Appendix I: Assessment framework

to the review report about the use of cable interception by the AIVD and the MIVD

The snapshot phase

CTIVD no. 75

Adopted on 26 January 2022

Review Committee
on the Intelligence and
Security Services

Review Committee
on the Intelligence
and Security Services

CTIVD no. 75

APPENDIX I: ASSESSMENT FRAMEWORK

to the review report about the use of cable interception by the AIVD and the MIVD

Contents

CTIVD no. 75

APPENDIX I: ASSESSMENT FRAMEWORK

to the review report about the use of cable interception by the AIVD and the MIVD

1. Introduction

In this review report, the Review Committee on the Intelligence and Security Services (hereinafter: CTIVD) answers the following question: in the period from 1 May 2018 to 31 March 2021, did the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD) (hereinafter: the services) lawfully operationalise an access location and lawfully implement cable interception in the snapshot phase? In this period, the services made it possible to intercept the cable and also actually intercepted the cable. Cable interception was conducted in the form of snapshotting, which involves the short, integral interception of data streams. After interception, the relevance of the data stored for one or more investigation assignments of the services is assessed on the basis of technical and substantive characteristics. In the investigation period, safeguards are used to limit the infringement of the fundamental rights of citizens.

The ISS Act 2017 does not provide any specific investigatory power for snapshotting. In practice, the services use snapshotting based on Section 48 (interception) of the ISS Act 2017. Data is investigated based on Section 49(1) (search aimed at interception). of the ISS Act 2017.

Cable interception

Cable interception means that the AIVD and the MIVD can intercept cable-bound communication (such as internet traffic) in large quantities without this interception being aimed at a specific target, such as a person or organisation. However, it must be possible to relate the interception to one or more investigation assignments of the services, which, in turn, arise from the Integrated Intelligence and Security Services Order. In this inherently untargeted form of interception, the services intercept (on a large scale) the data of persons who are not the subject of their investigation, nor ever will be. Large data collections in which the (vast) majority of data are about persons who are not the subject of investigation are called bulk data sets. Therefore, this form of interception is referred to as a bulk interception. In this report, the CTIVD wants to avoid any confusion between the terms 'investigation-related interception', 'bulk interception' and 'untargeted interception' on the cable and, therefore, uses the term 'cable interception' as much as possible in this report.

Assessment framework

This assessment framework discusses the legal requirements applicable to both the operationalisation of the access location and the implementation of interception.

They form the assessment framework for the in-depth investigation into the use of cable interception by the AIVD and the MIVD.[1] This framework is based on the ISS Act 2017 and on the policy rules, parliamentary history, any relevant case law, previous review reports and the recommendations that the Ministers of the Interior and Kingdom Relations (hereinafter: BZK) and Defence have adopted in this connection.

The assessment framework is structured as follows. Chapter 2 discusses the general provisions of the ISS Act 2017 that are relevant to data collection and data processing. Chapter 3 discusses the legal framework that applies to the operationalisation of the access location. Chapter 4 then discusses the frameworks for the implementation of interception. The assessment framework concludes in chapter 5, which summarises the legal requirements.

References to legislation

In this assessment framework, the CTIVD frequently refers to legislative Section numbers. Unless explicitly indicated otherwise, the CTIVD is referring to the ISS Act 2017.

1 This assessment framework pertains to the initial phase of the interception process (Sections 48, 49(1), 52 and 53 of the ISS Act 2017). See Section 4 of this assessment framework for an explanation of the various phases. As regards the legal provisions in respect of the next phases of the interception process, reference is made to the assessment frameworks for two CTIVD reports; report no. 63 about the use of filters in investigation-related interception by the AIVD and the MIVD and report no. 64 about the use of the special investigatory power of selection during investigation-related interception by the AIVD and the MIVD. These reports pertain to the investigation-related interception of satellite and radio communications.

2. General provisions, ISS Act 2017

The general requirements for data processing apply to the processing of data for the performance of the tasks of the services. The general provisions for data processing have been laid down in Sections 17 to 24. 'Processing' is a broad concept. The processing of data includes the collection, recording, organising, consulting and provision of data.[2] Added to this, the use of general and special in vestigatory powers is subject to general provisions that apply to the collection of data (Sections 25 to 31 inclusive). In this chapter, just some of the general provisions are discussed that apply to the collection and processing of data. It would be too much to discuss all of them.

