

Appendix B

On the application of filters in investigation-related interception by the AIVD and the MIVD

CTIVD no 63

(adopted on 17 July 2019)



Review Committee
on the Intelligence and
Security Services

Structure of the report

This report has the following components:

The review report

Appendix A: Elaboration of the review report

Appendix B: Assessment framework

Appendix C: Definitions

This report has a classified appendix.

Given the technical complexity of the subject matter, the CTIVD has opted to divide the report into a review report that includes the main findings and a separate appendix (A) that discusses the findings in greater detail. Appendix A should be read to obtain a deeper understanding of the subject matter. The review report and appendix A have been written to be read as separate documents and consequently some overlap cannot be avoided. The full assessment framework has been incorporated in appendix B. Appendix C contains the definitions.

CTIVD no 63

APPENDIX B: REVIEW REPORT

On the application of filters in
investigation-related interception
by the AIVD and the MIVD

Table of contents

B.1. Introduction	5
B.2. The three-stage model of investigation-related interception	6
2.1 Interception	6
2.2 Optimization of the interception process	8
a) Search aimed at interception	8
b) Search aimed at selection	8
2.3 Analysis of data	9
B.3. Filters	10
3.1 What is filtering?	10
3.2 Filtering in the three-stage model	10
a) Selecting communication media	10
b) Selecting data streams	11
c) Subsequent filtering and the storage of intercepted data	11
B.4. Requirements for the application of filters in the context of investigation-related interception	13
4.1 Tasks and investigation assignments	13
4.2 As targeted as possible	13
4.3 Data reduction	15
4.4 Cable interception	15
4.5 Other influences on the application of the filters	16
4.6 Internal control and effective review	18

APPENDIX B: REVIEW REPORT

On the application of filters in
investigation-related interception
by the AIVD and the MIVD

B.1. Introduction

This in-depth investigation into the application of filters in the deployment of investigation-related interception stems from the results of the progress report which the CTIVD presented in December 2018. In that report, the CTIVD comes to the conclusion that although the services use filters in the interception of satellite and radio communications in practice, this practice is not described in any policy, work processes or instructions. The CTIVD indicated that among other things these observations lead to the conclusion that the risk of unlawful conduct by the AIVD and the MIVD is high.

This (short-term) in-depth investigation will help to provide a picture of how the services apply filters and how a lawfulness assessment can subsequently be conducted, based on this assessment framework. This in-depth investigation will therefore assess whether the detected risks actually manifested themselves. This investigation not only examines the interception of satellite and radio communications but also the preparations for cable interception, a new investigatory power of bulk interception on the cable which provoked much public debate in the run up to the introduction of the Intelligence and Security Services Act (ISS Act 2017). The method of filtering may differ depending on the interception technology; particulars will therefore be specifically named.

The need for a lawfulness assessment relating to filtering not only ensues from the aforementioned statements but also from legislative history and case law. In legislative history, filters are quoted as being an instrument to mitigate any infringement of fundamental rights and freedoms by the use of investigation-related interception. In turn, the *Big Brother Watch* ruling of the European Court of Human Rights underlines the necessity of effective, independent oversight of the application of filters in the process of bulk interception.

The assessment framework for the investigation into the application of filters in investigation-related interception is structured as follows. Chapter 2 describes the process of investigation-related interception. Chapter 3 explains how filters are applied in the interception process. Finally, chapter 4 formulates the requirements set to the filters, as these follow for the AIVD and the MIVD from the ISS Act 2017 (including legislative history) and case law.

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

This chapter 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 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 of selection (Section 49(2) in conjunction with Section 50(1)(a) of the ISS Act 2017). This is further illustrated by the fact that the services work with five stages, not three, in their policy and practice.

