization.⁴¹ Furthermore it is important to clearly substantiate the circumstances under which persons are seen as members of the organization and why certain echelons of an organization are relevant to the investigation.⁴²

Implementation of the requirement to make the selection as targeted as possible is also important when handling selection criteria, such as telephone numbers and IP addresses. Selection criteria relate to, for example, technical characteristics of people, organizations and keywords related to a specified topic. It is important that the origin or source of the selection criterion is traceable and that a link is made with the person, organization or topic against which selection is aimed. For example, when selection criteria such as keywords or geographical information are used that may generate a great deal of additional data (causing 'collateral intrusion'), additional substantiation is required to explain how this unintentionally gathered information will be limited as much as possible. Another contributing factor to the implementation of this requirement is the authorization procedure to use, remove and supplement the selection criteria.

The following three elements must therefore be taken into account when implementing the requirement 'as targeted as possible' in the context of selection:

1. The minister involved grants authorization for the selection of data regarding a person, organization or topic. The services must substantiate why the selection cannot be more targeted and must describe the 'object' of the selection as specifically as possible. That description must include, among other things, the identity of the person or organization or an explanation of the topic, in conjunction with the reason this object is significant to the investigation. The TIB subsequently conducts its lawfulness assessment;
2. The substantiation must show that the selection criteria used can be linked to a person, organization or topic. A link which meets this requirement, for example, is a telephone number or email address belonging to a certain person;
3. The services must substantiate the choice for a certain type of selection criterion. In connection with this, the origin/source of the selection criterion must be disclosed as well as the reason to use technical features or broad selection criteria.

⁴⁰ See CTIVD report no. 40 (2014), report no. 51 (2016), report no. 53 (2017).

⁴¹ See CTIVD report no. 24 (2010), pp. 19-20, report no. 40 (2014), p. 10 and report no. 51 (2016), p. 7.

⁴² CTIVD report no. 34 (2013), pp. 9-10 and report no. 51 (2016), p. 8.

5. Data reduction in investigation-related interception

The parliamentary debate of the ISS Act 2017 clearly showed that investigation-related interception requires a continuous process of data reduction.⁴³ The reduction of data in investigation-related interception and selection follows from Section 48(5) of the ISS Act 2017, which stipulates that data obtained through investigation-related interception must be assessed for relevance. When certain data, after selection, is assessed as non-relevant, it must be destroyed immediately. This data is then irreversibly deleted from the systems.

Data is relevant if it has significance for the investigation for which it has been obtained, or for any other ongoing investigation that falls within the tasks as referred to in Section 8(2)(a) and (d) or Section 10(2)(a), (c) and (e) of the ISS Act 2017.⁴⁴ When data is assessed for relevance, it must be examined in substance “whether the data contributes in a positive sense to the investigation or whether that data could provide a negative response to certain questions, disprove hypotheses or otherwise be of crucial importance”.⁴⁵ In that sense, therefore, the law provides a relatively wide scope to interpret the term ‘relevance’.

If data is selected with the help of investigation-related interception by using the power of selection, it does not automatically imply that this data is relevant. The explanatory memorandum states that the selected data must first be reviewed for relevance before it can be used in the investigation.⁴⁶ Selection of data must therefore be followed by a substantive review for relevance.

Retention period for data obtained by investigation-related interception

Any data obtained by investigation-related interception must be assessed for relevance within a certain timeframe. This is called the ‘retention period’. Data obtained by investigation-related interception falls into one of the three retention periods below:⁴⁷

1. The retention period of data from investigation-related interception, not being cable interception, is three years (see Section 48(5) of the ISS Act 2017). This term may not be extended.
2. The retention period of data from cable interception⁴⁸ is one year (Article 4 of the Policy Rules on the ISS Act 2017). This retention period can be extended twice for the period of one year. An extension of the retention period requires ministerial authorization.
3. The retention period of encrypted data is three years (Section 48(6) of the ISS Act 2017). As long as that data has not been decrypted, the term may be extended each time by three years. This requires the authorization of the minister.

The retention period of data from investigation-related interception commences when the data is obtained and continues as described above, regardless of whether the data is selected. Regardless of the retention period, any data that has not been assessed for relevance must be destroyed immediately once the retention period expires.

⁴³ *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 111.

⁴⁴ See Section 48(5) of the ISS Act 2017.

⁴⁵ *Parliamentary Documents II* 2016/17, 34588, no. 18, p. 32.

⁴⁶ *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 107: “Selection of data is carried out with a view to learning the content of the selected data and to subsequently review it for relevance to the investigation for the purpose of which the selection took place. Information deemed relevant from the data examined is then included in the investigation in question and is made available for other investigations by the service as it has been determined that it concerns data relevant to national security.”

⁴⁷ The retention period for data obtained by other investigatory powers differs from the retention period of data in the system of investigation-related interception. The retention period of data from other investigatory powers is generally one year. This retention period may be extended only once by a maximum of six months with authorization of the head of the relevant service.

⁴⁸ Please note: during the period investigated no cable interception took place.

6. Duty of care

Section 24 of the ISS Act 2017 stipulates that the head of the AIVD or the MIVD has a duty of care to safeguard lawful data processing. One new element compared with the former ISS Act 2002 is the duty to promote the quality of the data processing. The duty of care requires more from the AIVD and the MIVD than simply implementing the legal requirements imposed on them for collecting, analysing and using data.⁴⁹ The duty of care means that both services continuously monitor how they process data and ensure that data processing is and remains in accordance with the applicable legal requirements (*compliance*). This ongoing monitoring requires the services to use a number of instruments that provide a central overview of the functioning of processes and data processing systems and that allow them to identify risks and take measures in time.


In the context of the power of selection, the duty of care is specifically expressed in the duty that the services have to validate and check that selection criteria are used lawfully when implementing the power of selection. For example, selection criteria must relate to technical features that are used by a person or organization and it must be possible to link keywords to topics. The next step is that the CTIVD is enabled to check the systems used to implement the duty of care.

⁴⁹ See also CTIVD report no. 59 (2018), p. 7.

7. The CTIVD assessment framework for selection

Based on the assessment framework, the following requirements exist for the exercise of the investigatory power of selection which is reviewed in this report:

1. **Authorization** by the Minister of the Interior and Kingdom Relations or the Minister of Defence and the TIB to use the **power of selection** for the purpose of investigation assignments.
2. Application of the **general requirements** of an assessment of necessity, proportionality and subsidiarity in the requests to use the investigatory power of selection.
3. The power of selection must be conducted in **as targeted a way as possible**.
4. The application of **data reduction** in the use of the power of selection.
5. Compliance with the **duty of care** in the use of the power of selection.



Oranjestraat 15, 2514 JB The Hague
P.O.Box 85556, 2508 CG The Hague

T 070 315 58 20 | **F** 070 381 71 68
E info@ctivd.nl | www.ctivd.nl