The CTIVD has not investigated the substantiation of the requests for authorisation because the Investigatory Powers Commission (TIB) has already assessed the lawfulness of these requests. This means that the CTIVD has not re-assessed the general requirements of necessity, proportionality and subsidiarity. However, the same does not apply to the specificity requirement. The CTIVD included this in its assessment because the Ministers of BZK and Defence explicitly asked it to report on this.[3]

Purpose limitation and necessity (Section 18)

Data may only be processed for a certain purpose and only if necessary for the performance of the tasks of the services. In the ISS Act 2017, these are referred to as purpose limitation and the necessity requirement respectively.[4] The purpose of data processing must also be recorded in the substantiation of an authorisation request to use an investigatory power.[5] The services must expect it to be possible to achieve this purpose by processing the data and must be able to substantiate this expectation.[6] In the authorisation request, the services must substantiate why use of the special investigatory power is necessary and explicitly consider proportionality and subsidiarity.[7]

Duty of care (Section 24)

The heads of the AIVD and the MIVD are responsible for applying technical, staffing and organisational measures to ensure lawful data processing.[8] Promotion of the quality of data processing to ensure that data processing is lawful is a new requirement that was not included in the old ISS Act 2002. The duty of care explicitly requires more from the AIVD and the MIVD than just the introduction of the duties that the law imposes on them when collecting and analysing data and when they are actually being used by employees of the services, among other things.[9]

Among other things, the duty of care entails that both services must continually be in control of the way in which they process data and ensure that data processing is and continues to be in line with the applicable legal regulations (compliance). Policy, process descriptions and working instructions, in which consideration is given to the allocation of roles and responsibility, may contribute positively to this.

2 Section 1(f) of the ISS Act 2017.
3 Letter to the President of the Senate dated 6 April 2018, Parliamentary papers I 2017/18, 34588, G.
4 Section 18 of the ISS Act 2017.
5 Also see report no. 38 (2014), p. 29.
6 See report no. 56 (2018) about the multilateral exchange of data on (alleged) jihadists by the AIVD, Appendix II, p. 2.
7 Parliamentary papers II 2016/17, 34588, no. 3, p. 47.
8 Section 24(2)(a) of the ISS Act 2017.
9 Also see report no. 59 (2018), p. 7.

The need to continually be in control also requires the services to use a number of tools that give them an insight (a central insight) into the functioning of data-processing processes and systems and, as such, puts them in a position to promptly identify risks and take appropriate measures. This is important for internal control in the services but also for the facilitation of effective oversight by the CTIVD.

Proportionality and subsidiarity (Section 26)

Proportionality involves the consideration of the purpose envisaged and the disadvantage for the data subject. The 'disadvantage for the data subject' refers to the associated infringement of the fundamental rights of the data subject. Use of the investigatory power must also be proportional to the purpose for which it is envisaged.

The subsidiarity assessment entails that the AIVD or the MIVD must opt for the investigatory power that is the least invasive for the data subject.[10] The use of special investigatory powers like cable interception are usually regarded as more invasive for the data subject than the use of general investigatory powers.

As targeted as possible (Section 26)

Further to the implementation of the adopted motion of Recourt, (then) a Member of the Dutch House of Representatives, (Parliamentary papers II 2016/17, 34588, no. 66), the power of cable interception must be used in a manner that is 'as targeted as possible'. In accordance with the pledge of the government in its letter of 6 April 2018 to both the Senate and the Dutch House of Representatives, the policy rule published on 25 April 2018 stated that the services are to use special investigatory powers in a manner that is as targeted as possible, among other things.[11] This pledge was included in Section 26 of the amended Act of 15 July 2021. The 'as targeted as possible' criterion applies to the entire interception process. The authorisation request referred to in Section 29 must explicitly state how the service will meet the requirement for the special investigatory power to be used in a manner that is as targeted as possible. However, legislative history does not indicate exactly what the 'as targeted as possible' requirement involves.

When defining the 'as targeted as possible' requirement, the government chose to be guided by the criterion of the TIB.[12] The government does its utmost to define the 'as targeted as possible' requirement in the explanatory memorandum to the proposed amendment:

"The services must address the 'targeted as possible' requirement as much as reasonably possible (and insofar as applicable) in the authorisation request by delineating the data to be collected: geographically, by time, by type of data/traffic, by object/target, by behaviour or otherwise. When doing this, consideration must also be given to the intelligence context in which the previously unknown threat is to be sought, to the phase of the investigation, the need for falsification, the time element and the technical options actually possible."[13]

The government points out that the criterion above leaves scope for the broader collection of data, in a less targeted manner in certain circumstances. For example, technological limitations may make it impossible to make a certain 'selection' in the data set collected and for this reason the entire set is collected. The phase of the investigation is decisive too.

10 *Parliamentary papers II* 2016/17, 34588, no. 3, p. 202.
11 Section 5, Policy rules ISS Act 2017.
12 "[T]he extent to which, when obtaining data, the collection of data that are not strictly necessary for the investigation are kept to a minimum, given the technical and operational circumstances of the case", see *Parliamentary papers II* 2018/19, 35 242, no. 3, p. 4 and 5.
13 *Parliamentary papers II* 2018/19, 35 242, no. 3, p. 5.