To sum up, the three stages are (1) interception of communication, (2) optimization of the interception process and (3) 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 and Security Services Order (hereinafter: Integrated Order). The Integrated Order is adopted by the Prime Minister, the Minister of General Affairs, the Minister of the Interior and Kingdom Relations and the Minister of Defence and forms the basis for the investigation assignments by the services. 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 task, 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 concern 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 tasks relating to intelligence and security.⁵

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

² *Parliamentary Documents II 2016/17*, 34588, no. 3, pp. 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).

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 is itself laid down in Section 48 of the ISS Act 2017. The investigatory power also entails decrypting 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.

The contents of the communication may only be checked during the technical analysis for the correct rendition of reception (i.e. a quality control), for example to check 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 chapter 4 for further details).⁸

The application for interception must contain a characterization of the telecommunication or data transfer using a computerized device or system in respect of which the investigatory power must 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.⁹ 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.¹⁰ The services select those data streams which are reasonably expected to be relevant to answering ongoing investigation assignments by the services.¹¹

Based on Section 48(3) of the ISS Act 2017, additional substantiation is required if the interception of only metadata 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 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.

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.

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

⁸ Policy Rules of the ISS Act 2017.

⁹ *Parliamentary Documents II* 2016/17, 34588, no. 3, pp. 99.

¹⁰ Section 52 of the ISS Act 2017 (information) and Section 53 of the ISS Act 2017 (assistance).

¹¹ *Parliamentary Documents II* 2016/17, 34588, no. 3, pp. 110.

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).¹² In 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.

a) 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, which 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.¹³

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 on a year-by-year basis. As noted in the introduction to this chapter, in practice this concerns an order combining Sections 48 and 49(1) of the ISS Act 2017.

b) 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 and organizations that are being investigated by the services. The resulting intercepted telecommunication can then be examined for selection criteria - established on the basis of Section 50(3) - 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.¹⁴

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.¹⁵ In other words, the investigatory power makes it possible to identify or pinpoint potential targets as well.¹⁶ 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 2017.¹⁷

¹² *Parliamentary Documents II* 2016/17, 34588, no. 3, pp. 95.

¹³ *Parliamentary Documents II* 2016/17, 34588, no. 3, pp. 104.

¹⁴ *Parliamentary Documents II* 2016/17, 34588, no. 3, pp. 106. See also CTIVD report no. 28 (2011), p. 43.

¹⁵ *Parliamentary Documents II* 2016/17, 34588, no. 3, pp. 107.

¹⁶ *Parliamentary Documents II* 2016/17, 34588, no. 3, pp. 106. See also CTIVD report no. 28 (2011), p. 44.

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

Under Section 49 of the ISS Act 2017, the use of the 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 civil servants may consult the stored content from investigation-related interception (division of positions and roles). 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.

2.3 Analysis of data

The third stage of the system of investigation-related interception is the selection of relevant communication with a view to learning the *content* of the selected data.¹⁸ The investigatory power to apply selection to the intercepted data is laid down in Section 50(1)(a) of the ISS Act 2017.

During this third stage of investigation-related interception, metadata analysis takes place, which can be focused on identifying persons or organizations. This investigation activity is regulated by the investigatory power of automated data analysis in Section 50(1)(b) of the ISS Act 2017 and Section 50(4) where it concerns metadata obtained through investigation-related interception and the analysis is aimed at identifying persons or organizations.

¹⁸ *Parliamentary Documents II* 2016/17, 34588, no. 3, pp. 107.

B.3. Filters

This chapter looks in more detail at what constitutes a filter and how the application of filters fits in the three-stage model explained in the previous chapter.

3.1 What is filtering?

In this investigation into the application of filters during the process of investigation-related interception, a filter is defined as the means that determines whether or not to store data (for operational investigations) from the communication media selected for interception. Filtering is the process that determines the distinction between the available data streams (communication) on the communication media selected by the services and the data from those streams that are ultimately stored for the intelligence process.

Filtering is therefore a reduction in the acquisition of raw (bulk) communication and should be seen as part of the requirement to reduce data. The filtering process starts the moment a data stream is selected, whereby the prior selection of the communication medium can indeed contribute to the interception being targeted but does not form part of the filtering process. The process ends as soon as data is stored for the subsequent intelligence process.

As a consequence of the above definition, selecting, for example, a certain satellite (the medium) to be intercepted from the total number of satellites does not constitute filtering. Filtering only starts when the satellite to be intercepted has actually been designated and when a selection must be made from the communication streams available on that satellite connection. Filtering ends when the data intended for potential use in the operational process has been stored in the databases of one of the services. The various choices to be made are discussed in the following section.

3.2 Filtering in the three-stage model

Given the definition and description of the filtering process above it is clear that the application of filters takes place in the first stage of the three-stage model: the interception of communication. It is important in this respect to point out that this interception stage consists of three parts: a) the selection of the communication media to be intercepted, b) the selection and interception of the data streams and c) subsequent filtering and storage of the intercepted data. In the implementation of these parts, the (outcomes of the) processes in the second and third stage – in particular the search aimed at interception – may play a role.

a) Selecting communication media

The acquisition stage primarily involves the choice of the communication media at which to aim the interception power.¹⁹ As regards interception of the cable, this takes place at a so-called access location, selected based on the current threat assessment. The services must select from the available fibre optic cables (also referred to as fibres) on the access location. Ether communication can be divided into data streams through communication media such as satellites and high frequency radio waves. These are intercepted in Burum and Eibergen by picking up signals using aerial dishes and antennae.²⁰

¹⁹ *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 118.

²⁰ CTIVD report no. 38 (5 February 2014), p. 12.

b) Selecting data streams

Each fibre of a cable consists of a further dozen channels. In the case of interception of satellites and HF radio waves, the data flows are spread over a range of frequencies or frequency bands. In satellite interception these are referred to as links. The services select those data streams (and therefore channels and links) 'which are reasonably expected to be relevant to answering ongoing investigations by the services'.²¹

Selecting certain data streams firstly arises from the knowledge the services already have, for example in the form of certain technical characteristics (including leads). Searching for the right channels or frequencies also takes place based on search aimed at interception, the purpose of which is to establish if the intended information is in fact being intercepted. The services look at protocols, frequencies, language and also the quality of the interception.²² In the context of search aimed at interception, the services routinely use *snapshotting* (a momentary recording of content and metadata), which means that they can investigate whether the channels or links contain relevant information. Selecting specific data streams to be intercepted can change on a daily basis,²³ making the selection of channels or links (within fibres or satellites respectively) a form of filtering.

Lastly, the actual interception of communication is done by picking up the signal of the required data streams (possibly having copied it first). In those cases, the services do not always know who will communicate through that channel and it is likely that data will be intercepted from people and organizations that are not, nor will be, the subject of investigation.²⁴

c) Subsequent filtering and the storage of intercepted data

Not all intercepted data streams are stored to be processed further. During and shortly after the actual interception, the data is filtered further. To understand this properly it is important to distinguish between negative and positive filters.²⁵ A positive filter generally concerns the content of communication, whereas a negative filter is concerned with metadata.²⁶ A negative filter defines data that should not be stored. Examples are data streams from video services such as Netflix and YouTube. Data excluded based on a negative filter does not end up with the services, because it has been 'deflected'.²⁷ All metadata that does pass through this filter is stored.

This also applies to content received through positive filtering. In short, a positive filter defines which data should be stored, for example based on a certain technical characteristic (such as a telephone number). The explanatory memorandum states in this respect: "In practice only content is stored when it is clear that this is necessary in stages 2 and 3 of the interception process and that it falls within specific investigation assignments. Firstly based on location data, specific encryption, country codes in telephony, cyber characteristics or a specific communication application (stage 2). That does not mean that the content is stored for long periods of time. Depending on the circumstances, this may be a week or a few months. In addition, the content is stored based on the fact that it meets the selection criteria (stage 3), such as numbers."²⁸

²¹ *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 110.