In the exploration phase, the broader use of investigatory powers will (often) be unavoidable initially.[14] Operational interests may also mean that an investigatory power is not used in a manner that is as targeted as possible. For example, the prevention of an awareness of the data on which the service has targeted its attention. Financial interests may play a role as well. It must be possible to expect the service to spend the financial resources available in an efficient manner. In the substantiation of the authorisation request, a persuasive explanation will need to be included of why the investigatory power *cannot* be used in a manner that is as targeted as possible and why it is justified for more data to be collected than necessary for the investigation itself. Therefore, the authorisation request must also describe the measures that will be taken to protect the data that are not substantively necessary for the investigation.[15]

In practice, the services meet the requirement of interception and storage being as targeted as possible in the following three ways: (1) the communication medium selected, (2) the data stream selected and (3) additional positive and negative filters.

The communication medium selected
In practice, the services first select a communication medium (such as a cable or satellite) that is expected to contain information relevant to the investigation assignments which the services must carry out. The physical transfer point at a communication service provider where the services receive the intercepted data is called an access location.

The data streams selected
Dozens of channels can be distinguished in the fibres of a cable. The legislator has stated that the services select data streams (and, as such, channels) that they expect to be relevant to the success of investigation assignments of the services.

The use of filters
Not all intercepted data streams are stored for further processing. This is because filtering takes place shortly after the actual interception of data.[16] Filtering is the process in which it is decided whether or not to store data based on (technical) characteristics like an IP address, language or an e-mail address. A positive filter entails that data are stored if they match the characteristic in question. A negative filter identifies data that is not to be stored.

Data reduction and relevance (Section 27)
The duty to reduce data for cable interception ensues from Sections 27 and 48(5). To summarise, these provisions entail that the amount of data collected by means of cable interception must be reduced to data that is potentially relevant as quickly as possible.

In a general sense, the relevance of data must be assessed after they have been intercepted and stored so that, ultimately, just relevant data are left.[17]
The relevance assessment must take place within a certain period of time; this is the so-called 'retention period'. The retention period starts at the time when the data are intercepted. The retention period for cable-interception data is one year (Section 4, Policy rules ISS Act 2017). This retention period may

14 *Parliamentary papers II* 2018/19, 35 242, no. 3, p. 5
15 *Parliamentary papers II* 2018/19, 35 242, no. 3, p. 6 and 7.
16 The use of filters is part of the interception power set out in Section 48.
17 Section 27(1) of the ISS Act 2017 states that relevance is the case when data are relevant for the investigation for which they have been obtained, or for any other ongoing investigation that falls under the tasks referred to in Section 8(2)(a) and (d), or Section 10(2)(a), (c) and (e) of the ISS Act 2017. The memorandum in response to the report adds that the relevance assessment is a substantive assessment "that, among other things, considers whether the data contribute to the investigation in a positive sense and also whether they could answer certain questions negatively, disprove hypotheses or otherwise be of decisive importance", see *Parliamentary papers II*, 2016-17, 34 588, no. 18, p. 32.

be extended twice, by a maximum of one year each time.[18] The Minister, or the head of the service on their behalf, must authorise an extension of the retention period. It is not necessary to submit the extension request to the TIB. Thus, data collected via cable interception may be retained for a maximum of three years. Intercepted data that have been encrypted may be retained for three years and this period may be extended by a period of three years each time. The requirement of Section 27(1), namely that the relevance assessment must take place 'as soon as possible' does not apply for data that have been obtained via cable interception.[19] However, according to the legislator, this does not mean that data will be retained for the full three years. Pursuant to Section 18, the services must reduce data as soon as possible in order to keep the infringement (if any) of the privacy of citizens to a minimum.[20]

Performance of tasks (Section 28 of the ISS Act 2017)

Section 28(1) states that a special investigatory power may only be used if necessary for the proper performance of the tasks of the AIVD, as referred to in Section 8(2)(a) and (d) and of the MIVD, as referred to in Section 10(2)(a), (c) and (e).[21] Specifically, this means that the investigatory powers in Sections 48, 49(1), 52 and 53 may only be used for the tasks below:

- The carrying out of investigations about organisations and persons that, by virtue of their activities or the goals they pursue, prompt the serious suspicion that they constitute a danger to the continued existence of the democratic legal system, or for the security of other State interests (AIVD) (Section 8(1)(a));
- The carrying out of an investigation about other countries (AIVD) (Section 8(1)(d);
- The carrying out of an investigation about the potential and armed forces of other powers for the purpose of ensuing a correct set-up and effective use of the armed forces (MIVD) (Section 10(2)(a));
- The carrying out of an investigation into factors that affect or could affect the enforcement and promotion of international legal order, insofar as the armed forces are involved or the expectation is that they could be involved (MIVD) (Section 10(2)(a));
- The carrying out of an investigation that is necessary to take measures to prevent activities designed to harm the safety or readiness of the armed forces (MIVD) (Section 10(2)(c));
- The carrying out of an investigation that is necessary to take measures to promote the correct course of the mobilisation and concentration of the military (MIVD) (Section 10(2)(c));
- The carrying out of an investigation about other countries, on subjects with military relevance (MIVD) (Section 10(2)(e)).