²² *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 104.

²³ CTIVD report no. 28 (23 August 2011), p. 28.

²⁴ CTIVD report no. 38 (5 February 2014), p. 12 ff.

²⁵ *Parliamentary Documents II* 2016/17, 34588, no. 18, pp. 71 and 72.

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

²⁷ *Parliamentary Documents II* 2016/17, 34588, no. 18, pp. 18. (This comment was made in the context of cable interception).

²⁸ *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 110. (This explanation refers to both cable and satellite interception)

Filters can also be combined to filter 'intelligently', for example: "Remove all voice traffic originating from a satellite, except from a certain region."²⁹ Data that has not passed through the various filters is not stored and cannot be retrieved at a later time.³⁰ Generally it can be said that 'determining the specific data stream, combined with negative and positive filtering as well as with the ultimate selection of data, protects against any large-scale infringement of the privacy of persons who are not the subject of investigation'.³¹

²⁹ *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 98.

³⁰ Appendix to *Parliamentary Documents II* 2017/18, 34588, no. 69, p. 3.

³¹ *Parliamentary Documents II* 2016/17, 34 588, no. E, p. 2.

B.4. Requirements for the application of filters in the context of investigation-related interception

Although the word ‘filter’ is not mentioned in the legislative text of the ISS Act 2017, the obligation to filter does exist. This situation also presented itself in the ISS Act 2002, where the CTIVD concluded in report 38 that the application of filters should be seen as part of the power of untargeted interception, which at the time was laid down in Sections 26 and 27 of the ISS Act 2002.³² There is no reason to depart from this view. Moreover, this interpretation is supported by the legislative history of the ISS Act 2017, not least because this Act emphasizes the obligation to reduce data and to apply investigatory powers in as targeted a way as possible. This chapter formulates the requirements set to the filters, as these can be derived for the AIVD and the MIVD from the ISS Act 2017 (including legislative history) and case law.

4.1 Tasks and investigation assignments

The tasks of the AIVD and the MIVD are described in Sections 8 and 10 of the ISS Act 2017 respectively. The services perform their tasks in the interest of national security. In order to perform their tasks, the services are able to use various investigatory powers. That includes investigatory powers. Section 28(1) of the ISS Act 2017 specifies that the use of investigatory powers is only permitted for legal intelligence and security tasks. In the context of national security, the services may use investigatory powers for a limited number of tasks, i.e. the A and D tasks of the AIVD and the A, C and E tasks of the MIVD.

By stating that the investigation into communication needs to be investigation-related, an unmistakeable connection is made with the Integrated Order. The services’ investigation assignments are based on the Integrated Order. In addition, there may be urgent investigation assignments that are also approved at ministerial level.

Investigation-related interception will therefore always have to take place in the context of previously formulated and approved investigation assignments. This sets a limit to the use of the power and influences the setting of the filters because this is a way to keep the interception within its limitations.

Interim conclusion/specific requirement: Investigation-related interception must be conducted within the context of legal intelligence and security tasks and the investigation assignments of the services approved at ministerial level, ensuing from the Integrated Intelligence and Security Services Order.

4.2 As targeted as possible

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

³² CTIVD report no. 38 (5 February 2014), p. 14.

³³ Policy Rules of the ISS Act 2017.

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

In addition to the assessments of necessity, proportionality and subsidiarity, the requirement of interception being as targeted as possible is therefore the fourth assessment when exercising the investigatory powers of the ISS Act 2017.³⁵ The requirement of as targeted as possible interception means that the services limit to a minimum any information not strictly necessary for the investigation, given the technical and operational circumstances of the case.³⁶

This certainly applies to the power of investigation-related interception, since legislative history records the following: "Investigation-related interception is set up to be as targeted as possible. The law does not allow the intentional wider collection of data with a view to later use." And in another section: "The principle in investigation-related interception is that the services work in as targeted and effective a way as possible, with as little infringement of citizens' privacy as possible."³⁷

Section 32 of the ISS Act 2017 stipulates that the power of investigation-related interception may only be used following authorization by the minister and a lawfulness assessment by the TIB. Section 29(2) of the ISS Act 2017 specifies the requirements set to the request for authorization, such as an indication of the investigatory power to be used, a description of the investigation and the reason to use the investigatory power. In addition to these requirements, Article 5 of the Policy Rules of the ISS Act 2017 stipulates that the request for authorization must expressly include how the target requirement will be implemented in the use of the requested investigatory power. The authorization request must also clarify how the application of filters, as part of the power of interception, will result in that use being as targeted as possible. Subsequently this should also be documented in the services' policy and work instructions.

In addition to the requirements of Section 29 of the ISS Act 2017, Section 48(3) of that same Act further requires that any authorization request for the use of investigation-related interception, where applicable, must include the reason why the use of that investigatory power should also relate to the contents (in addition to the metadata) of telecommunication or the data transfer using a computerized device or system. A second requirement is that a characterization is given of the types of telecommunication or data transfer.

Interim conclusion/specific requirement: The use and implementation of the power of investigation-related interception must be 'as targeted as possible' in addition to being necessary, proportional and subsidiary. The authorization request to the minister and the TIB as well as the policy and work instructions laid down must clarify how the application of filters will result in the use being as targeted as possible. Where the request concerns the interception of content, it must contain a substantiation. In addition, the request must in all cases include a characterization of the communication to be intercepted.

³⁵ See the explanation to Article 5 of the Policy Rules of the ISS Act 2017.

³⁶ Response by TIB to the draft amendment of the ISS Act 2017, p. 2.

³⁷ *Parliamentary Documents II* 2016/17, 34588, no. 18, pp. 72 and *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 95.

4.3 Data reduction

Filters are seen in legislative history as the principal way of complying with the requirements of data reduction.³⁸ The explanatory memorandum states as follows: “The result in particular of applying filters in interception is that the bulk of intercepted data is reduced to that data that could be relevant for further investigation.” In this way, ‘reducing data as quickly and as much as possible in the first stages of the interception is an important part of the interception process and a requirement of the draft amendment’.³⁹

It may be concluded from the above that filtering should be seen as part of the obligation to reduce data in the context of the interception power. The process plays an important role in separating relevant and potentially relevant data from non-relevant data. This occurs by examining the data stream to be intercepted for characteristics that can be related to current investigation assignments or investigations. This is mainly done based on geographical characteristics of traffic or on the presence of selection criteria (see below under 4.5.3).

And lastly, Section 48(5) of the ISS Act 2017 stipulates that any data established not to be relevant for the investigation or any other ongoing investigation that falls under the tasks referred to in Section 4.1 should be destroyed immediately.

Interim conclusion/specific requirement: Filters are to reduce the intercepted communication to only that information that are or might be relevant to the services’ ongoing investigations. Non-relevant data must be destroyed immediately (data reduction).

4.4 Cable interception

Sections of legislative history reiterate that in the case of investigation-related interception on the cable, a positive filter requires the authorization of the minister and the TIB. In addition, it is stipulated that data is filtered positively based on selection criteria such as numbers.⁴⁰ However, this is not a requirement in the law itself, which may cause some confusion. What’s more, the law allows the establishment of selection criteria to be mandated, making it less obvious to request ministerial authorization or a lawfulness assessment from the TIB for the establishment of individual criteria in the positive filter. Nonetheless, it may be assumed that only those criteria may be included in the positive filter that can be traced to an authorized warrant for selection (see Section 50(2) of the ISS Act 2017) or a warrant for search aimed at selection (Section 49(2) of the ISS Act 2017).⁴¹