Authorisation requirements (Section 29)

The service must substantiate its authorisation request and the extension of authorisation. Section 29 sets out the requirements to be met by requests of this nature. Added to the above, pursuant to Section 5 of the policy rules of the ISS Act 2017 (see section 3.3), additional substantiation is required for the 'as targeted as possible' criterion. So, the request must contain the following elements:

18 This is a different period than the retention period applicable to data collected via other special investigatory powers. A retention period of one year applies to these data (Section 27(1) of the ISS Act 2017).
19 *Parliamentary papers II* 2016/2017, 34588, no. 3, p. 102.
20 *Parliamentary papers II* 2018/19, 35 242, no. 3, p. 102.
21 The investigatory power may not be used to carry out security screening (the so-called B task).

- An indication of the investigatory powers for which authorisation is being requested;
- If applicable, the identity of the person or organisation in respect of whom or which use of the investigatory power is being required;
- The capacity of the data subject if they are a journalist or lawyer;
- A description of the investigation for which the investigatory power will be used;
- A description of the purpose envisaged;
- The reason why it is deemed necessary to use the investigatory power. Considerations in respect of the requirements of proportionality and subsidiarity must be set out here as well;
- Substantiation of how the investigatory power will be used in a manner that is as targeted as possible;
- If an extension is the case, an indication of the results achieved by using the investigatory power;
- The description of the investigation and the purpose for which the investigatory power will be used may not be a general description. It must be as specific as possible.

Record keeping (Section 31 of the ISS Act 2017)

Section 31 of the ISS Act 2017 states that records must be kept of the use of an investigatory power for the collection of data. The legislator does not specify how these records are to be kept. As such, they may also be kept in a manner other than in writing. Automated recording (logging) can be used as a format for record keeping.[22]

Interim conclusion

The general provisions of the ISS Act 2017 below apply in any event to the operationalisation of the access location and the implementation of interception:

- Data may only be processed for a certain purpose and only if necessary (and also proportional and subsidiary);
- Technical, staffing and organisational measures must have been taken that are such that the services are continually in control of the way in which data are processed and adequate control and effective oversight are possible (duty of care);
- Use of the power must be proportional to the purpose for which it is envisaged (proportionality requirement);
- The least invasive investigatory power must be chosen (subsidiarity requirement);
- The investigatory power must be used in a manner that is as targeted as possible;
- The services must reduce data as soon as possible in order to keep the infringement (if any) of the privacy of citizens to a minimum;
- Data that have not been assessed for relevance will be destroyed immediately when the retention period ends;
- Intercepted data that are not relevant must be destroyed immediately;
- Use of the investigatory power must be necessary for the duties to be exercised;
- The authorisation request must meet the relevant requirements;
- Records must be kept of the use of an investigatory power for the collection of data.

22 Also see *Parliamentary papers II* 2016/17, 35488, no. 3, p. 50.

3. Operationalisation of the access location

This chapter describes the specific duties for the services that are set out in Section 52 (duty to provide information) and Section 53 (duty to assist).

Information and the assistance of the communication service provider are essential if it is to be possible to implement cable interception properly. The same is not the case for the interception of satellite and radio communications. The service has its own satellite ground station (among other things) for this type of interception. Section 52 gives the services the power to instruct a communication service provider to provide the information necessary for the implementation of interception. The explanatory memorandum explains that Section 52 serves two purposes. On the one hand, this power gives the services the opportunity to map out the communication landscape and then use the interception power provided for in Section 48 in a 'targeted' manner.[23] On the other hand, this investigatory power enables the services to request information to substantiate a request for the use of Section 48 (interception) and the assistance required in this respect based on Section 53.

Section 53 provides the services with the investigatory power to instruct the relevant communication service provider to assist in the implementation of cable interception. The use of this investigatory power is linked to the use of interception as set out in Section 48. This means that the duty to assist can only be used if authorisation has been obtained for the use of interception. Providers have a duty to comply with the request for assistance. Failure to comply with a request of this nature is punishable (Section 143). The legislator has opted for a duty to ensure that the services do not have to rely on voluntary assistance in cases in which national security is in danger.

The interest to be protected as set out in Sections 52 and 53 is different to many other special investigatory powers of the services. Where the other investigatory powers often set standards in respect of the infringement of the fundamental rights of citizens, Sections 52 and 53 create a duty for market parties. Therefore, the interests to be protected are the interests, rights and duties of these private market parties. For example, the protection of company-sensitive data, the safeguarding of the continuity of service provision by the provider or the fact that a provider incurs costs to meet the duty to provide information and assist.