As regards cable interception, there were specific comments during the legislative procedure of the ISS Act 2017 about the reduction of the data volume. By applying filters in the first stage of the interception process, 95 to 98 percent of the intercepted data is ultimately not expected to be stored.⁴² In addition, the Minister of the Interior and Kingdom Relations and the Minister of Defence have stated that the

³⁸ Section 27(1) of the Act contains a general requirement to examine any data obtained through investigatory powers as soon as possible for relevance. However, in the case of investigation-related interception, a general obligation to filter does not follow because this provision of Section 48(5) was not declared applicable to data from investigation-related interception. According to that same subsection, this data may be stored for no more than three years. Furthermore, if it is established that the data is no longer relevant for the investigation or other ongoing investigations, it should be destroyed immediately.

³⁹ *Parliamentary Documents II* 2016/17, 34588, no. 18, pp. 71.

⁴⁰ *Parliamentary Documents II* 2016/17, 34588, no. 18, pp. 18 and Appendix to *Parliamentary Documents II* 2017/18, 34588, no. 69, p. 3.

⁴¹ Nor can it be ruled out that a (broadly defined) positive filter is used in the context of search aimed at interception (Section 49(1)). This concerns short-term recordings.

⁴² *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 111.

‘probability of traffic originating from and destined for the Netherlands being intercepted is practically nil’, except in the context of cyber defence.⁴³ These commitments can only be realized by using filters, which is why they are relevant to this investigation.

Interim conclusion/specific requirement: In the case of cable interception, a positive filter, aimed at storing content, may only consist of the criteria in the context of an authorized warrant for search aimed at selection. The application of filtering must also show that the services pay heed to the expectation that 95 to 98 percent of the volume of intercepted data is ultimately not stored and that the probability of traffic originating from and destined for the Netherlands (domestic traffic) being intercepted is practically nil, except in the context of cyber defence.

4.5 Other influences on the application of the filters

4.5.1 Professionals entitled to privilege

The law contains specific rules regarding the use of investigatory powers against journalists and lawyers. Section 30(2) 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. Subsection 3 subsequently stipulates that if the use of 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 must also grant authorization.

Section 27(2) of the ISS Act 2017 also applies to use of investigation-related interception and contains the obligation to immediately destroy any data if it foreseeably concerns the confidential communication between a lawyer and his client. One exception to this rule is the situation which requires further processing of data for the investigation in the context of which the data has been obtained and in which the court of The Hague has granted authorization. The explanatory memorandum clarifies this section further by stating that it pertains to the situation in which the communication between lawyer and client is obtained additionally (as ‘bycatch’) when using an investigatory power against another party. The conclusion of the explanatory memorandum is that it is undesirable to exclude this type of data in advance.⁴⁴

It follows from the above that the filters should be set in such a way that no data is obtained, other than additionally, that relates to confidential communication between a lawyer and his client or to the source of a journalist. 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 the court of The Hague has granted authorization. This requirement does not go as far as to exclude any additional acquisition by a negative filter.

Interim conclusion/specific requirement: The services should set the positive filter in such a way that no data is obtained that relates to confidential communication between a lawyer and his client or to the source of a journalist unless authorization has been granted by the court of The Hague. This requirement does not go as far as to exclude the data or metadata of lawyers or journalists by a negative filter.

⁴³ *Parliamentary Documents II* 2017/18, 34 588, no. G, p. 3.

⁴⁴ *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 42.

4.5.2 Special personal data

Another provision that could influence the application of filters is Section 19(3), which stipulates that the processing of data relating to someone's religious or personal beliefs, race, trade union membership, health and sexuality must not take place. 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 2017.⁴⁵ This requirement, combined with the condition that data is only processed in addition to the processing of other data, forms a 'double lock'. Legislative history cites for 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'.⁴⁶

This dovetails with the above reasoning in the explanatory memorandum relating to lawyers, where it states that it is undesirable to exclude in advance certain data from being intercepted. Indeed, there is no obligation to filter this out with a negative filter. Including criteria in a positive filter that lead inevitably and foreseeably to the acquisition of special personal data, without this being inevitable, is not permitted.