Nature of the duty to provide information

The *Besluit gegevensverstrekking onderzoek van communicatie Wiv 2017* (decree on the provision of data for a communication investigation under the ISS Act 2017) regulates which information can be requested for the purpose of cable interception.[24] This information includes the technical data of, for example, the telecommunications network or service operated by the relevant provider. Information may also be requested to make it possible to determine which technical provisions must be made to actually be able to use cable interception.

The data in question could also be data that could help map out the communication landscape. To be able to intercept in a targeted manner, it must be clear where and which type of communication will be processed or transported. Examples include information about business customers, lessees and lessors of the communication service provider and the known data about the services provided and characteristics of traffic flows.[25]

23 *Parliamentary papers II* 2016/17, 34588, no. 3, p. 113 et seq.
24 Bulletin of Acts and Decrees 2018, 116.
25 *Parliamentary papers II* 2016/17, 34588, no. 3, p. 114.

This insight can be obtained in part through the use of search aimed at interception. However, some of the information will only be possible to obtain from the relevant providers themselves.

Authorisation

No ministerial authorisation is required for the use of the duty to provide information. The head of the service will grant the assignment in writing. The legislator explains that the data in question are not those that jeopardise the privacy of specific persons. After all, the data in question are primarily of a technical and commercial nature. Nor does the Act provide for any maximum period of time in which the duty to provide information may be used. Pursuant to Section 29, an authorisation to use a special investigatory power as referred to in section 3.2.5 of the ISS Act 2017 may be granted for a period of no more than three months. Section 52 is a special investigatory power from section 3.2.5. However, no authorisation is granted here. Instead, the head of the service instructs a provider to provide data.

In contrast to Section 52, the authorisation of the Minister in question is required for use of the duty to assist. The authorisation will be granted for a period of no more than one year and can be extended by the same period of time each time. The head of the service may make the authorisation request to the Minister. After the Minister has granted authorisation, the TIB will assess the lawfulness of the authorisation granted. Section 29 sets out the requirements to be met by an authorisation request (see chapter 2). Added to this, Section 53 contains two additional conditions to be met by the authorisation request, namely the exact provider concerned and a description of the assistance expected of the provider.

Consultation prior to use of the duty to assist

Once authorisation has been granted to use the duty to assist, the services must first consult the provider in question. Among other things, the purpose of the consultation with the provider is to discuss the practical specifics of the assistance. For example, the exact nature of the technical provisions. Other matters may be discussed as well. For example, the implementation period and any staffing and organisational aspects associated with the implementation of the authorisation granted.[26] The actual assistance will only start after this consultation has taken place and technical measures may be taken to realise interception. The consultation above does not need to be repeated in the case of an extension.

Leaving technical provisions in place

If, at some point, it is no longer necessary to intercept telecommunication via the provider in question, the services will be authorised to leave the technical provisions in place at the provider. This could be the case, for example, in the event of a change to the investigation assignments of the services. Pursuant to Section 53(6), the provisions may be left in place for up to one year after the authorisation period ends. The legislator explains this by saying that use of the interception power at the provider in question requires a customised approach, in terms of both implementation time and investment. If it is necessary to call upon the assistance of the provider in question again within this year, this can be realised in the short term. If the technical provisions are no longer necessary, it will be possible to release the provider from its duties.[27]

26 *Parliamentary papers II* 2016/17, 34588, no. 3, p. 116.
27 Section 53(6) of the ISS Act 2017.

Interim conclusion

In addition to the duties applicable by virtue of the general provisions of the ISS Act 2017, Section 52 adds the following specific obligations in respect of the power to impose the duty to provide information on a party:

- The data requested must fall under the *Besluit gegevensverstrekking onderzoek van communicatie Wiv 2017*;
- The head of the service must have authorised use of the duty to provide information;
- The Minister must have authorised use of the duty to assist. The TIB will assess the lawfulness of this authorisation;
- Authorisation of the use of the duty to assist may be extended for a maximum of one year each time;
- The content of the authorisation request to use the duty to assist must meet the requirements above;
- If assistance is no longer necessary, the provisions may remain in place for a maximum of one year. If there is no longer a reason to keep the provisions in place, the provider will be relieved of its duty.

4. Implementing cable interception

This section describes the specific legal duties applicable when implementing cable interception. As described in the report, a limited form of interception took place in the investigation period, namely snapshotting. There is no legal basis for snapshotting in the ISS Act 2017, but it is used pursuant to Section 48 (cable interception). The data stored are then investigated based on Section 49(1) (search aimed at interception) with the object of determining their potential intelligence value.