Interim conclusion/specific requirement: Including criteria in a positive filter that lead inevitably and foreseeably to the acquisition of special personal data (data relating to someone's religious or philosophical beliefs, race, trade union membership, health and sexuality) is not permitted, unless this occurs in addition to the processing of other data and in so far as this is unavoidable for the purpose of the data processing.

4.5.3 Selection criteria

In view of the fact that selection criteria are a determining factor to the settings of positive filters, the relevant regulation is briefly discussed. The power of selection requires the authorization of the minister and the TIB according to Sections 50(2) and 32(2). The authorization to establish selection criteria in Section 50(3) lies in principle with the minister but may be mandated to the head of the relevant service. Further mandating to subordinate officials is possible. That means that the mandated official has an important duty to safeguard the correct setting of positive filters.

In addition, positive filters may be adjusted in connection with the provision of technical support, i.e. selecting data for (foreign) partner services.⁴⁷ This form of support is reflected in Section 89(4) of the ISS Act 2017. The power to provide technical or other forms of support is laid down in that section, which requires a prior written request from the relevant foreign service. Support is provided in the context of the foreign service's interests, provided that these are compatible with the interests of the Dutch services and that the performance of tasks does not prevent the provision of support. Nor may the support result in the foreign service independently collecting data in the Netherlands.

4.5.4 Information from communication service providers

Based on Section 52, the services are authorized to approach communication service providers with a request to collect data, which enables them to map out the 'communication landscape'.⁴⁸ This is primarily important to be able to select the access location for cable interception, taking into account the requirement to intercept in as targeted a way as possible. In that way, this information may have an effect on the lawful setting of filters.

⁴⁵ *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 34.

⁴⁶ *Parliamentary Documents II* 2016/17, 34588, no. 18, pp. 26.

⁴⁷ CTIVD report no. 38 (5 February 2014), p. 34 ff.

⁴⁸ *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 97.

4.6 Internal control and effective review

The duty of care of Section 24 of the ISS Act 2017 to ensure data is processed lawfully is a crucial safeguard, both for the protection of data and for subsequent review. One new element compared with the former ISS Act 2002 is the duty to promote the quality of the data processing. This element was included in the ISS Act 2017 because the services' data processing is becoming increasingly automated. The duty of care also creates safeguards in relation to the legislation's independence of technology. The duty of care clearly requires more from the AIVD and the MIVD than simply implementing the legal requirements for collecting, analysing and using data.⁴⁹


In specific terms, the duty of care means that the services have ongoing control over how they process data and that they ensure that this data processing is and continues to be in compliance with the legal requirements (compliance). Continuously being in control requires the services to use a number of instruments that provide (central) overview of the functioning of processes and systems of data processing and that enable them to identify risks and take measures promptly. Without these instruments, without a clear structure for the duty of care, it is not possible to exercise sufficient internal control over the data processing and any effective external review is out of the question.

As regards filters, the Big Brother Watch ruling of the European Court of Human Rights stipulates that independent oversight of the search and selection criteria used to filter intercepted communication, is important.⁵⁰ This ruling has been brought before the Grand Chamber of the European Court of Human Rights, which is why the conclusions contained in it are not yet definitive.

Interim conclusion/specific requirement: The services have a duty of care to exercise internal control on the functioning of the filters and their lawful application, in order to allow effective external review of the process of filtering.

⁴⁹ CTIVD report no. 59 (27 November 2018), p. 7.

⁵⁰ European Court of Human Rights 13 September 2018, nos. 58170/13, 62322/14 and 24960/15, ECLI:2018:0913JUD005817013, paragraphs 340 and 347.



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