Authorisation

The authorisation of the relevant Minister is required for use of the investigatory power of cable interception and search aimed at interception.[28] Given the close connection between the power to intercept and the power to search aimed at interception, it is only natural that 'combined requests' will often be the case, in which authorisation is sought for both investigatory powers. After the Minister has granted authorisation, the TIB will assess the lawfulness of the authorisation. The authorisation will be granted for a period no more than one year and can be extended by a maximum of one year each time. The legislator has deviated here from the regular period of three months. The reason for this is that the privacy infringement is just limited in this phase[29] because the content of the data may only be accessed for technical reasons in this phase.

Content of authorisation request

In addition to the general requirements of Section 29 that apply to the content of a request for authorisation (see chapter 2), two additional requirements apply to cable interception. It follows from Section 48(3) that additional substantiation will be required if both metadata and content are intercepted.

In the request, a description must also be provided of the telecommunication or data transfer by means of an automated device or system for which the investigatory power will be used. A clear description must be provided of the type of interception to be used. For example, the interception of cable or of satellite and radio communications. If possible, the nature of the communication (for example, GSM radio or internet traffic) must be described, whether or not with a geographical delineation. If possible, the services must also include which types of traffic are relevant and when. For example, speech, chat traffic or file exchange. Finally, the services must specify the part of the cable infrastructure concerned and also the type of traffic to be intercepted.[30]

Specific purpose for processing the data

Intercepted data may only be processed for the purposes set out in Sections 48 and 49(1). Pursuant to Section 48, the services may conduct a technical analysis to optimise use of the interception power. The services are also permitted to consult content for this purpose. In this context, 'content' refers to the content of communication (such as the text of an e-mail) in contrast to traffic data, i.e. metadata (who is communicating with whom. For example, the sender and receiver of an e-mail).

28 Section 48(2) of the ISS Act 2017.
29 *Parliamentary papers II* 2016/2017, 34588, no. 3, p. 99.
30 Section 48(3) of the ISS Act 2017 and *Parliamentary papers II* 2016/2017, 34588, no. 3, p. 99.

Based on Section 49(1) (search aimed at interception), the services may investigate data in order to:

- determine the characteristics and nature of the telecommunication;
- determine the identity of the person or organisation associated with the telecommunication.

In short, this investigatory power enables the services to determine whether they are actually intercepting the data envisaged.

Thus, the content of the intercepted data may only be accessed for the purpose of optimising interception. If the service observes that use of communication content is necessary for the proper execution of tasks, an authorisation request must be submitted for Section 47 (targeted interception) or Section 50 (selection).[31]

Division of tasks and roles

The various phases of the interception process serve a specific purpose. Both Sections 48 and 49 state that only designated employees may access the data collected for this particular purpose. Authorised employees are designated to the exclusion of others by order of the Minister. The Minister can mandate this power to the head of the service.[32] To comply with the duty of care and the general requirement to process data carefully, tasks and roles must be divided too. The division of tasks and roles can be achieved by granting digital access to data by means of authorisations but also via physical measures. Physical measures may include compartmentation by means of the use of an access card for the room in which the data are processed and measures to prevent employees being able to see the data displayed on a screen other than their own.[33]

Only designated employees may access intercepted data. Where Section 48 is concerned, employees may only access intercepted data for safeguarding purposes and to check that data are received properly and can be stored. Checking correct receipt may include organising and labelling data or checking for noise.[34] These employees may also decrypt data if possible. Once data have been decrypted, the content of the communication may be accessed but solely for the purpose described in Section 48.

As regards Section 49(2), only designated officials may access the data collected with the purpose of optimising interception and being able to answer the question of whether the data intercepted are the data envisaged.

Record keeping

It follows from Section 49(3) that the services may keep records of the results of the application of search aimed at interception when necessary for the proper execution of tasks. This form of record is separate to the legal duty to keep records (Section 31) of the use of the power as set out in Section 49(1). The exploration of data may lead to a certain view of the data stream or of 'the communication landscape', which can provide a starting point for future activities. For example, analyses that show that a certain fibre does not contain any relevant data, because of which interception must not continue.

An analysis of this nature may reveal what kind of data are sent over the cable and what persons and/or organisations generally use this fibre. An analysis like this may also be used for the purpose for which they were recorded. This does not mean that all employees may access these results. Access is limited to those employees who need to access the results to execute the tasks conferred on them.[35]

---

31 *Parliamentary papers II* 2016/2017, 34588, no. 3, p. 107.
32 Section 48(4) of the ISS Act 2017.
33 In CTIVD report no. 70, p. 28, the CTIVD stresses that physical distance also forms part of the safeguard function of the division of tasks and roles.
34 *Parliamentary papers II* 2016/2017, 34588, no. 3, p. 97 and 98.
35 Parliamentary papers II 2016/2017, 34588, no. 3, p. 104.

These employees may include those who are involved in the intelligence process and need to access a record for this purpose. For example, to prepare a new authorisation request.

No further investigation of content in the search phase

In this phase, the content of the intercepted data may only be accessed for the purpose of optimising interception. If the service observes that use of communication content is necessary for the proper execution of tasks, an authorisation request must be submitted for Section 47 (targeted interception) or Section 50 (selection).[36]

The explanatory memorandum to the Act states that targets are using open and anonymous ways to use the internet (such as Wi-Fi networks in hotels, restaurants and other public spaces) because of which the targeted interception of traditional telecommunications service providers in the Netherlands is becoming increasingly less effective and investigation-related interception is necessary.[37] However, if the target is encountered in the search, a targeted interception may be possible and it will be important to decide whether Section 47 is to be applied given the 'as targeted as possible' criterion and the requirement of subsidiarity.

According to the legislator, there are situations in which the service will encounter data or new persons or organisations in the search aimed at interception phase that are eligible for investigation by the service. In this situation, the service can submit an authorisation request for the selection of data (Section 50(1)(a).[38]

Termination and origination in the Netherlands

In the accompanying letter to the policy rules ISS Act 2017, the Ministers of BZK and Defence pledged that there was virtually no prospect of cable interception being used in the coming years for investigation into communication that originates and terminates in the Netherlands.[39] The idea is that a more targeted medium can be used in situations like this. For example, targeted interception. Other countries that use cable interception often apply a similar exception. An exception to this pledge has been made for the investigation of cyber defence. The reason that the Minister gives for this exception is that the Dutch digital infrastructure is misused in digital attacks and cable interception can be necessary to identify this misuse.

When the pledge was made, the question being asked in social debate was whether the new power of cable interception would enable the services to intercept entire residential districts, because of which arbitrary Dutch citizens could be caught up in 'the dragnet'. By making this pledge, the Ministers would seem to be wanting to put this assumption to bed once and for all. However, it is unclear exactly what the pledge entails in practice and which interest or interests it serves. The question is whether the purpose of the pledge is to protect Dutch State citizens or all persons in the Netherlands.

If the latter is the case, cable interception may not be used to intercept the communication of foreign targets that are in the Netherlands (temporarily) if the communication also terminates in the Netherlands.

36 *Parliamentary papers II* 2016/2017, 34588, no. 3, p. 107.
37 *Parliamentary papers II 2016/2017, 34588, no. 3, p. 92.*
38 In the investigation period, the requests for authorisation state that the data may not be used by the intelligence process.
39 *Parliamentary papers II* 2017/18, 34588, No. 76.

Retention periods

The retention period for cable-interception data is one year (chapter 4, Policy rules). This retention period may be extended twice, by a maximum of one year each time.[40] In the authorisation request, the services will be expected to demonstrate why the data in question should be retained for a further period of one year. The Minister, or the head of the service on their behalf, must authorise an extension of the retention period. It is not necessary to submit the extension request to the TIB, as applicable in respect of the investigatory powers for which the TIB plays a role. Thus, data collected via cable interception may be retained for a maximum of three years. Intercepted data that have been encrypted may be retained for three years and this period may be extended by periods of three years each time.

Interim conclusion

In addition to the duties applicable by virtue of the general provisions of ISS Act 2017, Section 48 adds the following specific duties in respect of the power of cable interception:

- Cable interception and search aimed at cable interception may only be used after the relevant authorisation has been obtained from the Minister in question;
- The TIB must assess the lawfulness of the authorisation of the Minister;
- Authorisation for the use of cable interception and search aimed at interception will be granted for a maximum of one year;
- Data may only be processed for the purposes set out in Sections 48 and 49(1);
- Tasks and roles must be divided when processing intercepted data;
- The employees in question must have been designated for the tasks and roles in question;
- Records may be kept of the results of the investigation based on Section 49(1);
- The power of cable interception will not be used to investigate communication that originates and terminates in the Netherlands, except where an investigation relates to cyber defence;
- Data that have been obtained by means of cable interception may be retained for a maximum of one year. This period may be extended by one year a maximum of two times. The extension must be substantiated. The Minister, or the head of the service on their behalf, must grant authorisation;
- Encrypted data may be retained for a maximum of three years. Until the data have been decrypted, the retention period for them may be extended by three years each time. This will only be possible with the authorisation of the Minister, or the head of the service on their behalf.

40 This is a different period than the retention period applicable to data collected via other special investigatory powers. A retention period of one year applies to these data (Section 27(1) of the ISS Act 2017).

5. Cyber defence

In their letter of 25 April 2018, the Ministers of BZK and Defence pledged that there was virtually no prospect of cable interception being used in the coming years for investigation into communication that originates and terminates in the Netherlands. However, in their letter, they did make an exception to their pledge for cyber defence. The reason that the Ministers give for this exception is that the Dutch digital infrastructure is misused in digital attacks and cable interception can be necessary to identify this misuse.

In contrast to investigations into other subjects, cyber defence investigations can take place on the basis of Section 48 and Section 49(1) of the ISS Act 2017. This means that the information collected that is used for search aimed at interception can be used for cyber-related investigations. These investigations take place through the use of network monitoring or network detection, among other things.

Network monitoring or network detection is used to detect anomalies in normal internet traffic. These anomalies may point to an attack on a server by a state actor, among other things. A DDoS attack, for example.[41] A DDoS attack is a cyber attack in which so much internet traffic is sent to a server, for example, that it is overwhelmed and crashes. Investigations of the Dutch network are necessary to recognise attacks of this nature. The explanatory memorandum states that Section 49(1)(a) of the ISS Act 2017 makes it possible to investigate characteristics of unwanted activities (for example, signatures of malware) and traffic that displays unusual anomalies (anomaly detection).

An investigation of this nature can be conducted both offline and online. In the first case, a data file of intercepted data is created, which is then investigated. In the second case, data traffic is analysed real time and online. The services perform this so-called network monitoring based on their intelligence and counterintelligence task.[42]

To be able to engage in network monitoring or network detection activities, authorisation must be obtained from the Minister and the relevant requirements (ensuing from Sections 29, 48(1) and 49(1) of the ISS Act 2017) must be met. The authorisation request must provide as much detail as possible about the investigation in question, the part of the cable-bound infrastructure to be investigated and for which purpose. The request must also clearly indicate exactly what the investigation will entail. As the network monitoring or network detection activity (Section 49(1) of the ISS Act 2017) cannot take place without the power of cable interception pursuant to Section 48 of the ISS Act 2017, a combined request will often be made.[43]

41 DDoS stands for Distributed Denial of Service and is an attack in which an attempt is made to (temporarily) disable a computer, network or service.
42 Section 8(2)(a) and Section 10(2)(a) and (c) of the ISS Act 2017.
43 *Parliamentary papers II* 2016/17, 34588, no. 3, p. 105.

6. Summary of legal requirements

Based on the legal requirements, the CTIVD has arrived at the assessment framework below for the review report about the use of cable interception by the AIVD and the MIVD.

Legal requirements - general provisions

- Data may only be processed for a certain purpose and only if necessary (and also proportional and subsidiary);
- Technical, staffing and organisational measures must have been taken that are such that the services are continually in control of the way in which the data are processed and adequate control and effective oversight are possible;
- Use of the power must be proportional to the purpose for which it is envisaged (proportionality requirement).
- The least invasive investigatory power must be chosen (subsidiarity requirement);
- The investigatory power must be used in a manner that is as targeted as possible;
- The services must reduce data as soon as possible in order to keep the infringement (if any) of the privacy of citizens to a minimum;
- Data that have not been assessed for relevance will be destroyed immediately when the retention period ends;
- Intercepted data that are not relevant must be destroyed immediately;
- Use of the investigatory power must be necessary for the duties to be exercised;
- The authorisation request must meet the relevant requirements;
- Records must be kept of the use of an investigatory power for the collection of data.

Legal requirements - operationalisation of access location

- The data requested must fall under the *Besluit gegevensverstrekking onderzoek van communicatie Wiv 2017;*
- The head of the service must have authorised use of the duty to provide information;
- The Minister must have authorised use of the duty to assist. The TIB will assess the lawfulness of this authorisation;
- Authorisation of the use of the duty to assist may be extended for a maximum of one year each time;
- The content of the authorisation request to use the duty to assist must meet the requirements above;
- If assistance is no longer necessary, the provisions may remain in place for a maximum of one year. If there is no longer a reason to keep the provisions in place, the provider will be relieved of its duty.

Legal requirements - implementing cable interception

- Cable interception and search aimed at cable interception may only be used after the relevant authorisation has been obtained from the Minister in question;
- The TIB must assess the lawfulness of the authorisation of the Minister;
- Authorisation for the use of cable interception and search aimed at interception will be granted for a maximum of one year;
- Data may only be processed for the purposes set out in Sections 48 and 49(1);
- Tasks and roles must be divided when processing intercepted data;
- The employees in question must have been designated for the tasks and roles in question;
- Records may be kept of the results of the investigation based on Section 49(1);
- The power of cable interception will not be used to investigate communication that originates and terminates in the Netherlands, except where an investigation relates to cyber defence;

- Data that have been obtained by means of cable interception may be retained for a maximum of one year. This period may be extended by one year a maximum of two times. The extension must be substantiated. The Minister, or the head of the service on their behalf, must grant authorisation;
- Encrypted data may be retained for a maximum of three years. Until the data have been decrypted, the retention period for them may be extended by three years each time. This will only be possible with the authorisation of the Minister, or the head of the service on their behalf.

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